PODER DIGITAL

ESTADO DE PODER 2023

FUHEM educación+ ecosocial
tni transnational institute
CLACSO

Estado de Poder 2023

Poder digital

Estado de Poder 2023 : poder digital / Apoorva PG ... [et al.]. - 1a ed. - Ciudad Autónoma de Buenos Aires : CLACSO ; Amsterdam : TNI Transnational Institute, 2023.

Libro digital, PDF

Archivo Digital: descarga y online

ISBN 978-987-813-629-5

1. Financiamiento. 2. Migración. 3. Inteligencia Artificial. I. PG, Apoorva.

CDD 306.2

Arte de tapa: Jimena Zazas
Diseño de interiores: Eleonora Silva
Corrección de estilo: Mariela Gurevich

Estado de Poder 2023

Poder digital

PLATAFORMAS PARA EL DIÁLOGO SOCIAL
FUHEM educación + ecosocial
tni transnationalinstitute
CLACSO

CLACSO
Consejo Latinoamericano de Ciencias Sociales
Conselho Latino-americano de Ciências Sociais

CLACSO Secretaría Ejecutiva
Karina Batthyány - Directora Ejecutiva
María Fernanda Pampín - Directora de Publicaciones

Equipo Editorial
Lucas Sablich - Coordinador Editorial
Solange Victory y Marcela Alemandi - Producción Editorial

Estado de Poder 2023. Poder digital (Buenos Aires: CLACSO, noviembre de 2023).
ISBN 978-987-813-629-5

CLACSO. Consejo Latinoamericano de Ciencias Sociales

Conselho Latino-americano de Ciências Sociais
Estados Unidos 1168 | C1023AAB Ciudad de Buenos Aires | Argentina
Tel [54 11] 4304 9145 | Fax [54 11] 4305 0875
<clacso@clacsoinst.edu.ar> | <www.clacso.org>

Suecia
Sverige

Este material/producción ha sido financiado por la Agencia Sueca de Cooperación Internacional para el Desarrollo, Asdi. La responsabilidad del contenido recae enteramente sobre el creador. Asdi no comparte necesariamente las opiniones e interpretaciones expresadas.

tni
transnationalinstitute

TNI
Editor: Nick Buxton
Traducciones: Mercedes Camps, Nuria del Viso
Equipo asesor editorial: Sofia Scasserra, Deepti Bhartur, Nuria del Viso
Ilustradores: Zoran Svilar y Anđela Janković
Investigación para infografías: Hannah Hasenberger
Diseño de infografías: Evan Clayburg

Transnational Institute – www.TNI.org
Noviembre 2023

Índice

Aprovechar los medios informáticos

De qué modo los movimientos populares pueden derribar los monopolios de las grandes empresas tecnológicas

Entrevista a Cory Doctorow

Traducción al español por Mercedes Camps
Ilustración de Anđela Janković

Cory Doctorow es un escritor prolífico, un brillante novelista de ciencia ficción, periodista y activista tecnológico. Es consultor especial de la Electronic Frontier Foundation, una organización no gubernamental que se dedica a la defensa de las libertades civiles y la libertad en la legislación, las políticas, las normas y los tratados relacionados con la tecnología. Su publicación más reciente, *Chokepoint Capitalism* (escrita junto con Rebecca Giblin), es una poderosa investigación sobre el modo en que los monopolios tecnológicos han limitado a los mercados de trabajo creativos y cómo los movimientos pueden defenderse. Nick Buxton, redactor responsable del informe el Estado del Poder del TNI, y Shaun Matsheza, presentador del podcast el Estado del Poder, conversaron con Cory tras las inundaciones en su ciudad natal Burbank, California. Lo que sigue es un fragmento editado de la entrevista.

Comencemos por la primera gran pregunta abierta que es el tema central del informe del Estado del Poder del TNI: ¿quién tiene el poder digital hoy en día?

Cory: Es una excelente pregunta. Como ha observado Tom Eastman, un desarrollador de software de Nueva Zelandia, Internet ha evolucionado en cinco sitios web gigantes repletos de capturas de pantalla de textos de los otros cuatro. Unas pocas empresas poderosas, a saber: Google, Amazon, Facebook, Apple y Microsoft, son, en términos de los reguladores europeos, las *guardianas*, es decir, las que tienen derecho a decidir quién puede expresarse, quién puede contactar a quién y cómo funciona. Se trata de un alejamiento profundo de los valores sobre los cuales se fundaron estas empresas, que se basaban en la idea de que Internet sería un nuevo tipo de red en el que todas las personas

que deseaban comunicarse con cualquier otra persona podían hacerlo sin la intervención de un tercero. Ahora tenemos una serie de *puestos de control* en los cuales una de muy pocas empresas puede controlar la libertad de expresión o actividades similares, como la recaudación de fondos.

Y cabe destacar que el motivo por el cual se permitió que esas empresas crecieran del modo en que lo hicieron, el motivo por el cual los reguladores hicieron la vista gorda es que los Estados consideran a esas empresas como posibles asistentes en sus propios ejercicios de poder.

LAS GRANDES EMPRESAS TECNOLÓGICAS SON LA INDUSTRIA MÁS RENTABLE Y VALIOSA

Las 10 principales empresas según las ventas, ganancias y el valor de mercado

Fuente: Forbes Global 2000, 2021

Es muy improbable, por ejemplo, que la Agencia de Seguridad Nacional (NSA) hubiera podido obtener autoridad regulatoria o convencer a los usuarios a tener aparatos que anuncian nuestra ubicación en todas partes del mundo. Al permitir que estas empresas hicieran eso mismo, al no intervenir y exigir que se impongan regulaciones, el Gobierno de los Estados Unidos ha forjado un futuro en el que la NSA no necesita interceptar nuestras comunicaciones. Simplemente puede pedir información a Facebook, Google o Apple, a la cual no podría acceder de otro modo. Es decir que eso debe entenderse como una asociación público-privada.

¿Cómo se da esta interacción de poder entre el Estado y las empresas?

Cory: Un ejemplo muy claro de ello es que Google recopila información sobre nuestra ubicación de un modo engañoso. Si apagas el rastreo de ubicación en tu dispositivo Android o iOS, el dispositivo seguirá rastreando tu ubicación. Hay al menos doce lugares en tu dispositivo en los que debes apagar el rastreo de ubicación para desactivarlo por completo. Y aun en ese caso, no está claro que el rastreo realmente se detenga. Incluso los empleados de Google se han quejado de que no saben cómo apagar el rastreo. Ahora bien, en un mundo cuerdo, esta sería una actividad prohibida. El artículo 5 de la Ley de la Comisión Federal de Comercio otorga al organismo amplias facultades para intervenir a fin de evitar prácticas "injustas y engañosas". Es difícil defender la idea de que si haces clic en el botón de "No rastrear mi ubicación" y el dispositivo rastrea tu ubicación de todos modos, esa práctica es justa y no engañosa. Claramente este es el tipo de actividad que prohíbe la ley. Y, sin embargo, los Gobiernos no han hecho nada. No se ha aprobado legislación ni normativa para impedirlo.

Al mismo tiempo, Google ha aumentado el uso de datos de ubicación y lo que los Estados denominan órdenes de allanamiento para barreras geográficas, también denominadas órdenes de allanamiento inversas. Ello ocurre cuando un organismo de aplicación de la ley acude a Google, con o sin orden de allanamiento, y describe una

ubicación –una manzana, calle por calle– y un periodo de tiempo, por ejemplo de las 13:00 a las 16:00 horas, y solicita información de todas las personas que se encuentran en esa manzana. Ello se utilizó ampliamente contra los manifestantes de Black Lives Matter y, posteriormente, contra quienes participaron en la sedición del 6 de enero.[1] De modo que, el Estado tiene un incentivo perverso para no impedir esta conducta engañosa e injusta.

Sin embargo, es una conducta peligrosa, porque una empresa del tamaño de Google siempre sufrirá amenazas internas, como los empleados que aceptan sobornos de otras personas. Es de público conocimiento que agentes saudíes infiltraron Twitter para robar datos de usuarios de Arabia Saudita y entregarlos a los servicios de inteligencia de ese país, de modo que ambos pudieran vigilar a los activistas y tomar represalias contra ellos de las formas más violentas y horrorosas.

También existen riesgos de que todo dato que se recopila puede terminar filtrándose y caer en manos de delincuentes. Se necesita una regulación razonable para poner fin a esta conducta. La única forma de entender por qué sigue siendo predominante es que hay demasiadas partes interesadas en el Gobierno que utilizan estas bases de datos peligrosas y engañosas para facilitar su trabajo. Por lo tanto, no solo no apoyan los esfuerzos para limitar el poder de Google y otras empresas, sino que de hecho se oponen a hacerlo tanto públicamente como en forma oculta. Como observó Upton Sinclair, es muy difícil hacer entender algo a alguien cuando su salario depende de que no lo entienda.

¿Cuáles son las repercusiones de esta relación entre Estados y empresas a nivel mundial?

Cory: De mediados de la primera década del siglo XXI a comienzos de la segunda, las empresas tecnológicas comenzaron a establecer oficinas locales en países donde el Estado de derecho era muy débil.

[1] N.T.: se refiere al asalto al Capitolio de los Estados Unidos el 6 de enero de 2021.

Hubo un momento crucial cuando Google se instaló en China y luego abandonó el país, y posteriormente muchas empresas se establecieron en Rusia tras su adhesión a la Organización Mundial del Comercio (OMC). Twitter instaló una oficina en Turquía. Y todo esto fue importante porque puso a la población en peligro. Otorgó a los Gobiernos de estos países el poder de manipular a personas importantes dentro de esa estructura empresarial y, de ese modo, coaccionar a esas empresas para que cooperaran de un modo mucho más fácil que si, por ejemplo, Erdogan amenazara a empleados de Google en California. Si el ejecutivo más cercano de Google estuviera en otro continente, Google tendría un cálculo muy diferente de su participación en la vigilancia turca que cuando se detiene y envía a la cárcel a determinadas personas de interés.

Algo similar sucede con la proliferación de grandes cortafuegos, en primer lugar en China y, posteriormente, como un producto *llave en mano* (instalado y listo para operar sistemas) en otros lugares, dado que las empresas chinas y occidentales venden sus soluciones *llave en mano* a Gobiernos que carecen de capacidad técnica propia.

Ello ha hecho que algunos Gobiernos digan a las empresas que no les permitirán ingresar a menos que envíen a alguien al país y almacenen datos allí. Y mencionan normas de localización de datos de la Unión Europea (UE), según las cuales empresas estadounidenses que operan en la UE no pueden trasladar datos de europeos a los Estados Unidos, donde la NSA pueda acceder a ellos. Es absolutamente razonable que la UE haya elaborado esa regulación, pero, dependiendo de las características del Gobierno, quizá respeten la privacidad menos que la NSA o incluso sean más propensos que los Estados Unidos a utilizar los datos de sus ciudadanos como un arma. Un ejemplo de ello es el modo en que el Estado etíope ha utilizado herramientas de vigilancia masiva de llave en mano para detener, arrestar, torturar y, en algunos casos, asesinar a figuras democráticas de la oposición. Entonces, para entender cómo las autoridades etíopes tienen acceso a los datos, es preciso entender el vínculo entre la localización de datos, la tecnología nacional

de cortafuegos y el imperativo de las empresas de establecer oficinas de ventas en países de todo el mundo para maximizar sus ganancias.

¿Y qué papel desempeñan aquí la inteligencia artificial y el aprendizaje automático?

Cory: No me gusta el término inteligencia artificial. No es ni artificial ni inteligente. Tampoco me gusta el término aprendizaje automático. A la expresión *inferencia estadística* le falta algo, así que utilizaré el término aprendizaje automático, que se entiende como permitir un juicio automático a una escala que los seres humanos no podrían alcanzar. Entonces, si se quiere identificar todo lo que tiene forma de rostro en una multitud al consultar la base de datos de todos los rostros que se conocen, la capacidad de un Estado de hacerlo estaría limitada por el número de personas incluidas en la base de datos. En la ex Alemania del Este una de cada sesenta personas trabajaba de un modo u otro para los servicios de inteligencia, pero no se acercaba a la escala de vigilancia actual.

Sin embargo, ello plantea una serie de problemas importantes. El primero es que quizá funcione, y el segundo es que quizá no. Si funciona, es una capacidad de inteligencia que supera los sueños de cualquier dictador de la historia. Cuanto más fácil le resulte a un Gobierno impedir la oposición, menos atención deberá prestar a gobernar bien para impedir la formación de la oposición en primer lugar. Cuanto más barato sea construir cárceles, menos hospitales, carreteras y escuelas deberán construirse, habrá menos necesidad de gobernar bien y se podrá gobernar en el interés de los poderosos. Por lo que, cuando funciona, es perverso. Y cuando fracasa, es malo porque, por definición, está funcionando a una escala que es demasiado rápida para mantener informado a un ser humano. Si a cada segundo se generan millones de juicios que ningún ser humano sería capaz de supervisar, y si solo hay un pequeño margen de error, de alrededor del 1 %; el 1 % de un millón es 10 mil, por lo que se cometerían 10 mil errores por segundo.

Entonces, ¿ha cambiado algo desde las revelaciones de Edward Snowden?

Cory: Creo que tenemos una idea más clara de que nos están vigilando. No es polémico decir que estamos bajo vigilancia masiva y que nuestros dispositivos digitales están siendo corrompidos por el Estado. Sus revelaciones han generado un espacio para que empresas y organizaciones sin fines de lucro creen y mantengan tecnologías resistentes a la vigilancia. Se puede observar el aumento del uso de tecnologías como Signal, así como la incorporación por grandes empresas como Facebook de tecnología contra la vigilancia en WhatsApp.

Y en la industria existe una mayor consciencia de que esta vigilancia masiva es nociva porque el mecanismo básico utilizado por los organismos de vigilancia gubernamentales es identificar defectos en la programación y, en lugar de informar a los fabricantes acerca de esos defectos, los acaparan y utilizan para atacar a adversarios del organismo. Es decir que cuando la NSA descubre un error en Windows, en lugar de notificar a Microsoft, lo utiliza para *hackear* a personas que considera son terroristas o espías o simplemente contrarios a los intereses nacionales de los Estados Unidos.

Y el problema con ello es que hay una probabilidad anual de alrededor de 1 en 5 de que cualquier falla específica será redescubierto de forma independiente y que será utilizado por delincuentes o por un Gobierno hostil, lo que significa que al descubrir estas fallas y no adoptar medidas de inmediato para resolver esas lagunas, el Gobierno de los Estados Unidos expone a sus partes interesadas, empresas e individuos, a un riesgo enorme. Y ese riesgo realmente se expresa de la mejor manera en la epidemia actual de programas de secuestro (*ransomware*), en la cual oleoductos, hospitales y organismos gubernamentales y ciudades enteras están siendo tomadas como rehenes por delincuentes menores.

Ese es el tipo de retroceso que hemos experimentado en la vigilancia masiva y ha impulsado un movimiento contrario a la vigilancia que está cobrando fuerza, aunque no haya llegado tan lejos como

se esperaba, si se tiene en cuenta el sacrificio que personas como Ed Snowden han hecho.

Lo que no puede sostenerse para siempre se detendrá en algún momento. Y la vigilancia masiva es tan tóxica para nuestro discurso, tan peligrosa e irresponsable, que no puede existir por siempre. Entonces, la cuestión no es si dejará de existir, sino cuánto peligro y daño provocará antes de que eso suceda. Y acontecimientos como las revelaciones de Snowden acelerarán ese proceso.

Volvamos a las empresas que están a cargo de esta tecnología. ¿Cómo caracterizaría el problema de las grandes empresas tecnológicas? ¿Se trata de unas pocas empresas o personas que tienen demasiado poder, como Elon Musk o Mark Zuckerberg? ¿El problema es el modelo de negocios, la vigilancia masiva? ¿O lo problemático es que las grandes empresas tecnológicas funcionan dentro de una estructura mucho más amplia?

Cory: Lo primero que debemos entender sobre las grandes empresas tecnológicas es que no son muy buenas en la innovación. Tomemos el ejemplo de Google. Es una empresa que creó tres productos exitosos. Crearon un motor de búsqueda muy bueno hace treinta años, un clon bastante bueno de Hotmail y un buscador bastante espeluznante. Todo lo demás que han hecho ha fracasado. Y todos los demás logros se alcanzaron mediante la compra de otras empresas. Cuando Google Video fracasó, compraron YouTube. Su plataforma de avisos tecnológicos, su plataforma digital, sus herramientas de gestión de servidores, sus herramientas de servicio al cliente: a excepción de estas tres herramientas, todas las partes de la empresa Google las adquirieron de otra persona.

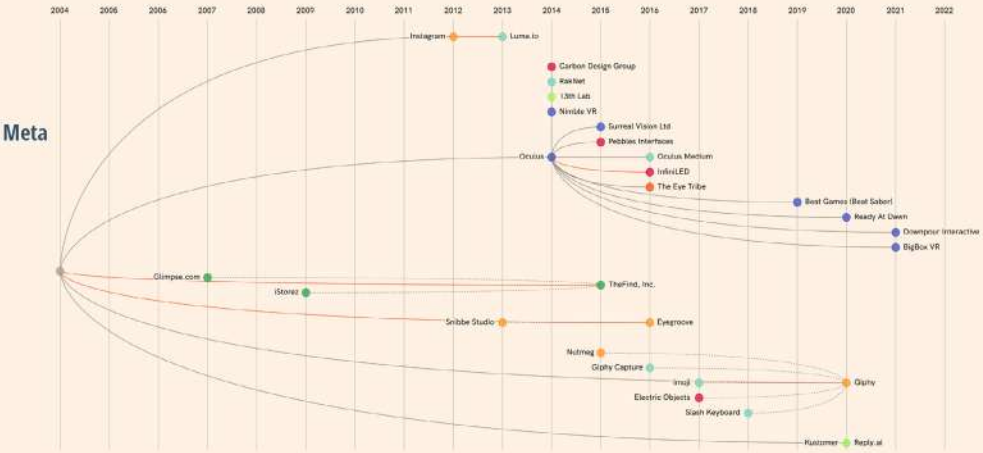
Históricamente, los reguladores antimonopolio habrían impedido estas fusiones y adquisiciones contrarias a la competencia y habrían obligado a estas empresas a buscar su propia forma de innovar o a no impedir que personas con mejores ideas las superen. El caso de Google no es excepcional. Apple, Facebook y Microsoft son fábricas de adquisición de otras empresas, aunque hacen de cuenta de que son fábricas generadoras de ideas. Hemos detenido el avance tecnológico

al permitir que empresas que tienen acceso a los mercados de capital decidan cómo será el futuro de la tecnología. Es una economía planificada, pero es planificada por los financieros y ejecutivos poderosos de unas pocas empresas, no por legisladores o un Gobierno democráticamente responsable –o un autócrata, o al menos un autócrata en el Gobierno–. Hay autócratas en los directorios de empresas estos días.

Y cuando se logra entender que la principal ventaja de estas empresas es acceder a mercados de capital y comprar y extinguir a los posi-

LAS GRANDES EMPRESAS TECNOLÓGICAS CRECIERON AL ABSORBER A PEQUEÑAS EMPRESAS TECNOLÓGICAS

Empresas adquiridas por Meta (Facebook) 2007–2022



Fuente: gafam.theglassroom.org

bles rivales antes de que puedan crecer de manera considerable, entonces se entiende dónde radica el poder. Es un error creer en el revuelo en torno a Google o Facebook, que salen a decir a posibles anunciantes que han construido una máquina para controlar mentes que podemos utilizar para vender cualquier cosa a cualquier persona si pagan una cuota. Desde la era de Rasputin, o incluso antes, muchas personas han afirmado, falsamente, haber construido una forma de controlar mentes. Las afirmaciones extraordinarias necesitan pruebas extraordinarias y las pruebas son muy escasas. En cambio, lo que vemos es que las empresas tienen un monopolio. Facebook puede llegar a 3 mil millones de personas porque las espía constantemente y porque es prácticamente imposible utilizar Internet sin utilizar Facebook. Incluso si no se es usuario de Facebook, todas las aplicaciones probablemente se hayan creado con el conjunto de herramientas de Facebook, lo que significa que siempre están recopilando nuestra información. Lo mismo ocurre con Google. No es el modelo de negocios de vigilancia lo que dio poder a estas empresas. Sino que su poder hizo que adoptaran un modelo de negocios de vigilancia que, de otro modo, habría estado prohibido en cualquier sistema regulatorio coherente, o habría sido socavado por los competidores.

Por ejemplo, muchas personas disfrutan de tener un excelente motor de búsqueda, pero muy pocos nos damos cuenta del modo en que Google nos espía. Históricamente, si una empresa cuyos productos digitales hacen tres cosas que sus clientes aprecian y una que desprecian, entonces alguien producirá un módulo posventa que nos ofrezca todo lo que deseamos y nada de lo que no deseamos. Sin embargo, cuando una empresa intenta construir algo de ese tipo, o bien es adquirida por Google, Facebook o Apple, u otra de las grandes empresas, o es demandada hasta el punto del olvido por haber incurrido en una conducta muy similar a la conducta en que estas mismas incurrieron cuando estaban creciendo. Cuando ellas lo hacen, es un proceso legítimo. Cuando lo hacemos nosotros, es robo.

Y ¿qué ocurre con quienes afirman que el problema es el modelo de negocios de vigilancia que empresas como Google están adoptando?

Cory: No creo que tenga que ver con el modelo de negocios. Existe esta idea de que si no pagas por el producto, eres el producto. Apple ha creado excelente tecnología anti vigilancia que impide que Facebook te espíe. Pero resulta que aunque escojas la opción "no espiar" en las herramientas de un dispositivo iOS, en tu iPhone o iPad, Apple igualmente espía tus actividades. Recopila de manera engañosa un conjunto prácticamente idéntico de información al que Facebook habría recopilado y lo utiliza para mostrarte anuncios. El mayor acuerdo que Apple realiza cada año, que es negociado en persona entre el principal ejecutivo de Apple, Tim Cook, y el principal ejecutivo de Google, Sundar Pichai, es el que hace que Google sea la herramienta de búsqueda por defecto en iOS, lo que significa que cada vez que utilizas tu iPhone, Google te está espiando.

Entonces, la idea de que hay empresas buenas y malas o de que el modelo de negocios de vigilancia convierte a nerds buenos y honestos en villanos malvados no tiene asidero. Las empresas te tratarán del modo en que pueden tratarte de manera impune. Y si pueden hallar la forma de hacer dinero al tratarte como un producto, lo harán. Si crees que darles dinero hará que se detengan, eres un tonto.

Cory, tu respuesta es la primera que de algún modo es alentadora cuando entendemos el poder digital de las grandes empresas tecnológicas como un poder basado en mediocres que logran obtener un monopolio. Entonces, básicamente, si podemos romper su monopolio, ¿quizá podremos reivindicar el poder?

Cory: Sí, creo que así es. El problema con la teoría del poder de controlar la mente que se esboza en libros como *La era del capitalismo de la vigilancia*, de Shoshana Zuboff, es que es consuelo de pobres. Hay una sección que dice: ¿qué ocurre con la ley de la competencia? ¿qué sucedería si dividiéramos a esas empresas y las hiciéramos menos

poderosas? La autora sostiene que eso no las volvería menos poderosas porque si haces que vuelvan a ser pequeñas, ahora tienen la máquina de controlar mentes. Y en lugar de que haya un solo super villano malvado a cargo de una máquina para controlar mentes, habrá cientos de supervillanos malvados, que es como tener dispositivos nucleares de maleta en manos de terroristas tontos, en lugar de la teoría súper racional de los juegos que actualmente juegan las superpotencias.

Eso sería cierto si, de hecho, hubieran fabricado armas superpoderosas. Pero no es así. Ni siquiera hacen bien su trabajo. Fabrican sus productos cada vez peor y cometen muchos errores terribles. Y, al igual que muchas personas poderosas, pueden cometer todo tipo de errores, y porque tienen un gran colchón –como el poder del mercado, las reservas de capital, el acceso a los mercados de capital, los aliados poderosos y los organismos gubernamentales y otras empresas que dependen de ellas para infraestructura y apoyo– pueden cometer todo tipo de errores y seguir como si nada. Elon Musk es el ejemplo más claro del fracaso. Un hombre que está tan aislado por su riqueza, su suerte y su privilegio que no importa cuántas veces se equivoque, siempre cae parado.

Entonces, ¿en qué se equivocó la izquierda? Ambos llegamos a la adultez en la década del noventa, cuando había la sensación de que Internet era una herramienta emancipadora y que las fuerzas progresistas de izquierda estaban a la vanguardia en ese sentido, ya fuera al cuestionar las estructuras de la Organización Mundial del Comercio o al derrocar Gobiernos antidemocráticos. Pero ahora vivimos en una época en que las grandes empresas tienen un cuello de botella de control, donde el discurso de Internet está plagado de desinformación y es la extrema derecha la que al parecer utiliza las tecnologías digitales de manera más exitosa. Entonces, ¿cuál crees que haya sido la causa de que esto sucediera y qué lecciones se pueden extraer?

Cory: La falla no consistió en ver el potencial liberador de la tecnología o no haber visto su potencial para coartar la libertad y el poder, sino, más bien, no haber entendido lo que había sucedido con la ley

de competencia, no solo en la tecnología, sino en todas las esferas de la legislación, que comenzó con Ronald Reagan y se aceleró durante la era tecnológica. Recuerden que Reagan fue electo el año en que la computadora Apple II Plus salió al mercado. Entonces, la economía neoliberal y el sector tecnológico no pueden disociarse. Están profundamente interconectados. No hemos logrado entender que algo fundamentalmente diferente estaba sucediendo en el modo en que permitíamos a las empresas realizar sus actividades, al permitirles adquirir cualquier competidor que se les interponía y al permitir a los mercados de capital financiar esas adquisiciones para crear estos monopolios, que cambiarían el equilibrio de fuerzas.

Mi experiencia personal es que me compré una Apple II Plus en 1979, de la que me enamoré y me convertí en un niño obsesionado con la tecnología. Al mismo tiempo, las empresas que en un momento habían sido gigantes estaban colapsando y nuevas empresas más interesantes pasaron a reemplazarlas. Era fácil pensar que esa era una característica intrínseca de la tecnología. En retrospectiva, esos fueron los últimos días del mercado competitivo para la tecnología. La Apple II Plus y las computadoras personales fueron posibles gracias a las leyes contra el monopolio en la industria de los semiconductores en la década del setenta. El módem fue posible debido a la división de AT&T en 1982.

Como consecuencia de ello, ahora vivimos en un mundo en que ya no existe ese dinamismo. Vivimos en un mundo fosilizado. Una época en que la tecnología, el entretenimiento y otros sectores se han fusionado no solo entre sí, sino también con las fuerzas armadas y el Estado, de modo que tenemos una masa de poder empresarial cada vez más concentrado que se entremezcla con el poder estatal en una forma que es difícil de desvincular.

Entonces, ¿diría que no hay marcha atrás? Parece que se han adoptado algunas medidas para regular el sector en los últimos años, como el Reglamento General de Protección de Datos en Europa o la Ley de Mercados Digitales. Hay algunas discusiones antimonopolio en los Estados Unidos y en general

las personas ahora son conscientes de esta problemática. ¿Qué piensa de estas iniciativas legislativas y de la concienciación del público en general?

Cory: Vivimos un momento extraordinario, un momento de reglamentación de las grandes empresas tecnológicas y otro tipo de poder empresarial que hacía falta hace tiempo y que ha tardado mucho en llegar. Creo que hay una idea cada vez más predominante de que las grandes empresas tecnológicas no son un fenómeno aislado, sino que son tan solo una expresión del fenómeno subyacente de poder empresarial cada vez más concentrado en todos los sectores. Entonces, cuando decimos que queremos controlar a las empresas tecnológicas, estamos participando en un movimiento que dice también que queremos que se controle a las grandes empresas agrícolas y las grandes empresas petroleras, financieras y de logística, y todos los demás grandes sectores integrados, concentrados que brindan un servicio cada vez peor obtienen cada vez más ganancias, infligen cada vez más daño y afrontan cada vez menos consecuencias.

Además, el modo en que la tecnología digital es profundamente diferente y verdaderamente excepcional respecto de otros tipos de tecnología, lo que significa que la tecnología digital es universal, puede ser esperanzador. Solo hay un tipo de computadora que sabemos fabricar. Es la máquina de von Neumann del sistema Turing completo. Formalmente, es una computadora en la que funciona cualquier programa que desarrollemos, por lo que si hay una computadora diseñada para vigilarnos, también hay un programa que puede funcionar en esa computadora que impedirá la vigilancia. Es muy diferente de otros tipos de tecnología, porque estos programas pueden reproducirse al infinito simplemente al hacer clic en un ratón e instalarse en todo el mundo. Ahora, ello significa, por un lado, que organizaciones delictivas pueden explotar tecnologías de modos terribles. No existe algo como una computadora hospital que pueda solamente hacer funcionar la máquina de rayos X, sin además hacer funcionar el programa de secuestro. Pero significa que lo que solíamos llamar *hacktivismo* y lo que cada vez más se está llamando simplemente buenas políticas

industriales, como se pueden ver en la Ley de Mercados Digitales de la Unión Europea, puede inclinar la balanza de modo que la estructura de estas grandes empresas y los Estados que las apoyan sean sobornados para apoyar a quienes se oponen a ellas.

*Entonces, ¿cómo crees que podemos aprovechar este momento al máximo? ¿*cómo podemos *contribuir a que sea un punto de inflexión?*

Cory: Quizá hablar de punto de inflexión no sea la mejor forma de analizarlo. En estadística existe la curva de crecimiento *punteada* (*scalloped*). Probablemente la hayan visto. Es una curva que asciende, llega a un pico, luego desciende a un nivel superior al inicial y luego vuelve a ascender a un nuevo pico, y de allí a un nivel más elevado que antes. De modo que es como un crecimiento punteado.

Y el modo de entenderlo en términos de las sospechas del poder empresarial es que los abusos de las empresas –que ocurren inevitablemente como consecuencia del poder concentrado– crearán progresivamente su propia oposición. Por ejemplo, el mes pasado, la aerolínea Southwest dejó a un millón de pasajeros varados en la semana de Navidad. La empresa recibió 85 mil millones de dólares como parte del rescate a las aerolíneas y ha declarado un dividendo de 460 millones de dólares para sus accionistas. El Secretario de Transporte, que está a cargo de su regulación, Pete Buttigieg, no hizo nada, aunque tiene amplios poderes para intervenir. Y ello dio lugar a que muchas personas fueran partidarias de adoptar medidas para regular el poder de las empresas. Ahora, esas personas tienen otras cosas que hacer. Algunas abandonarán la lucha, pero otras, impulsadas por su enojo, serán parte de un movimiento para controlar el poder empresarial. Y debido a que estas empresas están tan poco reguladas, vaciadas, y ejercen poder de un modo tan provinciano y venal, en algún momento generarán más crisis y aún más personas se sumarán al movimiento.

Entonces, no creo que habrá un punto de inflexión, sino más bien una especie de acumulación lenta e inexorable de la voluntad popular. Y creo que nuestro desafío es lograr que las personas dirijan sus

críticas al lugar correcto, que entiendan que la causa es el poder empresarial desenfrenado y los funcionarios que lo permiten, que no se trata del mal de la tecnología o de una, muy improbable, máquina para controlar mentes. O, creo que va de suyo: no son los inmigrantes, no es George Soros, no son las personas *queer*. Es el poder empresarial descontrolado.

Me ha gustado mucho tu libro, Chokepoint Capitalism, y supongo que gran parte de nuestra conversación se ha centrado en nosotros como consumidores y activistas. Pero no hemos hablado mucho de los trabajadores. En tu libro hay anécdotas interesantes sobre cómo activistas y trabajadores se enfrentaron al poder empresarial y lograron revertirlo. ¿Puedes compartir una de las historias inspiradoras de las que deberíamos extraer lecciones?

Cory: Sí, claro. Mi preferida es la historia de los conductores de Uber, que utilizamos como una anécdota ejemplar en el libro. Aquí, en California, Uber ha robado abiertamente el salario de los conductores. No se trata del robo habitual del salario que es consecuencia de no categorizar correctamente a los trabajadores, sino una forma diferente de robo de salario, en la cual la empresa se estaba quedando con dinero que adeudaba a los conductores. En California, los conductores de Uber debieron firmar un acuerdo de arbitraje vinculante para poder conducir para la empresa, según el cual todas las disputas las resolvería un árbitro, caso por caso.

Un árbitro es un juez de mentira que trabaja para una empresa empleada por la compañía que infligió el daño y que, como no es de extrañar, rara vez falla en contra de la empresa que paga sus honorarios. Pero, aunque lo haga, eso no importa porque en general el acuerdo es confidencial y no sienta un precedente, lo que significa que la siguiente persona no puede utilizar el mismo argumento para obtener un resultado similar. Cabe destacar que un acuerdo de arbitraje vinculante prohíbe entablar una demanda colectiva, lo que significa que todos los conductores de Uber deben contratar individualmente a un abogado para que los represente, lo cual no sería económicamente

razonable o viable. Todo ello ha implicado que Uber robara todo ese dinero impunemente.

De modo que los conductores de Uber trabajaron con un bufete de abogados inteligente y hallaron el modo de automatizar los reclamos de arbitraje. Contratar a un árbitro, que Uber debe pagar por ser la entidad que impone el arbitraje, cuesta unos miles de dólares. Entonces, si un millón de personas recurren a arbitraje, rechazar sus reclamos costaría más que hacer lo correcto y pagarles. Por lo que, ante la posibilidad de tener que pagar cientos de millones de dólares en honorarios de arbitraje, Uber llegó a un acuerdo con los conductores y les dio 150 millones de dólares en efectivo, lo cual es maravilloso.

Es genial. Es una señal de que de algún modo es posible que haya un cambio. Y, a propósito de ello, ¿crees que se puede reconfigurar el poder digital, definido ampliamente como lo describiste al comienzo en el interés público, y utilizarlo para hacer frente a las grandes crisis, como la catástrofe ambiental?

Cory: Creo que la tecnología que responde a las necesidades de los usuarios, la tecnología diseñada para maximizar la autodeterminación tecnológica, es fundamental para todo futuro en el que abordamos nuestras principales crisis. La tecnología digital baja los costos de transacción, es decir, los costos que debes soportar cuando intentas hacer cosas con otra persona. Esa es la mejor forma de entender su poder transformador.

Cuando era chico, por ejemplo, si quería ir al cine con mis amigos un viernes por la noche o bien teníamos que planificarlo de antemano o teníamos que llamar a cada uno desde teléfonos públicos y dejar un mensaje, y esperar que de algún modo lo recibieran. Hoy en día basta con enviar un mensaje de texto grupal y preguntar: ¿quieren ver una película? Es un ejemplo simple y claro de cómo bajamos los costos de transacción.

Internet reduce significativamente los costos de transacción. Nos permite hacer cosas como crear enciclopedias y sistemas operativos y otros proyectos ambiciosos de manera fácil e improvisada. Bajar los

costos de transacción es realmente importante para fomentar el cambio social porque, por definición, los actores poderosos han descifrado los costos de transacción. Si eres un dictador o una gran empresa, tu función es resolver cómo coordinar que muchas personas hagan lo mismo al mismo tiempo. Allí es donde está la fuente del poder, en coordinar que muchas personas actúen al unísono para amplificar tu voluntad en el mundo.

Entonces, mientras que para la policía el costo de determinar quién está en una manifestación es más bajo que nunca, el costo de organizar una manifestación también es más bajo que nunca. Pasé gran parte de mi infancia andando en bicicleta en el centro de Toronto, pegando afiches en postes de teléfono, intentando movilizar a personas para que participaran en manifestaciones en contra de la proliferación nuclear, contra el *apartheid*, a favor del aborto, etcétera. Entonces, aunque mucha gente se burla de la cultura de Internet, tiene una riqueza que, apenas unos decenios atrás, jamás habríamos imaginado ni en nuestros sueños más descabellados.

Entonces, nuestro proyecto no debe ser poner fin a la tecnología, sino ver la forma de aprovechar los medios de la informática, de construir un sustrato tecnológico que responda a las necesidades de las personas, que nos permita construir el mundo que queremos, en particular un mundo con menos carbono, menos injusticia, más derechos laborales, etcétera.

Este es un ejemplo de cómo podemos lograrlo para abordar la crisis ambiental. A menudo se nos pide que elijamos entre el decrecimiento y la abundancia material, entonces se nos dice que el decrecimiento significa hacer menos con menos. Pero, de algún modo, tener más coordinación nos permitiría hacer mucho más con menos. Vivo en una casa en los suburbios de Los Ángeles, por ejemplo, y tengo un taladro barato porque solo necesito hacer un agujero en la pared seis veces al año. Mis vecinos también tienen taladros de mala calidad por la misma razón. Pero hay muy buenos taladros. Si viviéramos en un mundo en que no nos tuviéramos que preocupar por la vigilancia porque nuestros Estados nos rendirían cuentas, y no nos preocupara

el poder coercitivo, entonces tendríamos taladros estadísticamente distribuidos en los barrios y los taladros te dirían donde están. Ese es el mundo en que tienes un mejor taladro, siempre hay un taladro disponible al alcance de tu mano, pero lo que pagas por el material, la energía y la mano de obra disminuye por orden de magnitud. Solo hace falta coordinación y rendición de cuentas respecto de la tecnología que utilizamos.

Ya no hay mercados

Del neoliberalismo a las grandes empresas tecnológicas

Kean Birch

Traducción al español por Mercedes Camps
Ilustración de Zoran Svilar

El poder de las grandes empresas tecnológicas no solo se debe a su tamaño, sino al hecho de que recopilan, controlan y monetizan la información que necesitamos para que los mercados funcionen. Se han convertido en mercados en sí mismos. Para controlarlas será necesario realizar un análisis que trascienda la regulación.

En sus inicios, el lema original de Google era "No seas malvado". Hoy en día, la empresa no es capaz de honrar este noble principio, como lo ha demostrado ampliamente un juicio pendiente en su contra. El documento más reciente relacionado con el litigio afirma que "intenta asegurar que Google deje de ser malvado". Aunque esta demanda no es muy conocida, nos da una idea no solo de cómo actúa Google, sino también de la estructura que las grandes empresas tecnológicas han construido en los últimos diez años y que progresivamente ha asumido el control de las economías y socavado los mercados.

El juicio contra Google fue entablado por el estado de Texas, junto con otros dieciséis estados de los Estados Unidos. Se trata de una demanda antimonopolio titulada *In re: Litigio contra el monopolio de Google respecto de la publicidad digital* , que fue anunciada en 2020 por el Fiscal General de Texas, y cuya versión más reciente fue publicada en enero de 2022.[1] El juicio tiene lugar al mismo tiempo que la demanda antimonopolio que el Departamento de Justicia entabló contra Google a finales de 2020.[2]

[1] Texas Attorney General et al. (2022). Google Digital Advertising Antitrust Litigation. https://www.nysd.uscourts.gov/sites/default/files/2022-09/In%20re%20Gogle%20Digital%20Advertising%20Antitrust%20Lirtigation.pdf

[2] Departamento de Justicia de los Estados Unidos (2020). Justice Department Sues Monopolist Google For Violating Antitrust Laws, Washington DC: Departamento de Justicia. https://www.justice.gov/opa/pr/justice-department-sues-monopolist-googleviolating-antitrust-laws

El argumento principal de la demanda sobre la publicidad digital de Google radica en el monopolio de la empresa respecto de las tecnologías y la información de mercado en las que se basa la publicidad programática en línea, incluido el uso de nuestros datos personales para intentar vendernos productos.[3] La publicidad programática es un enorme y complejo sistema dominado por Google, ya que es a la vez comprador y vendedor del espacio publicitario en Internet. De modo similar, Facebook (ahora Meta) desempeña un papel central en este mercado de publicidad en línea.

A continuación, ofrecemos una breve descripción del modo en que funciona la publicidad programática y cómo se ha explotado este mercado.

Imagina que eres un anunciante y quieres vender un libro –aunque podría ser cualquier otro producto o servicio–, por lo que probablemente quieras llegar a las personas que realmente lo comprarán. Google ofrece conectarte con el espacio publicitario en Internet más adecuado para ese fin mediante su *intercambio de anuncios*. Lo hace mediante la recopilación y acumulación de tus datos personales a partir de tus búsquedas, correos electrónicos, teléfonos inteligentes, terceros que utilizan sus aplicaciones analíticas, etcétera. No somos conscientes de la medida en que entregamos nuestros datos personales. Es parte de la letra chica que figura en los términos y condiciones que la mayoría de las personas simplemente firmamos para utilizar productos y servicios digitales.

Mediante el uso de nuestros datos personales, Google puede realizar inferencias acerca de nuestras preferencias personales –por ejemplo, me gusta la ciencia ficción– y decisiones –probablemente haré clic en un anuncio en línea. Con esta información, Google automatiza la compra y venta de espacio publicitario en los microsegundos que

[3] Dentro de la publicidad en línea se puede diferenciar entre la publicidad programática y la contextual. La primera representa la publicidad dirigida a personas sobre la base de sus intereses y preferencias, que se infieren de sus datos personales, mientras que la segunda representa la publicidad que figura en los sitios web que corresponden a los contenidos del anuncio. Para más información, véase Hwang (2020).

transcurren entre que abrimos una página web y vemos un anuncio. Google vende espacio publicitario en Internet a anunciantes para que todos los usuarios de una página puedan ver tu anuncio. Un tercero, como un periódico, por ejemplo, vende espacio publicitario en su sitio web a Google. Es decir, que Google compra y vende espacio publicitario, además de mediar entre compradores y vendedores a través de una subasta que controla y de la que obtiene un porcentaje.

PROGRAMA BERNANKE DE GOOGLE

Como consecuencia del Programa Bernanke Adx disminuyó la segunda oferta de la subasta y se redujeron las ganancias de los publicadores de anuncios. Google se quedó con la diferencia, que utiliza para inflar otras ofertas.

Fuente: Texas Attorney General, 2022, p.107

El juicio de Texas realiza dos denuncias fundamentales.

- En primer lugar, que Google y Facebook han conspirado para tener el monopolio del mercado de publicidad en Internet, excluyendo a los competidores del mercado; este acuerdo fue denominado *Jedi Blue*.
- En segundo lugar, que Google inició un programa secreto en 2013 denominado *Proyecto Bernanke*, que supuestamente estaba diseñado para engañar a los anunciantes y los publicadores de sitios web.

El proyecto Bernanke gira en torno al diseño de Google del sistema de subasta utilizado para vender y comprar espacio publicitario.

Las subastas pueden diseñarse de diferentes maneras. Por ejemplo, las subastas que utilizan *ofertas en pliegos cerrados* suelen presentarse como una función clave de la competencia del mercado debido a que permiten a actores del mercado revelar sus verdaderas preferencias sin temor a ser explotados o a que otros actores del mercado utilicen el sistema en beneficio propio. Ello se debe a que nadie puede ver la otras ofertas hasta que estas se hayan revelado al final del proceso de subasta. Por lo tanto, nadie puede cambiar su oferta en función de la oferta de otros postores. Las subastas con ofertas en pliegos cerrados deberían, entonces, ser el mecanismo más eficiente para determinar los precios *ideales* en una economía de mercado.

Los economistas han intentado teorizar durante mucho tiempo acerca del cuál sería el diseño óptimo de una subasta. William Vickery ganó el Premio Nobel por su labor sobre los beneficios de las subastas de la segunda mejor oferta, ahora denominadas subastas *Vickery*. La subasta de segunda mejor oferta se establece para asegurar que gane el mejor postor, pero que este pague el precio ofrecido por la segunda mejor oferta, por lo que se incentiva a los oferentes a revelar sus verdaderas preferencias (es decir que no tendrán problema en ofrecer un precio demasiado elevado). También hay subastas de tercer mejor postor, en las cuales el mejor oferente pagará el valor ofrecido por el tercer mejor postor (Mirowski y Nik-Khah, 2017).

Google y el Proyecto Bernanke. Según el juicio entablado en Texas, Google diseñó su intercambio de anuncios publicitarios como subastas de segundo mejor postor e informó a todas las partes al respecto. Sin embargo, de acuerdo con la demanda, Google "cambió de manera subrepticia el intercambio de anuncios Google Adx de una subasta de segundo mejor postor a una subasta de tercer mejor postor en miles de millones de impresiones al mes" (Texas Attorney General et al., 2022, p. 104).

Aunque puede parecer complicado, no lo es. Básicamente, Google dijo a los anunciantes que pagarían la segunda mejor oferta y dijo a los

sitios web que publicarían los anuncios que recibieran el precio de la segunda mejor oferta. Se alega que, en realidad, el Proyecto Bernanke cambió el sistema para que los publicadores de anuncios recibieran el precio de la tercera mejor oferta, mientras que Google se quedó con la diferencia. Según los alegatos, ello significó que los publicadores de anuncios perdieron alrededor de un 40 % de sus ganancias sin saberlo. A continuación, Google utilizó los ingresos adicionales para "inflar las ofertas de los anunciantes mediante Google Ads para ayudarlos a ganar impresiones que de otro modo habrían perdido frente a otros anunciantes que realizaron ofertas a través de herramientas de compra distintas de la de Google" (Texas Attorney General et al., 2022, p. 107).

Como observó un analista, Google básicamente cobró más dinero a los anunciantes y pagó menos dinero a los publicadores al controlar las tecnologías y la arquitectura de los precios del mercado. Google diseñó el mercado para beneficiarse y eliminar a la competencia.

Los mercados y la cola larga del neoliberalismo

El mensaje es que el control de las plataformas digitales permite a las grandes empresas tecnológicas como Google diseñar mercados en formas que mejor les convienen. La falta de transparencia en estas plataformas implica que los mercados pueden alejarse considerablemente de los supuestos de pensadores y responsables de políticas favorables al mercado, que han dominado el modo en que entendemos las economías y sociedades desde la década del setenta.

A menudo definidos como *neoliberalismo*, los supuestos en que se basa esta visión del mundo pueden describirse como un proyecto político-económico y moral para rediseñar sociedades a fin de colocar a los mercados en el centro de la adopción de decisiones de Gobiernos, organizaciones o personas (Birch, 2017). Evocando la obra de pensadores como Friedrich Hayek, –el famoso economista peripatético de Austria– el neoliberalismo se basa en la premisa de que ningún organismo (por ejemplo, el Gobierno) puede coordinar la economía o

la sociedad debido a que carece de capacidad cognitiva para procesar toda la información que producimos y utilizamos individualmente para tomar decisiones a diario. Para Hayek y otros neoliberales, los mercados son los mejores procesadores de información para coordinar nuestras sociedades de manera eficiente. Como explica Hayek:

"La razón de esta insuficiencia estriba en que los 'datos' de los que parte el cálculo económico no están, y nunca pueden estar, 'dados' para una mente individual que pueda establecer las implicaciones para el conjunto de la sociedad" (Hayek, 1945).

Por lo tanto, los mercados son la mejor forma de coordinar la sociedad, ya que nos pueden brindar información para adoptar las decisiones *correctas*. Lo hacen a través del mecanismo de precios, en que los precios representan información sobre qué debemos producir y cuándo, cuándo hemos de cambiar nuestras preferencias y cómo hemos de gestionar nuestros recursos colectivos de la mejor manera. En este marco, los mercados son tanto un mecanismo fáctico como moral; nos dicen cómo tomar decisiones y cuáles son las mejores decisiones que debemos adoptar.

En esta narrativa neoliberal, la información se vuelve un elemento fundamental del funcionamiento de los mercados. Las personas no pueden revelar sus preferencias ni adoptar decisiones sin información. Desde Hayek, el problema de la información atraviesa gran parte del pensamiento económico ortodoxo.[4] Sin embargo, es precisamente en el pensamiento neoliberal sobre la información que sus hipótesis sobre los mercados comienzan a fallar. Ello se debe a que, al menos en las esferas legal y de políticas, el pensamiento neoliberal pasó progresivamente del punto de vista de Hayek, de que las sociedades evolucionan gradualmente hacia los mercados y el pensamiento de los mercados, a una perspectiva en que se supone que las sociedades simplemente funcionan como mercados y todas las personas se comportan como si

[4] Véase el libro de Mirowski y Nik-Khah sobre la historia de la *información* en la economía ortodoxa.

fueran actores del mercado que responden a incentivos, definidos por precios, que representan información.

S.M. Amadae plantea esto de manera excelente en su libro *Prisoners of Reason* (2016). Su argumento básico es que el objetivo del pensamiento y la elaboración de políticas neoliberales es que una vez que hemos descifrado lo que los mercados deberían hacer, ya no es necesario dejar que los mercados surjan espontáneamente, como planteaba Hayek. Sino que es posible diseñar mercados para que hagan lo necesario a fin de lograr el resultado deseado en materia de políticas.

Y eso es exactamente lo que sucedió. Las diversas ideas acerca del diseño del mercado o mecanismo, como las subastas del segundo mejor postor, se vincularon con suposiciones acerca de cuáles deberían ser nuestros objetivos individuales y colectivos a fin de que los responsables de la elaboración de políticas puedan diseñar mercados con ese fin. Entonces, cuando los Gobiernos intentan privatizar activos públicos, desregular el suministro de electricidad o licitar los servicios de radio o telefonía celular, utilizan el diseño de mecanismos (McMillan, 2003). Los resultados son variados, a veces generan grandes ingresos gubernamentales (por ejemplo, la licencia G3 en el Reino Unido), pero otras veces generan problemas considerables (como la desregulación de la electricidad en California).

Este tipo de diseño de mercado o mecanismo tiene una historia relativamente breve. Se remonta a la labor de economistas como Vickery en la década del sesenta, pero fue recién en la década del ochenta que realmente se volvió exitoso y se convirtió en un elemento fundamental de la elaboración de políticas (Birch, 2020). Las subastas del segundo y tercer mejor postor, explicadas anteriormente, son un ejemplo de cómo diseñar mercados. Dichas subastas se basan en la suposición de que somos seres racionales que actuamos en interés propio, lo cual generará beneficios sociales colectivos. Por ejemplo, las subastas de telefonía celular deberían generar los máximos ingresos posibles para el Gobierno, sin desalentar la innovación.

Entonces, la clave es crear mecanismos de mercado mediante los cuales revelemos nuestras preferencias a través del diseño de

arquitecturas de la elección, como subastas, que aseguren que siempre seamos fieles a nuestros deseos en la adopción de decisiones. Muchas concepciones contemporáneas de los mercados –y no solo la versión neoliberal– están fundadas en esta idea de que los mercados revelan información sobre la base de la cual todos podemos actuar en cuanto individuos sin la (supuesta) interferencia distorsionadora de un planificador central (por ejemplo, un Gobierno). Sin embargo, el diseño de los mercados contradice esta teoría. Los diseñadores de mercados pueden crear los mercados que deseen para alcanzar los resultados que deseen; las preferencias y decisiones individuales quedan relegadas, ya que los diseñadores de mercados pueden construir la arquitectura de mercado que necesitan para incentivarnos a hacer lo que *ellos* quieren (por ejemplo, aumentar los ingresos, el bienestar o la eficiencia).

Mientras que los críticos, entre los que me incluyo, debatían si el neoliberalismo estaba muerto, estaba muriendo o había resurgido tras la crisis financiera mundial de 2008, las grandes empresas tecnológicas simplemente se sumaron a la ola del dinero fácil desatada por los bancos centrales mediante la expansión cuantitativa para asentarse como los actores dominantes de nuestras economías.

El ascenso de las grandes empresas tecnológicas

Hasta hace relativamente poco tiempo, no era posible ampliar el diseño del mercado más allá de un objetivo o resultado específico. Sin embargo, todo ello ha cambiado con el auge de las grandes empresas tecnológicas como Apple, Amazon, Alphabet/Google, Microsoft y Meta/Facebook (Birch y Bronson, 2022).[5] Estas empresas han transfor-

[5] Birch, Kean y Bronson, Kelly (2022). Introduction: Big Tech. *Science as Culture* 31(1), 1-14. Hay varios libros sobre el auge de las grandes empresas tecnológicas que vale la pena leer (y muchos que no). Sugiero leer a Cohen (2019), Doctorow (2020), Foroohar (2019), Lanier (2014), Pasquale (2015), Srnicek (2016) y Zuboff (2019). Existen, por supuesto, muchos otros libros, artículos, etc. que vale la pena leer, pero simplemente no tengo espacio de incluirlos en esta nota al pie.

mado el modo en que funcionan nuestras economías y sociedades, y cada vez tienen más problemas de funcionamiento –como temores sobre la desinformación, impactos cognitivos, patrones oscuros, etcétera. Volveré sobre este punto más adelante.

En la actualidad, podemos decir con certeza que las grandes empresas tecnológicas son las intermediarias clave en nuestra vida cotidiana y de la información de la que dependemos: nos conectan con otras personas, hacen que funcione la infraestructura que utilizamos para trabajar o en nuestro tiempo libre, nos brindan productos y servicios útiles y mucho más. En gran parte de esta mediación se utilizan plataformas digitales, como las que nos conectan con otras personas (como Uber), con contenido (como YouTube) o con anuncios (como Facebook/Meta). Obviamente, no lo hacen por amabilidad, sino que, a cambio de sus servicios obtienen nuestros datos personales, comerciales y de usuario, y esos datos a su vez se convierten en otros productos, servicios e infraestructuras.

Estas empresas han diseñado y reconfigurado sus tecnologías cada vez más, como plataformas digitales o interfaces de programación de aplicaciones, con el objetivo específico de recopilar nuestros datos, ya que su éxito depende de sus enclaves de datos.[6] Estos enclaves representan el acervo de datos creado mediante la ampliación de la influencia de las grandes empresas tecnológicas a través de su ecosistema de dispositivos, aplicaciones, programas informáticos y plataformas.

[6] Utilizo el término *enclaves* en lugar de *recinto* para reflejar el hecho de que los datos personales digitales deben fabricarse y no existen en estado bruto para que alguien los recopile y utilice. De modo que su recopilación define el uso en modos que dan lugar a resultados problemáticos, como he discutido en un artículo periodístico de libre acceso que escribí junto a dos colegas (Birch et al., 2021).

CAPITALIZACIÓN DE MERCADO DE LAS GRANDES EMPRESAS TECNOLÓGICAS

Estados Unidos, S&P 500

Fuente: https://journals.sagepub.com/doi/full/10.1177/20539517211017308

Es preciso entender el tamaño monumental de las grandes empresas tecnológicas para tener una idea clara del modo en que su existencia hace una enorme diferencia en nuestras vidas, en comparación con otras empresas. Hasta hace poco, las grandes empresas tecnológicas formaban parte de las cinco mayores empresas del mundo con una capitalización de mercado superior a los 5 billones de dólares en 2020, lo cual representa casi el 25% del mercado de capitalización de mercado de valores de los Estados Unidos. Desde entonces, su valor en

el mercado ha disminuido, pero no porque se hayan vuelto menos importantes para nuestras vidas. Según un informe de 2020, que es el resultado de una investigación del Congreso de los Estados Unidos, el 81 % de todas las búsquedas generales y el 94 % de todas las búsquedas en teléfonos celulares utilizan Google; el 99 % de los teléfonos inteligentes utilizan los sistemas operativos Android o Apple; el 80 % de los buscadores son Google Chrome o Safari de Apple; Facebook, Instagram, Messenger y WhatsApp, tomados en conjunto, tienen 2.470 millones de usuarios activos a diario; alrededor del 50 % de todo el comercio digital de los Estados Unidos tiene lugar a través de Amazon; y Amazon, Microsoft y Google dominan la infraestructura de computación en la nube.[7] Las grandes empresas tecnológicas son tan omnipresentes que resulta difícil vivir sin ellas.

Mientras que los críticos, entre los que me incluyo, debatían si el neoliberalismo estaba muerto, estaba muriendo o había resurgido tras la crisis financiera mundial de 2008, las grandes empresas tecnológicas simplemente se sumaron a la ola del dinero fácil desatada por los bancos centrales mediante la expansión cuantitativa para asentarse como los actores dominantes de nuestras economías. Este es especialmente el caso de los Estados Unidos, donde la Reserva Federal imprimió más dinero entre 2008 y 2010 que en los noventa y cinco años anteriores. El periodista Christopher Leonard señala las consecuencias negativas e imprevistas de esta política en *The Lords of Easy Money* (2022). Según señala, este flujo de dinero fácil dio lugar a un sistema de bajas tasas de interés durante diez años, –que solo se estancó con el reciente aumento de la inflación– en que los bancos centrales habían tenido la esperanza de aprovechar el dinero barato para invertir en nuevos activos y empleos. Pocos lo hicieron y prefirieron en cambio utilizar ese dinero para la recompra de acciones o para invertir en burbujas de activos, incluida la industria tecnológica en auge, que experimentó un crecimiento espectacular en la financiación de capital de riesgo.

[7] Cámara de Representantes de los Estados Unidos (2020). In*vestigation of Competition in Digital Markets*. Washington, DC: House of Representatives.

En cambio, las grandes empresas tecnológicas hicieron un buen uso de ese dinero, especialmente al aumentar su oferta de activos tangibles, como los centros de datos, cables de alta velocidad y similares, lo que les permitió ampliar sus actividades de recopilación de datos y la capacidad informática necesaria para convertir a esos datos en valor y consolidar su poder en el mercado (Birch, Cochrane y Ward, 2021; Morozov, 2022). Amazon, Google y Facebook (Meta), en particular, aumentaron considerablemente la cuota de activos tangibles en sus balances.

Pero la peor parte ocurrió con la digitalización del diseño de mercado instituido por el ascenso de las grandes empresas tecnológicas y sus ecosistemas de plataformas. Como señalan Salomé Viljoen, Jake Goldenfein y Lee McGuigan, el diseño de mercado ha estado cargado de tecnologías algorítmicas propiciadas por la recolección masiva de datos personales y la enorme capacidad informática de las grandes empresas tecnológicas.[8] Los autores se refieren al modo en que el "diseño del mecanismo algorítmico o automático" otorga a las grandes empresas tecnológicas una capacidad especial sin precedentes para establecer perfiles de usuarios, clientes, proveedores y otros.

En lugar de preocuparse sobre los resultados de políticas, las grandes empresas tecnológicas han aplicado el diseño de mecanismos para hacer dinero, como lo ilustra mi ejemplo inicial, en sus diversas

[8] Viljoen, Salomé, Goldenfein, Jake y McGuigan, Lee (2021). Design choices: Mechanism design and platform capitalis. *Big Data & Society,* 8(2), 1-13. Las tecnologías algorítmicas se refieren a una serie de desarrollos a menudo referidos como *inteligencia artificial* o *aprendizaje automático*. En lugar de debatir en qué medida estas tecnologías representan una *inteligencia* real (personalmente no creo que lo hagan), prefiero referirme a ellas en términos de cómo funcionan, es decir, fundamentalmente como algoritmos (toman insumos y expulsan productos basadosen alguna operación interna, que puede ser transparente u opaca). Me gusta especialmente la opinión de Meredith Whittaker (2021) sobre estas tecnologías, ya que las desmitifica: "debemos reconocer, en primer lugar, que los 'avances' en inteligencia artificial celebrados en los últimos 10 años no se debieron a acontecimientos científicos fundamentales en técnicas de inteligencia artificial. Sino que fueron y son principalmente el producto de datos y recursos informáticos muy concentrados que están en manos de unas pocas grandes empresas tecnológicas".

plataformas y ecosistemas. Están utilizando el diseño de mecanismos para incentivar tipos específicos de participación e impresiones de usuarios con y dentro de sus ecosistemas, alentándonos a pasar más tiempo utilizando sus productos y servicios.

Como observan los diseñadores de la experiencia de los usuarios (Collins, 2020), una función simple como deslizar verticalmente de manera constante (*scrolling*), que es una característica determinante de plataformas como Facebook, Twitter e Instagram, fue diseñada precisamente porque las empresas sabían que generaría una conducta adictiva, que haría que nuestra atención no se despegara de la pantalla. Lo mismo ocurre con las notificaciones, los *me gusta* y otras herramientas de la interacción digital. Y cuanto más tiempo y atención dediquemos a nuestros dispositivos, las grandes empresas tecnológicas podrán obtener más valor a partir de nuestro comportamiento. Al diseñar mercados de este modo, Viljoen y otros afirman que las grandes empresas tecnológicas pueden cultivar y explotar las denominadas *asimetrías de información*, es decir, la información que las grandes empresas tecnológicas poseen, pero que no es accesible a los usuarios.

La oposición a las grandes empresas tecnológicas

Debido a su poder social y en el mercado, las grandes empresas tecnológicas afrontan una creciente oposición a su dominio. En algunos casos se trata de oposición colectiva, pero en otros surge de las contradicciones inherentes e internas dentro de sus propias estrategias y funcionamiento.

El juicio entablado en Texas mencionado al comienzo es tan solo una de varias demandas colectivas presentadas contra grandes empresas tecnológicas, tanto por Gobiernos como por competidores. Diversas jurisdicciones han realizado esfuerzos más concertados para limitar el poder de las grandes empresas tecnológicas, algunos de ellos

parecen ser más eficaces que otros.[9] La Unión Europea, en particular, ha estado activa en este ámbito a medida que ha aumentado la preocupación acerca de los efectos anticompetitivos de las grandes empresas tecnológicas. Recientemente, la Unión Europea ha presentado varias políticas y reglamentos, como, por ejemplo:

- La *Ley de Mercados Digitales* que establece reglamentaciones *ex ante* para controlar el comportamiento de las empresas denominadas *guardianas*, como las grandes empresas tecnológicas. La Ley prohíbe determinadas acciones como combinar datos personales de plataformas con datos recopilados de otros servicios. Entró en vigor en 2023;
- La *Ley de Servicios Digitales* diseñada para aumentar la transparencia de la publicidad en línea y reducir el contenido ilegal y la desinformación. Entrará en vigor en 2024; y
- El *Reglamento de Gobernanza de Datos* para la libre circulación y la normalización del intercambio de datos entre organizaciones, a través de la limitación de la capacidad de las empresas para acumular datos. Aún se encuentra en la fase legislativa.

Otros países y jurisdicciones, como Australia y los Estados Unidos, están adoptando medidas a pesar de la fuerte presión de las grandes empresas tecnológicas y las empresas impulsadas por datos.

Otro tipo de oposición parece estar surgiendo de las propias empresas tecnológicas, a saber, los crecientes efectos contradictorios provocados por sus operaciones y estrategias. Como probablemente todos los usuarios lo hayan notado, los productos y servicios ofrecidos por las grandes empresas tecnológicas son cada vez menos útiles e incluso

[9] Donde vivo, en Canadá, el Gobierno federal ha propuesto legislación para actualizar las reglamentaciones sobre protección y privacidad de datos, que no han cambiado en los últimos veinte años. Sin embargo, el enfoque del Gobierno a la reforma se basa en permitir a las empresas seguir recopilando y procesando nuestros datos en un nuevo marco de privacidad, en lugar de cuestionar la recopilación y el uso de esos datos en sí (Birch, 2022).

disfuncionales. Mis experiencias personales incluyen: comprar productos de dudosa calidad en Amazon que son imitaciones o estafas; tener que deslizar el ratón hasta la mitad de la página para evitar los anuncios en el motor de búsqueda de Google; desistir de buscar en Facebook debido a la cantidad de anuncios; tener que cambiar la configuración de los productos de Microsoft debido a algún efecto automático extraño; y evitar a Apple a toda costa porque no quiero quedar atascado en un enclave.

Otras plataformas están teniendo experiencias similares; a las empresas impulsadas por datos les resulta cada vez más difícil alcanzar sus objetivos: por ejemplo, las empresas de arrendamiento en línea de vehículos con conductor como Uber y Lyft han debido aumentar sus precios al mismo nivel o incluso a niveles más elevados que las empresas de taxis (Doctorow, 2021); las empresas de entrega de comida como Doordash o Deliveroo han perjudicado a los restaurantes de los que depende su propia existencia (Roy, 2020); y Airbnb está plagado de estafas, además de que está transformando el mercado inmobiliario de un modo problemático (Goldfischer, 2022). Y ni hablemos de productos como *las granjas de clics* (Birch, 2020).

En general, debemos encontrar formas de limitar la recolección y el uso de nuestros datos personales y creo que cada vez hay más espacio político para hacerlo, a medida que empresas impulsadas por datos encuentran nuevos problemas con sus modelos de negocios e innovación. Existen opciones. Una de ellas consiste en canalizar los sentimientos a favor del mercado al convertir nuestros datos en nuestra propiedad (Posner y Weyl, 2019), lo cual, aunque suena atractivo, probablemente no resuelva nada, ya que es difícil determinar quién debería ser propietario de qué información. Otra opción es crear fideicomisos de datos (Wiley y McDonald, 2018), quizá administrados por Gobiernos u organismos públicos, que brinden acceso a todo tipo de datos digitales, mientras que supervisan el modo en que se utilizan. Ello podría contribuir a resolver algunos problemas y permitir que nuestros datos se utilicen de modos en los que estamos de acuerdo. Sin embargo, no impediría necesariamente que las grandes empresas

tecnológicas accedan a nuestra información personal. Una tercera opción es crear cooperativas o comunas de datos descentralizadas (Scholz y Calzada, 2021), que colectivicen nuestros datos personales y permitan una mayor supervisión y rendición de cuentas a nivel local. Estas cooperativas estarían administradas por grupos, organizaciones o comunidades, pero daría mucho trabajo gestionar todas las preocupaciones de las personas respecto de la seguridad de sus datos personales.

Hay algo que es seguro: veremos muchos más datos digitales a lo largo de nuestras vidas y si queremos utilizarlos para nuestro beneficio colectivo, tendremos que hallar el modo de controlarlos en forma colectiva y democrática, en lugar de dejarlos en manos de las empresas poderosas que harán lo que les plazca.

En conclusión

El diseño de mercado ha sustentado el auge de las grandes empresas tecnológicas en los últimos diez años. Un nuevo conjunto de tecnologías digitales y algorítmicas ha permitido que estas y otras empresas impulsadas por datos moneticen la información de la cual se supone que dependen los mercados (por ejemplo, quién quiere comprar X, qué persona Y pagaría por Z, cuántas personas ven A). Esta información sobre el mercado intenta ser transparente y veraz para asegurar la competencia, pero cada vez más se acapara y oculta en enclaves de datos creados por grandes empresas tecnológicas a fin de garantizar su monopolio. Entonces, en lugar de simplemente monetizar información personal, las grandes empresas tecnológicas han ido mucho más allá de los temores de *vigilancia* expresados por muchos críticos, como Shoshana Zuboff.[10]

[10] Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism*. Nueva York: Public Affairs.

No obstante, en la actualidad, las grandes empresas tecnológicas afrontan distintos tipos de cuestionamientos: tanto de políticos y responsables de la formulación de políticas que elaboran nuevos marcos para limitar su poder, como los que surgen de las contradicciones internas y el mal funcionamiento de sus propias operaciones. Todo ello hace que nos planteemos la siguiente pregunta: ¿regresarán los mercados para vengarse o es este el comienzo de algo nuevo? Es importante que activistas, grupos de la sociedad civil, organizaciones no gubernamentales y el público en general recuerden que al sensibilizar e interactuar con Gobiernos acerca del poder de las grandes empresas tecnológicas, si ya no hay mercados, las formas anticuadas de los reguladores de entender el mundo no servirán para controlar a las grandes empresas tecnológicas. Debemos pensar más allá del mercado.

Bibliografía

Amadae, S.M. (2016). *Prisoners of Reason*. Cambridge: Cambridge University Press.

Birch, Kean (2 de noviembre de 2017). What Exactly is Neoliberalism? *The Conversation.* https://theconversation.com/what-exactly-is-neoliberalism-84755

Birch, Kean (2020). Automated neoliberalism? The digital organization of markets in technoscientific capitalism. *New Formations*, 100-101, 10-27.

Birch, Kean, Cochrane, D.T. y Ward, Callum (2021). Data as asset? Unpacking the measurement, governance, and valuation of digital personal data by Big Tech. *Big Data & Society,* 8(1), 1-15.

Birch, Kean y Bronson, Kelly (2022). Introduction: Big Tech. *Science as Culture* 31(1), 1-14.

Cámara de Representantes de los Estados Unidos (2020). In*vestigation of Competition in Digital Markets*. Washington, DC: House of Representatives.

Collins, Grant (2020). *Why the infinite scroll is so addictive*. https://uxdesign.cc/why-the-infinite-scroll-is-so-addictive-9928367019c5

Departamento de Justicia de los Estados Unidos (2020). Justice Department Sues Monopolist Google For Violating Antitrust Laws, Washington DC: Departamento de Justicia. https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws

Doctorow, Cory (10 de agosto de2021). End of the Line for Uber. *Pluralistic*. https://pluralistic.net/2021/08/10/unter/#bezzle-no-more

Goldfischer, Emily (3 de agosto de 2022). Scams: The Dark Side of Alternative Accommodations. *Hertelier*. https://www.hertelier.com/post/airbnb-booking-com-scams

Hayek, Friedrich (1945). *The Use of Knowledge in Society*. https://www.econlib.org/library/Essays/hykKnw.html?chapter_num=1#book-reader

Leonard, Christopher (2022). *The Lords of Easy Money*. Nueva York: Simon & Schuster.

McMillan, John (2003). *Market Design: The Policy Uses of Theory*. Stanford Business School: Working Paper No.1781. https://www.gsb.stanford.edu/faculty-research/working-papers/market-design-policy-uses-theory

Mirowski, Philip y Nik-Khah, Edward (2017). *The Knowledge We Lost in Information*. Oxford: Oxford University Press.

Morozov, Evgeny (2022). Critique of Technofeudal Reaso. *New Left Review*, 133/134, 89-126.

Posner, Eric y Weyl, Eric Glen (2019). *Radical Markets*. Princeton: Princeton University Press.

Roy, Ranjan (17 de mayo de 2020). Doordash and Pizza Arbitrage. *Margins*. https://www.readmargins.com/p/doordash-and-pizza-arbitrage

Scholz, Trebor y Calzada, Igor (19 de abril de 2021). Data Cooperatives for Pandemic Times. *Public Seminar*. https://publicseminar.org/essays/data-cooperatives-for-pandemic-times/

Texas Attorney General et al. (2022). Google Digital Advertising Antitrust Litigation. https://www.nysd.uscourts.gov/sites/default/files/2022-09/In%20re%20Gogle%20Digital%20Advertising%20Antitrust%20Lirtigation.pdf

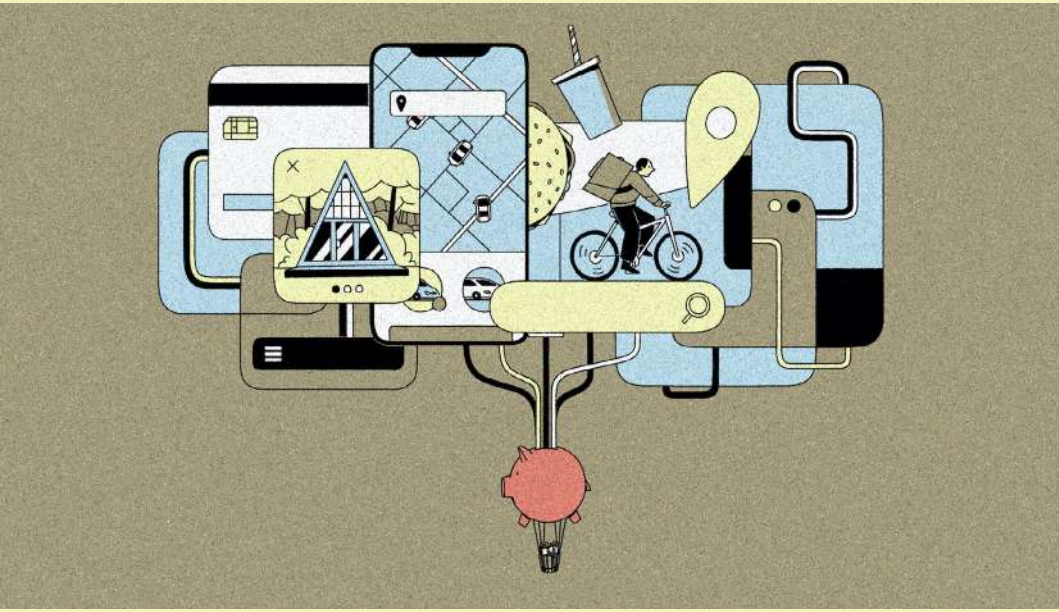
Viljoen, Salomé, Goldenfein, Jake y McGuigan, Lee (2021). Design choices: Mechanism design and platform capitalis*. Big Data & Society,* 8(2), 1-13.

Wiley, Bianca y McDonald, Sean Martin (9 de octubre de 2018). What is a Data Trust? *Centre for International Governance Innovation.* https://www.cigionline.org/articles/what-data-trust/

Zuboff, Shoshana (2019). *The Age of Surveillance Capitalism*. Nueva York: Public Affairs.

Control económico

El papel de la financiación en las grandes empresas tecnológicas



Nils Peters

Traducción al español por Mercedes Camps
Ilustración de Anđela Janković

Para entender el poder de las grandes empresas tecnológicas es preciso examinar a sus financiadores. El capital de riesgo ha alentado el entusiasmo y la especulación y ha motivado a plataformas a monopolizar al público y limitar la remuneración y los derechos de los trabajadores.

Web3 ocupa un lugar destacado en la agenda de los fundadores y financiadores de Silicon Valley. El más reciente paradigma tecnológico del libertarismo promete a grandes rasgos descentralizar Internet, mediante el uso de tecnologías como la cadena de bloques, para salvarlo del actual control empresarial de las plataformas. A un año del entusiasmo inicial, el resultado es, en el mejor de los casos, dispar (Wayt, 2021). Pero, además de las deficiencias y la falta de entusiasmo del público en general, las personas del medio han identificado un problema más profundo con respecto al próximo gran avance tecnológico. Jack Dorsey, cofundador de Twitter, señaló el motivo por el cual el optimismo de quienes promueven la descentralización es infundado. El 21 de diciembre de 2021, tuiteó: "No se es propietario de 'Web3'. El capital de riesgo y sus socios limitados lo son. Nunca escapará a sus incentivos" (Muoio, 2017).

En el debate contemporáneo sobre el poder digital no se suele prestar mucha atención a los inversores de capital de riesgo y sus financiadores (socios limitados). Sin embargo, hace tiempo que deberíamos centrarnos en los actores financieros que están detrás de las revoluciones tecnológicas. ¿Cómo funcionó Uber durante casi diez años sin obtener ganancias? ¿por qué Google creó su negocio de publicidad en primer lugar? ¿cómo Facebook (ahora Meta) ahuyentó a sus competidores iniciales? Construir y mantener una plataforma es extremadamente costoso. Cuando intentamos indagar en el poder digital y analizar las medidas que adoptaron determinadas empresas

para ser dominantes, debemos formular la siguiente pregunta: ¿cómo se financiaron?

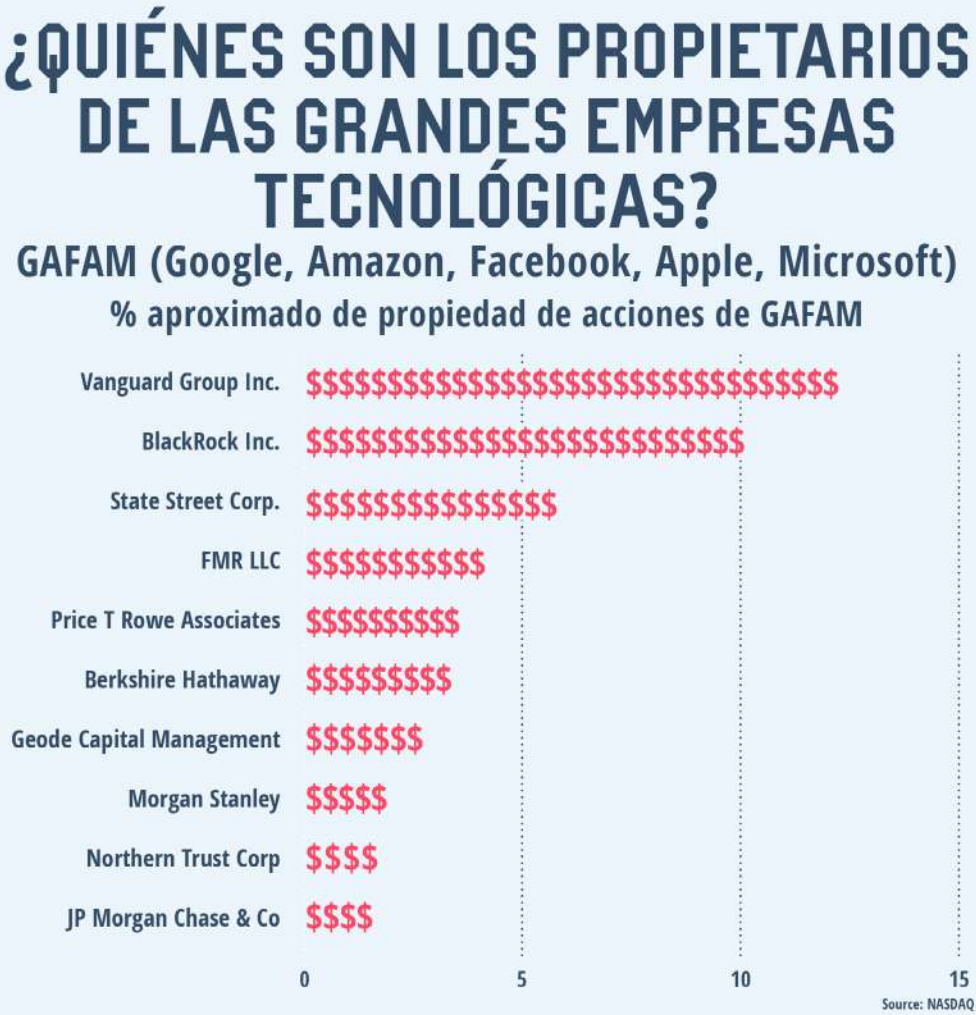
El capital de riesgo es una forma de inversión de alto riesgo y alto beneficio. La mayoría de las inversiones fracasan, pero un pequeño número de inversiones extremadamente exitosas generan ingresos enormes. Un famoso ejemplo de ello es la inversión de 12 millones de dólares de la empresa de capital de riesgo Benchmark en Uber, que aumentó su valor en 7 mil millones de dólares.[11] Los inversores de capital de riesgo, a su vez, recaudan el dinero que invierten de fondos de jubilación, legados, aseguradoras, empresas y personas con un alto valor neto. Al invertir, se convierten en socios limitados de un fondo de capital de riesgo.

Los financiadores están muy lejos de ser intermediarios neutros que simplemente asignan capital. Afrontan presión para obtener ganancias para sus accionistas y partes interesadas, y participan activamente en transformar el mundo que los rodea para que se adapte a sus objetivos financieros. Muy pocas grandes empresas tecnológicas pueden crecer sin fondos de capital de riesgo. Algunos ejemplos destacados son Amazon (que recibió US$8 millones en financiación de capital de riesgo), Google (que recibió US$36 millones), Facebook (que recibió US$800 millones), Airbnb (que recibió US$2.444 millones) y Uber (que recibió US$6 523 millones).[12] Habida cuenta de la magnitud de las inyecciones de efectivo, es muy poco probable que se pueda fundar una gran empresa tecnológica sin fondos de capital de riesgo. ¿Cómo puede un emprendedor cualquiera competir con una empresa que atrae fondos de esta magnitud? Y si no puede, ¿no debería la financiación ser un aspecto más importante de nuestro análisis del poder digital?

Es decir, si queremos entender el poder digital, debemos entender cómo está financiado. A fin de cuentas, el poder digital es parte de una

[11] Ver Crunchbase (2022a) Amazon—Funding, Financials, Valuation & Investors. https://www.crunchbase.com/organization/amazon/company_financials

[12] Ver Crunchbase, 2022b, 2022d, 2022e; StartupRanking, 2022c; Klinge et al., 2022.



economía financiarizada (Summers, 2016). Si ignoramos los pilares financieros de la economía de plataformas corremos el riesgo de perder de vista el modo en que las grandes empresas tecnológicas nos afectan más allá de la naturaleza del trabajo y las preocupaciones sobre la privacidad. Como demostrará este ensayo, los elementos financiarizados de la vida diaria, desde las contribuciones jubilatorias y de seguros hasta los préstamos, están vinculados con la suerte de las grandes empresas tecnológicas.

Podemos aprender mucho sobre el funcionamiento de las grandes empresas tecnológicas que cotizan en la bolsa mediante el estudio de sus comienzos en el mercado privado. No me centraré en las grandes empresas tecnológicas ya consolidadas, como Amazon, Alphabet, Apple y Meta. Cuando las empresas tecnológicas comienzan a cotizar en la bolsa, las compañías de capital de riesgo pierden la mayor parte de su influencia sobre ellas. Sin embargo, durante el periodo crucial entre su constitución y el momento en que empiezan a cotizar en la bolsa, los financiadores desempeñan un papel fundamental en la configuración de las empresas tecnológicas emergentes. Entender cómo se forja la próxima generación de grandes empresas tecnológicas puede contribuir a protegernos contra su poder. Al centrar la atención en ello, el presente artículo intenta desarrollar herramientas para entender y resistir a las grandes empresas tecnológicas a medida que se desarrollan.

La financiación del auge tecnológico

Larry Summers sostuvo que desde el comienzo de la primera década del siglo XXI, las economías de Occidente están en un estado de "estancamiento secular".[13] De ese modo se describe a la situación en que los ahorros excesivos provocan un descenso de la demanda porque no se gastan ni generan nuevos ingresos. Como se ha demostrado, el aumento de la riqueza desenfrenada ha provocado un crecimiento considerable de los ahorros entre el 1 % más rico de la población. Los ahorros excesivos en este caso reflejan las enormes desigualdades en el ingreso y la distribución de la riqueza. Además de ello, Summers explica que las plataformas digitales conservan el capital al estimular los ahorros: "Un ejemplo de ello es el impacto de Airbnb en la construcción de hoteles, el impacto de Uber en la demanda de automóviles, el impacto de

[13] Ver Bank of England (2022). Quantitative easing. https://www.bankofengland.co.uk/monetary-policy/quantitative-easing

Amazon en la construcción de centros comerciales o el impacto más general de la informática en la demanda de fotocopiadoras, impresoras y espacios de oficina"(Summers, 2016). Los resultados de estos dos acontecimientos son la baja inversión, el bajo crecimiento, una recuperación débil de las crisis económicas y un capitalismo desprovisto de dinamismo. Este es el contexto financiero en el que debe interpretarse el auge de la economía de plataformas.

Este acontecimiento fue especialmente problemático tras la crisis financiera mundial de 2008. Los Gobiernos y los bancos centrales debían contener la crisis y trazar una recuperación a partir de lo que pasaría a conocerse como la *Gran recesión*. Las respuestas clave fueron la austeridad fiscal y una política monetaria expansiva. Los principales bancos centrales como la Reserva Federal, el Banco de Inglaterra y el Banco Central Europeo disminuyeron las tasas de interés casi a cero. Al mismo tiempo, los bancos centrales implementaron programas de *expansión cuantitativa*.[14] Sin entrar en los detalles más técnicos, ello significó que los bancos centrales comenzaron a adquirir bonos del Gobierno y de empresas, lo que, a su vez, provocó un aumento del precio y una disminución del interés de dichos bonos. La intención era fomentar la inversión y el crecimiento económico al abaratar la obtención del crédito.

En efecto, la expansión cuantitativa dificultó que muchos inversores dependieran del pago de intereses para obtener los ingresos deseados. Ese fue especialmente el caso de inversores institucionales como los fondos jubilatorios, dotaciones de fondos y aseguradoras, a las que les resulta cada vez más difícil hallar salidas rentables para su capital, por lo que quedan a merced de grandes administradoras de activos como BlackRock. Si hubo un crecimiento significativo en este clima, este ha provenido de ganancias de capital en mercados bursátiles. Ello provocó la conversión de ahorros en niveles de inversión insosteniblemente elevados, como consecuencia de la deuda. El flujo

[14] Ver Tech Nation (2021). *The future UK tech built*—Tech Nation Report 2021. https://technation.io/report2021/

de capital barato causó una disminución aún mayor del rendimiento de los bonos y un aumento del rendimiento del capital accionario. Es decir que la estrategia de comprar las deudas de los Gobiernos y las empresas (bonos) –que ha sido demostrada, pero que resulta cada vez más inadecuada para los inversores institucionales– se complementó mediante la compra de acciones y valores (capital) de las empresas.

Ello dio lugar a diez años de mercado alcista de las acciones de las grandes empresas tecnológicas que cotizan en la bolsa –y de acciones privadas de empresas tecnológicas emergentes–, en el cual los precios de los activos aumentaron sin cesar. Los *unicornios*, es decir, las empresas privadas con una valoración superior a los 1.000 millones de dólares, se volvieron figuras centrales muy publicitadas de la aparentemente incesante trayectoria al alza. El *número de unicornios* en el Reino Unido aumentó de diez en 2010 a ochenta en 2020.[15] Lo mismo ocurrió con el exceso de ahorros, lo cual demuestra la estrecha relación entre las tendencias macroeconómicas, las finanzas y el destino de las grandes empresas tecnológicas.

El nexo entre el capital de riesgo y la plataforma

Los inversores de capital de riesgo adquieren participaciones minoritarias en empresas privadas en la fase inicial. En general, los inversores de capital de riesgo son miembros de las juntas directivas de esas empresas, les brindan asesoramiento y consultoría. Son conocidos por financiar a la nueva generación tecnológica. Por ese motivo, el capital de riesgo a menudo es considerado un capital *paciente*, debido a que los inversores deben asumir un compromiso de diez años antes de ver resultados. La única forma en que los inversores de capital de riesgo pueden obtener ganancias es cuando la empresa en la que invierten es adquirida (generalmente mediante algún tipo de fusión o

[15] Ver Comisión Europea (2017). Un sistema impositivo justo y eficaz en la Unión Europea para el Mercado Único Digital.COM/2017/0547 final.

adquisición) o empieza a cotizar en la bolsa de valores mediante una oferta pública inicial. En el caso de Uber, transcurrieron diez años desde su constitución hasta la oferta pública inicial. A pesar de la *paciencia*, los fondos de capital de riesgo suelen tener una duración limitada, lo que significa que el entendimiento entre los inversores y las empresas emergentes es que estas últimas deben procurar tasas de crecimiento ambiciosas para ampliar su escala rápidamente.

Para obtener ganancias, los inversores institucionales están optando cada vez más por salidas alternativas y más riesgosas para su capital. El capital de riesgo es el principal beneficiario de esta dinámica. La relación entre los inversores institucionales y los inversores de capital de riesgo puede imaginarse como una cadena de inversiones. Los inversores institucionales gestionan grandes carteras de inversión de manera conservadora. Las ganancias que generan financian planes de jubilación, prestaciones de seguros, gastos de dotación de fondos o simplemente enriquecen aún más a los ricos. Los fondos de capital de riesgo gestionan volúmenes y carteras mucho más pequeños y tienen una estructura inversa de riesgo-recompensa. Actúan como intermediarios entre los inversores institucionales y las empresas tecnológicas emergentes que aún no han despegado, absorbiendo así el desfase en el riesgo y enviando el dinero a mercados privados de dudosa reputación.

Además de los factores macroeconómicos, las características del capital de riesgo impulsaron el aumento de las inversiones en sus fondos. Los inversores de capital de riesgo invirtieron en primer lugar en empresas relacionadas con la tecnología, uno de los pocos sectores que aún generaba crecimiento en una fase de recesión del capitalismo (Tech Nation, 2021). Además, el sector del capital de riesgo sabe cómo vender y publicitar ampliamente sus triunfos. Las empresas de capital de riesgo más exitosas generan ganancias más elevadas de las que puede ofrecer el mercado de valores. Como consecuencia de ello, el capital de riesgo experimentó un aumento pronunciado de los volúmenes de financiación a finales de la primera década del siglo XXI . En 2020, la inversión de capital de riesgo en empresas tecnológicas en el Reino

Unido fue de 14.900 millones de dólares (Teare, 2022). Esa cifra se ve opacada por el mercado de capital de riesgo de los Estados Unidos, que alcanzó inversiones de 144.300 millones de dólares. A nivel mundial, las inversiones de capital de riesgo aumentaron de 59.000 millones de dólares en 2012 a más de 650.000 millones en 2021(Nicholas, 2019).

Además del dinero barato, los inversores de capital de riesgo se vieron atraídos por los nuevos modelos de negocios. El ensayo general para la economía de plataformas actual fue el auge de las empresas *puntocom* de la década del noventa, cuando las empresas de comercio digital fueron las primeras en proponer muchas de las ideas que diez años más tarde se volvieron moneda corriente. La burbuja de las empresas *puntocom* (y su posterior explosión) suele ser objeto de burla debido a que muchas ideas ridículas terminaron en los mercados públicos a valores exorbitantes. Sin embargo, los modelos de negocios y la financiación de empresas como Pets.com (que entregaba insumos para mascotas pedidos en línea) no eran drásticamente diferentes de las gigantes de plataformas de hoy en día.[16]

Las estrategias de negocios de las plataformas dependen de inversores que estén dispuestos a soportar pérdidas financieras durante un año entero. A través de un acuerdo mutuo, las plataformas como Uber pierden dinero porque dan más importancia al crecimiento rápido (o el aumento de escala) que a la rentabilidad. Las plataformas aplican estrategias diferentes para impulsar su crecimiento. Por un lado, hay un crecimiento impulsado por los usuarios mediante lo que se denominan efectos de red. La posición de las plataformas como intermediarias digitales de grupos de usuarios diferentes implica que creen redes de usuarios. Los efectos de red ocurren cuando el valor del servicio o producto que ofrece la plataforma aumenta a medida que más personas comienzan a utilizarla. Por ejemplo, el valor de utilizar Instagram aumenta a medida que aumentan sus usuarios (efectos de

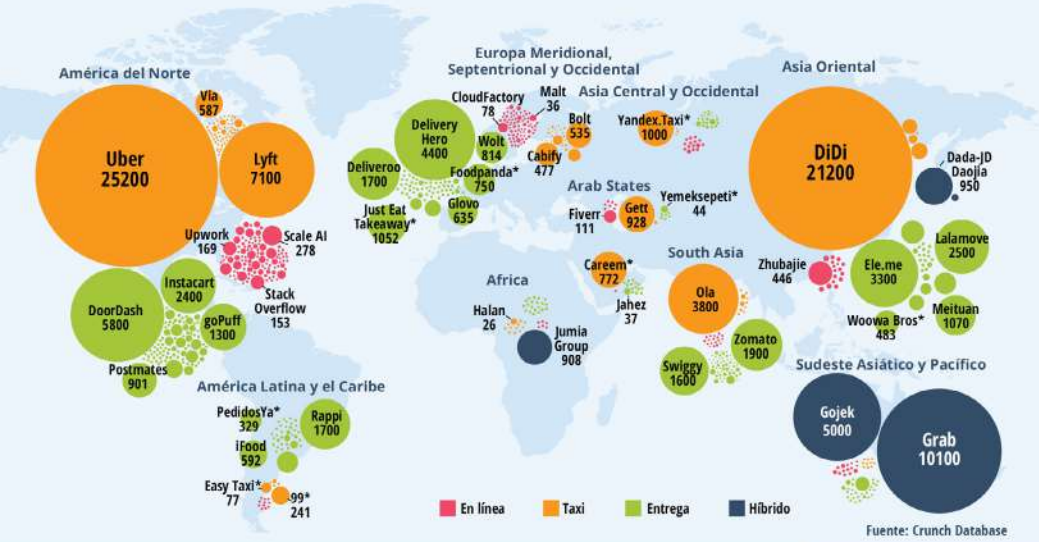
[16] Ver Uber Technologies Inc. (2019). Form S-1 Registration Statement. https://www.sec.gov/Archives/edgar/data/1543151/000119312519103850/d647752ds1.htm#toc647752_16

red directos) y el valor de solicitar un coche o de conducir para Uber aumenta a medida que cada grupo crece (efectos de red indirectos). En algún momento, los efectos de red se convierten básicamente en un monopolio natural, similar a la infraestructura de ancho de banda o los sistemas de ferrocarriles, donde los usuarios dependen cada vez más de los servicios, mientras que a los competidores les resulta cada vez más difícil ingresar.

De manera alternativa o adicionalmente, las plataformas pueden gastar el dinero de los inversores al duplicar sus gastos. Pueden usar el

LA ECONOMÍA DE PLATAFORMAS HA TENIDO UN AUGE GRACIAS AL CAPITAL FINANCIERO

Financiación total de capital de riesgo y otros inversores, categorías seleccionadas de plataformas de trabajo digital por región, 1998–2020 (en millones de dólares).



Fuente: Crunch Database

Inversión financiera mundial en plataformas de trabajo digital: 119.000 millones de dólares (1998–2020)

Ganancia mundial: 52.000 millones de dólares

Remuneración de trabajador promedio: 3,40 dólares por hora

dinero de los inversores para obtener clientes, como a través de descuentos o publicidad. Mediante el crecimiento impulsado por el capital de riesgo, las plataformas pueden expulsar a los competidores y mantenerlos alejados. Más que una opción, el crecimiento rápido es una condición necesaria para que muchas plataformas sean rentables en el futuro, debido a que su rentabilidad depende del dominio del mercado.

En resumen, el modelo de las plataformas se basa en grandes volúmenes de capital *paciente* que financia la rápida ampliación de escala de las operaciones de la plataforma. Los efectos de red son una herramienta poderosa que hace posible este proceso. Dominar el mercado no solo es deseable, sino que es necesario para que las plataformas sean sostenibles y para que sus inversores de capital de riesgo obtengan ganancias suficientes por sus inversiones. Ello fue propiciado por un entorno macroeconómico de bajos intereses a partir de la primera década del siglo XXI, que generó condiciones en las cuales las plataformas no obtuvieron ganancias durante años. Aunque este acuerdo de financiación es anterior a Internet, la digitalización aumentó la velocidad y la escala de la expansión de las empresas en las que se invierte.

Se puede concluir, entonces, que existe una estrecha relación entre el capitalismo financiero y de plataformas. El surgimiento de las plataformas desempeña una función en una búsqueda más amplia de ingresos para los inversores. El problema de las bajas ganancias de los inversores institucionales se *resolvió* al canalizar dinero a los fondos de capital de riesgo. Los inversores de capital de riesgo corrieron hacia las plataformas debido a su capacidad para utilizar grandes volúmenes de efectivo y la baja probabilidad de obtener grandes ganancias. A cambio, la disponibilidad de este capital empujó a las grandes empresas tecnológicas a modelos que intentaban volverse dominantes y excluían a los competidores. La otra cara del ahorro excesivo fue un régimen de inversión liderado por capital de riesgo para el cual las plataformas se volvieron una salida ideal. La financiación desempeña un papel fundamental respecto de quién avanza en la economía digital, y el poder digital se reduce al poder de financiación.

El poder digital desde una perspectiva financiera

Examinar las plataformas emergentes desde una perspectiva financiera permite realizar un análisis diferente de la situación actual. Alphabet, Amazon y compañía acaparan la mayor parte de la atención pública. Sin embargo, decenas de plataformas emergentes intentan hacerse espacio y *trastocar* a los sectores tradicionales. Al parecer, la atención de los inversores se centra cada año en un producto nuevo. Hace algunos años, los servicios de transporte privado con conductor inauguraron esta tradición con un enfrentamiento feroz entre Uber y Lyft. Desde entonces, los servicios de envío de alimentos (JustEat, Uber Eats, Deliveroo), la micromovilidad a través del alquiler de bicicletas y monopatines (Bird, Lime, Bolt) y los bancos retadores (Monzo, Revolut, N26) se han sumado a esta tendencia. Más específicamente, tras la pandemia, el envío rápido de comestibles (Getir, Gorillas) y las herramientas de colaboración de oficina se han visto inundados de efectivo de inversores.

Cada una de estas plataformas fue presentada al público como un cambio revolucionario en el modo en que funcionan la economía y la sociedad. Uber es el caso más destacado. Tras años de escándalos en que se han visto involucradas las grandes empresas tecnológicas, resulta difícil recordar que, en sus inicios, Uber fue aplaudida como la precursora de la *economía colaborativa*. Por un periodo muy breve, se creyó verdaderamente que las plataformas podían lograr un capitalismo más democrático y sostenible al permitir que las personas compartieran sus activos subutilizados. Gracias a ese discurso, Uber obtuvo más de 6 mil millones de dólares en financiación de capital de riesgo en los años posteriores para cumplir esta profecía. Su lista de inversores abarca a los nombres más importantes en inversión de mercado, en los que se incluyen la empresa de capital de riesgo Benchmark, Vision Fund de SoftBank y el fondo de riqueza soberana de Arabia Saudita, el Fondo de Inversión Pública (Davies et al., 2022).

Con su *cofre* repleto, Uber se embarcó en la típica estrategia de plataforma señalada anteriormente. Como han revelado más

recientemente los archivos de Uber, los empleados optaron por estrategias agresivas para provocar la quiebra de las industrias tradicionales de servicios de vehículos con conductor (es decir, los taxistas) (Chen, 2021). Los competidores fueron superados en los precios, donde Uber podía fijar tarifas por debajo del costo para aumentar su cuota de mercado. Para mantener los efectos de red, la empresa pudo utilizar el dinero de sus inversores para mantener costos de adquisición sorprendentes. En un momento, la empresa pagaba a sus conductores un bono de recomendación de 750 dólares: los nuevos conductores recibían 750 dólares por inscribirse y se daba 750 dólares a la persona que los había recomendado. Como se jactaba el entonces ejecutivo de Uber, Andrew Chen: "gastamos cientos de millones de dólares tan solo en programas de recomendación de conductores y casi mil millones en *marketing*" (Horan, 2019). A la luz de estas estrategias, la falta de rentabilidad de Uber no resulta sorprendente.

Aunque en sus comienzos Uber parecía imparable, un análisis más sobrio plantea la pregunta de qué quedaría de este poder digital sin el enorme apoyo financiero. "Uber Technologies Inc." es el nombre oficial registrado de la empresa, pero ¿qué cambios considerables logró su tecnología? Es cierto que Uber construyó una excelente aplicación con una buena interfaz de usuario. Pero ello no resolvió ninguno de los problemas que los servicios de taxi han tenido desde siempre: trayectos de regreso vacíos debido a un desequilibrio geográfico en la demanda, el elevado costo de la capacidad máxima o el riesgo de sobrecapacidad (Levingston, 2022). Esto es emblemático de la economía de plataformas en general, donde unas pocas empresas tecnológicas a menudo disfrazan el hecho de que las empresas de plataformas no están resolviendo antiguos problemas, sino que simplemente los están repitiendo.

Entonces, ¿por qué los servicios de plataformas son tan populares con los consumidores? En este artículo, la demanda de servicios de plataforma se explica en gran medida a través de la distorsión de los precios posibilitada por el dinero de capital de riesgo. Ello significa que, en el comienzo, los servicios o bien son gratuitos o son

insosteniblemente baratos. No resulta para nada sorprendente que a las personas les encantan las cosas gratis. Pero la demanda del servicio al precio *real* que los consumidores pagarán a la larga será inevitablemente más baja. Por lo tanto, el reto para la plataforma es perjudicar a sus competidores e insertarse en el deseo de conveniencia de las personas antes de alcanzar ese punto. A medida que la financiación del capital de riesgo y las ganancias de la oferta pública inicial de Uber comienzan a acabarse, la empresa ha comenzado a aumentar los precios de manera constante.[17]

Algo similar ha ocurrido en otros sectores. Las plataformas de micro movilidad llenaron a ciudades europeas de servicios de alquiler de bicicletas y monopatines eléctricos ante la consternación de los habitantes locales (Taylor, 2018). Al analizar las narrativas del acceso fácil, el intercambio y la conveniencia, muchas de estas empresas parecen ser el resultado de un acto de desesperación por crear el "próximo gran producto" (Lunden, 2022). Ello pone de manifiesto los límites de la plataformización propiciada por el apoyo financiero. Estos límites ahora se han vuelto cada vez más evidentes debido a las cambiantes condiciones macroeconómicas. La inflación elevada y el aumento de las tasas de interés han disminuido el flujo de efectivo hacia las empresas emergentes de alto riesgo. En un momento en que los inversores quieren ver un flujo positivo de efectivo, en lugar de un índice elevado de gasto de ese efectivo, muchos factores *alteradores* están sumidos en el caos. Un ejemplo destacado de ello es el sector del envío rápido de productos alimenticios, en el que Gorillas despidió a cientos de trabajadores y se fue de cuatro países (Lee, 2022). Ni las gigantes tecnológicas Meta, Alphabet, Amazon y Twitter se salvaron, y según los datos de despidos se estima que se eliminaron más de 130 mil puestos de trabajo (Steinschaden, 2019).

Un análisis de la situación actual de las plataformas emergentes desde el punto de vista financiero, nos hace cuestionar nuestra

[17] Ver Agence France-Presse (25 de febrero de 2018). Gobee.bike pulls out of France due to 'mass destruction' of its dockless bike fleet. *The Guardian*.

como una revolución en el transporte o en las compras comienzan a parecer intentos desesperados de inversores para obtener ganancias en un entorno de bajo rendimiento. La capacidad de Uber, Bolt y Gorillas (por nombrar a algunas) para convertir a su tambaleante modelo de negocios en una profecía autovalidante se basó en torrentes de capital de sus inversores de capital de riesgo. Y estos grandes flujos de capital eran una función de una economía mundial inundada de

efectivo. La cuestión es que muchos servicios de plataformas existen únicamente debido a que la abundancia de capital debe canalizarse en algún lado.

Desfinanciarizar para desplataformizar: Repercusiones y resistencia

No es posible hablar de poder digital sin hacer referencia al poder financiero que está detrás de las plataformas. Este nuevo ángulo revela nuevas dependencias a medida que la marea macroeconómica en 2022 ha puesto mucha presión en las empresas tecnológicas. El aumento de las tasas de inflación ha provocado que los bancos centrales aumenten sus tasas de interés. Los inversores lo sintieron de inmediato y adoptaron un enfoque más conservador hacia las inversiones de alto riesgo.

Pero este no es motivo de regocijo. Si seguimos la cadena de inversores, la disminución de la inversión en tecnología tendrá efectos colaterales para la sociedad en general. Cuando el dinero era barato y los mercados estaban al alza, las empresas emergentes mantenían felices a los inversores de capital de riesgo. El aumento de los valores de la cartera de capital de riesgo implicó mejores ganancias para sus socios de responsabilidad limitada, los fondos jubilatorios, las empresas de seguros, las dotaciones, etcétera. Ello, en última instancia, aseguró la viabilidad de programas de contribución jubilatoria y planes de seguros definidos. Los inversores institucionales asignan tan solo un pequeño porcentaje de sus carteras a clases de activos riesgosos y no se verán afectados drásticamente por la desaceleración en el sector tecnológico. No obstante, cabe señalar que nuestras decisiones cotidianas están vinculadas con las altas finanzas.

Aunque el capital de riesgo es una forma de inversión extremadamente especulativa, las decisiones de inversión tienen efectos concretos en el presente. Hay sumas de dinero considerables vinculadas con empresas cuya existencia depende de gastar el dinero de inversores

de capital de riesgo. Independientemente de las estrategias financieras sostenibles, las plataformas han perjudicado de forma permanente a los competidores y las industrias tradicionales. Las empresas de transporte como Uber son un ejemplo claro de ello, y lo mismo puede decirse de los efectos de las plataformas de alojamiento en las cadenas hoteleras (o los hoteles familiares), el efecto de las redes sociales en los periódicos y la perturbación provocada por las plataformas de *streaming* en las industrias musical y cinematográfica. En su ausencia, podríamos correr el riesgo de no tener acceso a servicios importantes.

Y más allá de la relación entre las plataformas y los consumidores, las plataformas también podrían depender unas de otras: al igual que muchas empresas emergentes son clientes de otras, la quiebra de una de ellas puede tener consecuencias sistémicas (Wigglesworth, 2021). Los intercambios de criptomonedas son un ejemplo de ello. Un ejemplo extremo es lo que el Financial Times denominó el "complejo financiero Tesla" en referencia a su impacto desproporcionado en el mercado de valores (Greenfield, 2019). Ello describe una "red vasta e interrelacionada de vehículos dependientes de la inversión, simuladores empresariales y un gran mercado de productos derivados de una amplitud, profundidad e hiperactividad sin parangón".

La conclusión es que si queremos desplataformizar y reducir el poder digital, primero debemos desfinanciarizar. El poder digital es el producto de un sistema financiero con características específicas. Sin embargo, disminuir la financiarización es una tarea mucho más difícil. Los cambios fiscales, monetarios y legales que han permitido la financiarización en términos más generales y han alentado flujos de dinero en la industria del capital de riesgo, más específicamente, están vinculados con el deseo más amplio de reactivar el crecimiento en economías estancadas. Limitar estos flujos haría necesario un sistema de crecimiento alternativo creíble. Entonces, ¿qué se puede hacer al respecto?

A pesar de que es un plan ambicioso, en el pasado ya se ha cuestionado el poder de los sistemas financieros establecidos. Más recientemente, y especialmente en relación con la catástrofe climática, el

activismo se ha centrado mucho más en los actores financieros que la han provocado (Buller y Braun, 2021). Estudios realizados por activistas han revelado el modo en que las administradoras de activos como BlackRock, Vanguard y State Street acumularon poder mediante la concentración de acciones (Kruppa y Parkin, 2021). Tan solo BlackRock gestiona 10 billones de dólares. La empresa ha utilizado este dinero para comprar acciones en empresas que cotizan en la bolsa. Por ser accionistas importantes en empresas que abarcan toda la economía, las administradoras de activos como BlackRock han influido en el índice de mercado, al construir una cartera que sigue el rendimiento de grandes partes de la economía. Es decir, cuando el mercado está al alza, la cartera de BlackRock también lo está. Un *efecto secundario* de ello es que BlackRock como accionista tiene poder de decisión respecto de la gobernanza empresarial de un gran número de empresas. Se ha politizado cada vez más el modo en que se utiliza ese poder y para qué fines, ya que las campañas de activistas intentan coaccionar a las administradoras de activos para que asuman la responsabilidad que corresponde a su poder.

Cuestionar el capitalismo de las administradoras de activos es una vía de resistencia contra el sistema de inversiones impulsado por el capital de riesgo. Además de vigilar a los mercados públicos, se debe prestar más atención a lo que está ocurriendo en los mercados privados. Resulta interesante que algunos inversores de capital de riesgo han comenzado a imitar la estrategia de indexación de las grandes administradoras de activos. Por ejemplo, Tiger Global y Vision Fund de Softbank han adquirido acciones en un gran número de empresas privadas (Muoio, 2017). Debido a que los requisitos para la presentación de informes son más flexibles, es más difícil vigilar a los mercados privados. Sin embargo, un esfuerzo concertado para reunir la información disponible al público podría contribuir a conocer mejor el panorama de inversión.

Asimismo, es preciso saber qué inversores institucionales suministran capital al sector del capital de riesgo. Queda mucho por hacer para realizar un relevamiento de esas relaciones y dar seguimiento a la

cadena de inversión de inversores institucionales a fondos de capital de riesgo o empresas emergentes. Algunos inversores institucionales poseen requisitos de presentación de informes públicos, lo cual podría ser una medida inicial que contribuiría a determinar el desempeño financiero real de los fondos de capital de riesgo.

En lugar de responder a las crisis existentes, centrarnos en los actores financieros de las grandes empresas tecnológicas nos permitirá prever los problemas que podrían surgir en el futuro. Si queremos saber qué ocurrirá, debemos analizar qué tipos de fondos están recaudando las empresas de capital de riesgo, cuál es su finalidad y qué empresas se incluyen en las carteras de los fondos de capital de riesgo más exitosos. Ello podría darnos una idea de qué sectores serán los próximos en afrontar presiones y cuáles, debido a su naturaleza, están a punto de experimentar una importante transformación. Por ejemplo, desde hace mucho tiempo se ha intentado que los servicios de oficina formen parte de un sistema laboral de plataforma. Prepararse para los efectos que ello tendría podría permitir a los trabajadores organizarse y prever problemas futuros.

El entorno macroeconómico en constante evolución promete un cambio, aunque es imposible determinar en este momento de qué tipo de cambio se trata. Para desafiar el poder digital hay que comenzar por cambiar el suministro de capital, y este se ve extremadamente afectado por el endurecimiento de la política monetaria. Si bien esto está fuera del control de los activistas, se pueden extraer lecciones históricas de situaciones similares. La molestia de Jack Dorsey por la trayectoria de web3 debería convertirse en el grito de batalla de los activistas. En el deseo de descentralización hay una añoranza de la Internet de los inicios, de restaurar las nobles ambiciones de la web 1.0, antes de la captura empresarial de la web 2.0. Ello tiene un potencial progresista. Entender los incentivos de las empresas de capital de riesgo y los socios limitados de los inversores institucionales puede allanar el camino para cuestionar el poder digital y hacerlo efectivo.

Bibliografía

Agence France-Presse (25 de febrero de 2018). Gobee.bike pulls out of France due to 'mass destruction' of its dockless bike fleet. *The Guardian*.

Bank of England (2022). Quantitative easing. https://www.bankofengland.co.uk/monetary-policy/quantitative-easing

Buller, Adrienne y Braun, Benjamin (7 de septiembre de 2021). Under new management: Share ownership and the growth of UK asset manager capitalism (Finance). *Common Wealth*. https://www.common-wealth.co.uk/reports/under-newmanagement-share-ownership-and-the-growth-of-uk-asset-manager-capitalism

Chen, Andrew (2021). *The cold start problem: How to start and scale network effects*. Nueva York: Harper Business.

Comisión Europea (2017). Un sistema impositivo justo y eficaz en la Unión Europea para el Mercado Único Digital.COM/2017/0547 final.

Crunchbase (2022a). Amazon—Funding, Financials, Valuation & Investors. https://www.crunchbase.com/organization/amazon/company_financials

Crunchbase (2022b). Query Builder . Google Funding Rounds. https://www.crunchbase.com/search/funding_rounds/field/organization.has_investor.reverse/funding_total/google

Crunchbase (2022d). Airbnb—Funding, Financials, Valuation & Investors. https://www.crunchbase.com/organization/airbnb/company_financials

Crunchbase (2022e). Uber—Funding, Financials, Valuation & Investors. https://www.crunchbase.com/organization/uber/company_financials

Davies, Harry et al. (11 de julio de 2022). Uber broke laws, duped police and secretly lobbied governments, leak reveals. *The Guardian*. https://www.theguardian.com/news/2022/jul/10/uber-files-leak-reveals-global-lobbying-campaign

Greenfield, Patrick (2 de octubre de 2019). World's top three asset managers oversee $300bn fossil fuel investments. *The Guardian*. https://www.theguardian.com/environment/2019/oct/12/top-three-asset-managers-fossil-fuelinvestments

Horan, Hubert (2019). Uber's path of destruction. *American Affairs Journal*, 3(2). https://americanaffairsjournal.org/2019/05/ubers-path-of-destruction/

Kruppa, Miles y Parkin, Benjamin (27 de julio de 2021). Tiger Global: the technology investor ruffling Silicon Valley feathers. *Financial Times*. https://www.ft.com/content/54bb342c-230f-4438-a4d7-7cbde010ea1a

Klinge, Tobías J. et al. (2022). Augmenting digital monopolies: A corporate financialization perspective on the rise of Big Tech. *Competition & Change* 10245294221105572. https://doi.org/10.1177/10245294221105573

Lee, Roger (2022). *Layoffs*.fyi. https://layoffs.fyi/

Levingston, Iván (15 de agosto de 2022). Uber raises prices by about 5% in London to attract more drivers. *Bloomberg*. https://www.bloomberg.com/news/articles/2022-08-15/uber-raises-prices-by-about-5-in-london-to-attract-moredrivers

Lunden, Ingrid (2022). Berlin's Gorillas lays off 300, exits four markets. *TechCrunch*.https://techcrunch.com/2022/05/24/berlins-gorillas-lays-off-300-explores-strategic-options-in-4-countries-as-funds-dry-up-for-its-3b-instant-grocery-play/

Muoio, Danielle (2017). The early Uber investor suing Travis Kalanick turned its $12 million investment into $7 billion stake. *Business Insider*. https://www.businessinsider.com/benchmarks-uber-investment-worth-7-billion-2017-8

Nicholas, Tom (2019). *VC: an American history*. Cambridge: Harvard University Press.

StartupRanking (2022c). Facebook Funding Rounds. *Startup Ranking.* https://www.startupranking.com/startup/facebook/funding-rounds

Steinschaden, Jakob (2019). Startups Spend $44b on Google, Facebook and Amazon. Could this be a sign for a new bubble burst? *Trending Topics*. https://www.trendingtopics.eu/startups-spend-44b-on-google-facebook-andamazon-could-this-be-a-sign-for-a-new-bubble-burst/

Summers, Lawrence H. (15 de febrero de 2016). The age of secular stagnation. *Foreign Affairs*. https://www.foreignaffairs.com/articles/united-states/2016-02-15/age-secular-stagnation

Taylor, Alan (22 de marzo de 2018). Bike share oversupply in China: Huge piles of abandoned and broken bicycles. *The Atlantic.* https://www.theatlantic.com/photo/2018/03/bike-share-oversupply-in-china-huge-piles-ofabandoned-and-broken-bicycles/556268/

Teare, Gené (2022). Global Venture Funding And Unicorn Creation In 2021 Shattered All Records. *Crunchbase News*. https://news.crunchbase.com/business/global-vc-funding-unicorns-2021-monthly-recap/

Tech Nation (2021). *The future UK tech built*. Tech Nation Report 2021. https://technation.io/report2021/

Uber Technologies Inc. (2019). Form S-1 Registration Statement. https://www.sec.gov/Archives/edgar/data/1543151/000119312519103850/d647752ds1.htm#toc647752_16

Wayt, Theo (23 de diciembre de 2021). Jack Dorsey blocked on Twitter by Marc Andreessen over 'Web3' heckling. *New York Post*. https://nypost.com/2021/12/23/jack-dorsey-blocked-on-twitter-by-marc-andreesen-over-web3-tiff/

Wigglesworth, R. (23 de noviembre de 2021). The 'Tesla-financial complex': how carmaker gained influence over the markets. *Financial Times*.

La militarización de las grandes empresas tecnológicas

El auge de la industria de defensa de Silicon Valley

Roberto J. González

Traducción al español por Mercedes Camps
Ilustración de Anđela Janković

Las grandes empresas tecnológicas y las fuerzas armadas de los Estados Unidos están cada vez más interrelacionadas como consecuencia de la financiación, los proyectos, la investigación y la infraestructura comunes. Desvincularlas será clave para evitar guerras interminables en el extranjero y el control policial militarizado dentro del país.

En septiembre de 2011, personal de la CIA y las fuerzas armadas de los Estados Unidos, con autorización del entonces Presidente Barack Obama, lanzaron un ataque con drones en Yemen. El clérigo musulmán nacido en los Estados Unidos, Anwar al Awlaki, fue asesinado en el ataque. Quienes organizaron el ataque apuntaron a Awlaki, sobre la base de datos de geolocalización supervisados por la Agencia de Seguridad Nacional como parte de un programa de vigilancia (Scahill y Greenwald 2014). Dos semanas más tarde, otro ciudadano estadounidense fue asesinado en un ataque con drones lanzado por la CIA, en el que se utilizó el mismo tipo de datos: se trataba del hijo de al Awlaki, Abdulrahman al Awlaki, que tenía de 16 años de edad (Friedersdorf, 2012).

Aunque al Awlaki fue asesinado en forma deliberada por fuerzas estadounidenses, otros ciudadanos estadounidenses –y miles de civiles en Afganistán y otros países de Asia Central y Oriente Medio– fueron asesinados por drones en forma accidental (Taylor, 2015). Estos casos presagian un defecto grave en la versión más reciente de la guerra automatizada: la imprecisión de las tecnologías y el enorme margen de error de los nuevos sistemas armamentísticos más sofisticados. En su forma más avanzada, las herramientas computarizadas utilizan inteligencia artificial y aprendizaje automático y pronto podrían tener capacidades autónomas.

Los dispositivos digitales de bolsillo conectados a Internet han transformado a miles de millones de personas de todo el mundo en

máquinas de producción de datos, que transmiten información a cientos o incluso miles de algoritmos al día. Aunque hemos integrado rápidamente a los teléfonos inteligentes y las tabletas en nuestras vidas, no solemos reflexionar sobre la facilidad en que los datos almacenados y transmitidos por estos dispositivos pueden militarizarse. Por ejemplo, informes recientes describen el modo en que la Agencia de Inteligencia de la Defensa de los Estados Unidos, junto con el Departamento de Defensa, utiliza periódicamente datos de geolocalización disponibles comercialmente, que se recopilan a partir de los teléfonos celulares personales, en ocasiones sin órdenes judiciales (Tau, 2021). Las agencias militares y de inteligencia pueden utilizar este tipo de datos no solo para espiar, sino también para reconstruir redes sociales e incluso para lanzar ataques mortales contra personas.

Los drones, los programas informáticos de geolocalización, los programas espía y otras herramientas similares son emblemáticas de una nueva serie de colaboraciones entre las grandes empresas tecnológicas y los organismos de defensa. En los últimos veinte años, el Departamento de Defensa y diecisiete organismos gubernamentales de los Estados Unidos que, en conjunto, son conocidos como la comunidad de inteligencia estadounidense, han intentado captar la innovación tecnológica en su origen: Silicon Valley. Agencias militares y de espionaje lo han logrado mediante la creación de puestos en la costa oeste del país; la organización de una junta asesora de alto perfil que vincula al Pentágono con grandes empresas tecnológicas; la coordinación de cumbres, foros y reuniones privadas con inversores y empresarios influyentes; y apelando al compromiso emocional e intelectual de emprendedores, ingenieros, informáticos e investigadores que, en ocasiones, son escépticos respecto de los burócratas del Gobierno, especialmente los que trabajan en el Departamento de Defensa.

No es posible tener un entendimiento cabal de las fuerzas armadas estadounidenses en la actualidad sin realizar un análisis de su profunda conexión con la industria tecnológica.

Las interconexiones entre los mundos de la tecnología de red y la defensa se remontan a más de cincuenta años atrás. Por ejemplo,

desde comienzos de la década del sesenta, la Agencia de Proyectos de Investigación Avanzada del Departamento de Defensa (DARPA) desempeñó un papel crucial en financiar la investigación en informática que dio lugar a la creación de ARPANET, precursora de Internet. El desarrollo temprano de Silicon Valley fue financiado en gran parte por organismos de defensa y de inteligencia, y el Pentágono tuvo un interés especial en las empresas tecnológicas durante la Guerra Fría (Heinrich, 2002).

¿Qué es la guerra virtual?

La guerra virtual tiene significados diferentes para diferentes personas. No hay una definición acordada –lo cual deja espacio para interpretar el término ampliamente, holísticamente y antropológicamente. Personalmente, tengo una visión amplia, centrada en cuatro elementos diferentes: sistemas robóticos y de armas autónomas; una versión de alta tecnología de operaciones psicológicas; programas de estimulación y modelización predictiva, que algunas personas denominan *contrainsurgencia informática*; y guerra cibernética, es decir, el ataque y la defensa de infraestructuras fundamentales. Estas tecnologías y técnicas se basan en la producción, disponibilidad y análisis de un volumen enorme de datos –a menudo datos de vigilancia– recopilados a partir de drones, satélites, cámaras, teléfonos celulares, transacciones electrónicas, redes sociales, mensajes de correo electrónico y otras fuentes de Internet.

También podemos pensarlo en términos de una guerra por algoritmos. Las tecnologías utilizan cada vez más inteligencia artificial para automatizar procesos de adopción de decisiones. La elaboración de armas virtuales se basa en los esfuerzos combinados de una gran variedad de científicos y expertos técnicos, no solo químicos, físicos, ingenieros, informáticos y analistas de datos, sino también investigadores de biotecnología, politólogos, psicólogos y antropólogos. Gran parte de la labor es banal y tiene lugar en edificios anodinos dentro de

parques de oficinas suburbanos, campus tecnológicos o laboratorios universitarios. Silicon Valley se convirtió en el principal centro para este tipo de trabajo de defensa e inteligencia.

De algún modo, la guerra virtual es una continuación de la denominada *Revolución en Asuntos Militares*, una doctrina elaborada por la Oficina de Evaluación Neta del Pentágono en las décadas del ochenta y del noventa. Se orientaba fundamentalmente a hallar soluciones tecnológicas. Tras los atentados del 11 de septiembre, cuando los Estados Unidos iniciaron la guerra mundial contra el terrorismo y entraron en guerra con redes mundiales de insurgentes con tecnologías relativamente sencillas, como bombas improvisadas, rifles y lanza granadas, la Revolución de Asuntos Militares perdió impulso y la contrainsurgencia se puso de moda tras una larga pausa. Pero en la actualidad, en un periodo marcado por la rápida innovación, los modos de gobernanza algorítmicos y el ascenso al poder de naciones rivales como China y Rusia –que están desarrollando sus propias tecnologías bélicas virtuales– el combate informatizado ha vuelto a ocupar un lugar central entre las élites de las instituciones militares estadounidenses.

La intersección entre las grandes agencias de defensa y las grandes empresas tecnológicas: la creación de DIUx

Mountain View se encuentra entre las montañas boscosas de Santa Cruz y las costas del sur de la Bahía de San Francisco. Durante la primera mitad del siglo XX era una localidad tranquila, donde había explotaciones de ganado, huertas frutales y calles pintorescas. Pero después de que un equipo de científicos, encabezado por William Shockley, inventara el semiconductor allí en 1956, la localidad creció rápidamente junto con el resto de Silicon Valley. Hoy en día es un barrio periférico con más de 80 mil habitantes.

A primera vista, parece extraño que las agencias militares y de inteligencia se instalen allí. Mountain View está a casi 4.000 km de

distancia del Pentágono. Es más cerca viajar de San Francisco a Honolulu que a Washington, D.C.

El Pentágono y Silicon Valley no solo están geográficamente lejos, sino que además hay otras diferencias. El Departamento de Defensa suele considerarse una burocracia inflada, tediosa y derrochadora, con estructuras institucionales jerárquicas y normas de trabajo inflexibles. En cambio, la mayor empleadora de Mountain View, Alphabet, la empresa matriz de Google, es una de las compañías más valiosas del mundo. Su campus de diez hectáreas, conocido como Googleplex, incluye más de treinta cafés, comida y bebida gratuitas para sus empleados, gimnasios y piscinas. Frente al edificio principal se erige el esqueleto de un tiranosaurio rex de tamaño real, que los empleados de Google apodaron Stan, de manera cariñosa.

A pesar de estas diferencias –y como consecuencia de ellas– el Secretario de Defensa durante el Gobierno de Obama, Ash Carter, creó un puesto del Pentágono a menos de 3 km de distancia de Googleplex. La Unidad de Innovación de Defensa (DIU, por sus siglas en inglés), fue creada en agosto de 2015 para identificar rápidamente a empresas que desarrollan tecnologías de vanguardia, que podrían ser útiles para las fuerzas armadas, e invertir en ellas (Kaplan, 2016). Con DIUx, el Pentágono construyó su propia aceleradora de empresas emergentes dedicada a financiar empresas especializadas en inteligencia artificial, sistemas robóticos, análisis de megadatos, ciberseguridad y biotecnología.

La nueva sede de DIUx no estaba tan fuera de lugar. Su sede estaba en un edificio que había sido ocupado por la Guardia Nacional del Ejército, en territorio del Centro de Investigación Ames, la mayor instalación de campo de la NASA, y Moffett Field, que en otra época albergaba al Escuadrón de Rescate número 130 de la Guardia Nacional Aérea de California. Las gigantes de defensa Lockheed Martin y Northrop Grumman tiene oficinas a menos de 3 km de distancia. En 2008, el propio Google estaba ocupando ilegalmente territorio del Gobierno: firmó un contrato de alquiler de cuarenta años con NASA Ames por un nuevo campus de investigación. Luego firmó un acuerdo

de sesenta años con la NASA para alquilar Moffett Field, una superficie de 400 hectáreas, que incluye enormes hangares para dirigibles (Kastrenakes, 2014). Hoy en día, Google utiliza los hangares para construir globos estratosféricos que un día podrían brindar servicios de Internet a personas que viven en zonas rurales (Myrow, 2019), o quizá puedan llevar a cabo misiones de vigilancia militar a gran altitud.

La oficina de DIUx estaba muy cerca de las oficinas de otras empresas tecnológicas: Lab126 de Amazon (donde se crearon Kindle, Amazon Echo y otros dispositivos digitales); la sede de LinkedIn; y el campus de Microsoft en Silicon Valley. Las oficinas de Apple se encuentran a 8km de distancia en la localidad vecina de Cupertino. Las nuevas oficinas del Pentágono estaban literalmente en la intersección de las grandes empresas tecnológicas y las grandes compañías de defensa. La oficina de DIUx, que se encuentra en un edificio de ladrillos ocupado, personificaba las contradicciones de la oficina del Pentágono en el oeste de los Estados Unidos. "Los pasillos son grises, las puertas tienen cerraduras de combinación. Pero dentro del edificio, los recién llegados han renovado sus espacios con pizarrones, pizarras y escritorios colocados en diagonales aleatorias para que estén en armonía con el estilo no jerárquico de una empresa emergente de Silicon Valley", informó un observador (Kaplan, 2016).

El plan de Ash Carter era ambicioso: aprovechar las mentes más brillantes de la industria tecnológica para beneficio del Pentágono. Carter, que es originario de Pennsylvania, trabajó durante varios años en la Universidad de Stanford antes de ser nombrado Secretario de Defensa y quedó impresionado con el espíritu innovador y los magnates millonarios de la Bahía de San Francisco. "Están creando nueva tecnología, prosperidad, conectividad y libertad" afirmó Carter (Hempel, 2015). "Se consideran empleados públicos y quisieran tener a alguien en Washington con quien establecer un contacto". Sorprendentemente, Carter fue el primer Secretario de Defensa que visitó Silicon Valley en más de veinte años.

El Pentágono tiene su propio organismo de investigación y desarrollo (DARPA), pero promueve proyectos que tardarán decenios, no

meses. Carter quería una oficina ágil y optimizada que pudiera servir como una especie de intermediario, que canalizara decenas o cientos de millones de dólares del enorme presupuesto del Departamento de Defensa a empresas prometedoras que desarrollan tecnologías a punto de concluirse. Idealmente, DIUx funcionaría como enlace para negociar las necesidades de generales veteranos de cuatro estrellas, líderes civiles del Pentágono e ingenieros y emprendedores jóvenes. Pronto, DIUx abrió oficinas en otras ciudades con un sector tecnológico pujante: Boston y Austin.

Carter esperaba que, en el corto plazo, DIUx entablaría relaciones con empresas emergentes locales, contrataría personal de alto nivel, contaría con la participación de reservistas del Ejército en proyectos específicos y simplificaría los engorrosos procesos de adquisiciones del Pentágono. Sus objetivos de largo plazo eran aún más ambiciosos: asignar a oficiales militares de carrera a proyectos futuristas en Silicon Valley durante periodos de varios meses, para "exponerlos a nuevas culturas e ideas, que puedan aplicar en el Pentágono e invitar a los expertos informáticos a pasar un tiempo en el Departamento de Defensa" (Hempel, 2015).

En marzo de 2016, Carter organizó la Junta de Innovación de Defensa (DIB), un grupo de especialistas civiles encargado de brindar asesoramiento y recomendaciones a las autoridades del Pentágono (Mehta, 2016). Nombró al ex director ejecutivo de Google y miembro de la junta directiva de Alphabet, Eric Schmidt, para presidir la junta, que incluía a actuales y antiguos ejecutivos de Facebook, Google e Instagram, entre otros.

Tres años después del lanzamiento de DIUx, el organismo fue renombrado Unidad de Innovación de Defensa (DIU), para señalar que ya no estaba en una fase experimental. A pesar de haber atravesado algunas dificultades iniciales, el entonces Subsecretario de Defensa Patrick Shanahan describió a DIUx como "un activo demostradamente valioso". "La organización en sí ya no es experimental", afirmó en 2018 (Mitchell, 2018). "DIU sigue siendo fundamental para fomentar la innovación en todo el Departamento y transformar el modo en que este

construye una fuerza más letal". A comienzos de 2018, el Gobierno de Trump solicitó un aumento considerable del presupuesto de la DIU para el año fiscal 2019, de 30 millones de dólares a 71 millones de dólares (Williams, 2018). Para 2020, el Gobierno solicitó 164 millones de dólares, más del doble de lo que había solicitado el año anterior (Behrens, 2019).

El fondo de capital de riesgo de la CIA

Si bien funcionarios del Pentágono presentaron a la DIUx como una organización pionera, en realidad se inspiró en otra empresa fundada para brindar servicios a la comunidad de inteligencia de los Estados Unidos. A finales de la década del noventa, la CIA creó una entidad sin fines de lucro denominada Peleus, con el fin de capitalizar las innovaciones que se estaban desarrollando en el sector privado, con especial hincapié en Silicon Valley (Reinert, 2013). Poco tiempo después, la organización pasó a llamarse In-Q-Tel.

Su primer presidente, Gilman Louie, describió como la organización fue creada para resolver "el problema de los megadatos":

[Las autoridades de la CIA] temían lo que en el momento denominaron un posible "Pearl Harbor digital"...Cuando ocurrió el ataque a Pearl Harbor, las diferentes partes del Gobierno tenían información parcial, pero no lograron reunirla para concluir que "el ataque a Pearl Harbor es inminente"...En 1998, comenzaron a darse cuenta de que la información estaba aislada en diferentes agencias de inteligencia y que no era posible vincularla...por lo que estaban intentando resolver el problema de los megadatos. ¿Cómo reunir esa información para obtener inteligencia? (Louie,2017).

Al destinar fondos de la CIA a empresas emergentes que desarrollan tecnologías de vigilancia, recopilación de inteligencia, análisis de datos y guerra cibernética, el organismo esperaba obtener una ventaja respecto de sus rivales internacionales al cooptar a ingenieros, *hackers*, científicos y programadores creativos. En 2005, la CIA destinó

alrededor de 37 millones de dólares a In-Q-Tel. En 2014, la financiación anual destinada a la organización aumentó exponencialmente a alrededor de 94 millones de dólares. Ese mismo año, la CIA había realizado 325 inversiones en una serie de empresas tecnológicas (Paletta, 2016).

Si In-Q-Tel suena a algo salido de una película de James Bond es porque la organización (al igual que su nombre) está parcialmente inspirada en la División Q, la oficina ficticia de investigación y desarrollo del servicio secreto británico en las novelas de espionaje de Ian Fleming, popularizada en su exitosa adaptación cinematográfica de Hollywood. In-Q-Tel y DIUx se crearon para transferir tecnologías emergentes del sector privado a agencias militares y de inteligencia de los Estados Unidos, respectivamente. Una interpretación un tanto diferente es que estas organizaciones se crearon para "captar innovaciones tecnológicas...y nuevas ideas" (Cook, 2016). Algunos críticos señalan a In-Q-Tel como un excelente ejemplo de la militarización de la industria tecnológica.

En términos monetarios y tecnológicos, probablemente la inversión más rentable de InQTel haya sido Keyhole, una empresa con sede en San Francisco que desarrolló un programa informático que conectaba imágenes satelitales con fotos aéreas para crear modelos tridimensionales de la superficie de la Tierra. El programa podía básicamente crear un mapa de alta resolución de todo el planeta. In-Q-Tel brindó financiación al programa en 2003 y en unos meses, las fuerzas armadas de los Estados Unidos estaban usando Keyhole para apoyar a los soldados estadounidenses en Irak (Schachtman, 2010).

Fuentes oficiales nunca revelaron cuánto In-Q-Tel había invertido en Keyhole, pero en 2004, Google adquirió la empresa emergente. La renombró Google Earth. La adquisición fue significativa: el periodista Yasha Levine señaló que el acuerdo entre Keyhole y Google "marcó el momento en que la empresa dejó de ser exclusivamente una empresa de Internet dirigida a los consumidores y comenzó a integrarse en el Gobierno de los Estados Unidos" (Levine, 2018). En 2007, Google

estaba intentando obtener contratos con el Gobierno en organismos militares, de inteligencia y civiles (Kehualani Goo y Klein, 2007)

Además de Google, la cartera de In-Q-Tel incluye a empresas con proyectos futuristas como Cyphy, que fabrica drones conectados a Internet que pueden realizar misiones de reconocimiento durante periodos prolongados gracias a una continua fuente de energía; Atlas Wearables, que produce rastreadores de actividad física que monitorizan los movimientos del cuerpo y los signos vitales; Fuel3d, que vende un dispositivo de bolsillo que produce imágenes tridimensionales detalladas de estructuras u objetos; y Sonitus, que ha desarrollado un sistema de comunicaciones inalámbricas, que entra parcialmente en la boca del usuario (Szoldra, 2016). Mientras que DIUx ha apostado a las empresas de robótica e inteligencia artificial, In-Q-Tel ha intentado generar tecnologías de vigilancia –empresas de satélites geoespaciales, sensores avanzados, equipos biométricos, analistas de ADN, dispositivos de lenguaje y traducción y sistemas de ciberdefensa–.

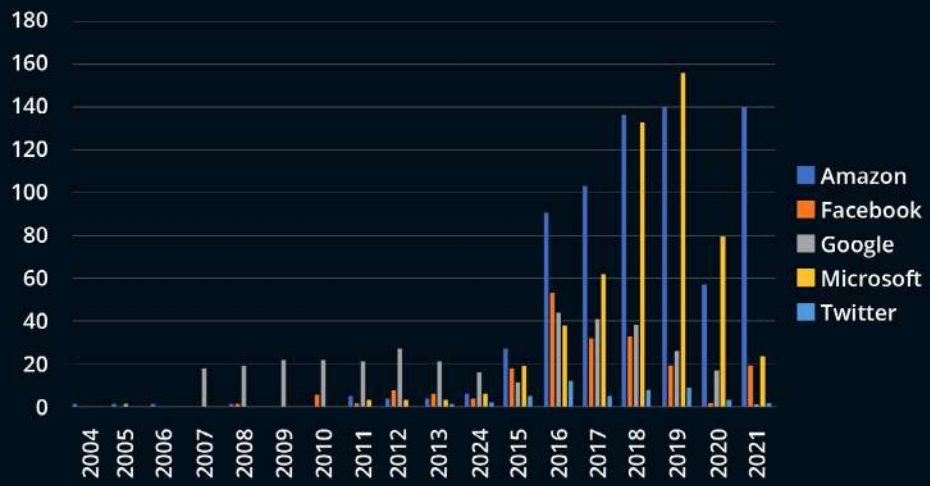
Más recientemente, In-Q-Tel ha comenzado a centrarse en empresas que se especializan en extraer datos de las redes sociales y otras plataformas de Internet. Estas incluyen Dataminr, que transmite datos de Twitter para detectar tendencias y posibles amenazas; Geofeedia, que recopila mensajes de redes sociales indexados geográficamente, vinculados con noticias de último momento, como protestas; y TrasnVoyant, una empresa que recopila datos de satélites, radares, drones y otros sensores (Fang, 2016).

Es probable que algunas personas incluso aplaudan que los organismos militares y de inteligencia de los Estados Unidos hayan contratado a empresas tecnológicas. Habida cuenta del rápido desarrollo y despliegue de sistemas armamentísticos y programas de vigilancia de alta tecnología por países rivales como China –que ha puesto en marcha tecnologías similares contra sus propios ciudadanos en la provincia de Xinjiang (Wang, 2019)–, sus defensores suelen afirmar que las fuerzas armadas de los Estados Unidos no pueden darse el lujo de estar rezagadas en la carrera armamentista de inteligencia artificial.

Pero esos argumentos no tienen en cuenta que la fusión de las grandes empresas de defensa con otra gran industria atará aún más a la economía estadounidense a guerras interminables en el extranjero y al control policial militarizado dentro del país.

CONTRATOS DE GRANDES EMPRESAS TECNOLÓGICAS CON LOS DEPARTAMENTOS DE SEGURIDAD DE LOS ESTADOS UNIDOS

Número total de contratos y subcontratos gubernamentales desde 2004, por empresa tecnológica]



Fuente: Big Tech Sells War, 2022

El Proyecto Maven

Muchas empresas financiadas por In-Q-Tel y DIUx son pequeñas empresas emergentes desesperadas por efectivo. Pero el interés del Pentágono en Silicon Valley también se extiende a las mayores empresas en Internet.

Analicemos el caso del Proyecto Maven, conocido formalmente como el Equipo Interfuncional de Guerra Algorítmica. El Subsecretario de Defensa Robert Work creó el programa en abril de 2017 y lo describió como un intento de "acelerar la integración por el Departamento de Defensa de megadatos y aprendizaje automático y para convertir el enorme volumen de datos disponible en inteligencia y análisis con aplicaciones prácticas" (Work, 2017). El *Boletín de Científicos Atómicos* resume el problema:

Aviones y satélites estadounidenses recopilan más datos brutos de los que el Departamento de Defensa podría analizar incluso si dedicara toda su fuerza de trabajo a ello. Lamentablemente, el análisis de imágenes suele ser una tarea tediosa –implica mirar pantallas para contar automóviles, personas o actividades...la mayoría de los datos de los sensores simplemente desaparecen y nunca se observan–, a pesar de que el Departamento ha contratado a la mayor cantidad posible de analistas durante años (Allen, 2017).

El Pentágono había gastado decenas de miles de millones de dólares en sensores. Crear algoritmos para clasificar y analizar las imágenes tenía sentido desde el punto de vista económico. A un costo previsto de 70 millones de dólares, el Proyecto Maven seguramente pareciera una ganga. La magnitud de la labor era abrumadora. En su estado actual, los sistemas de inteligencia artificial necesitan una gran cantidad de datos para el "aprendizaje profundo", que básicamente significa aprender mediante el ejemplo. En la segunda mitad de 2017, las personas que trabajaban en el Proyecto Maven supuestamente etiquetaron más de 150.000 imágenes visuales para crear los primeros conjuntos de datos con el fin de entrenar a los algoritmos. Las imágenes –fotos de vehículos, personas, objetos y acontecimientos– debían

representar cientos o incluso miles de condiciones variables: diferentes altitudes, ángulos fotográficos, resolución de imagen, condiciones de iluminación, etcétera.

¿Qué organización podía asumir una tarea de esa magnitud? Funcionarios del Pentágono no revelaron qué empresas participaron, pero personal interno dio a entender que actores de importantes empresas tecnológicas estuvieron involucrados (Allen, 2017). El Coronel de la Infantería de Marina, Drew Cukor, que encabezaba el proyecto Maven, observó: "Estamos en una carrera armamentista de inteligencia artificial. Está ocurriendo en la industria y las cinco grandes empresas de Internet están dedicando todos sus recursos a desarrollar esta tecnología". Muchos habrán notado que Eric Schmidt [el entonces director ejecutivo de Alphabet, Inc., la empresa matriz de Google] ahora considera a Google una empresa de inteligencia artificial, no una empresa de datos" (Pellerin, 2017).

Apenas ocho meses después de que el Departamento de Defensa lanzara el Proyecto Maven, las fuerzas armadas estaban utilizando los algoritmos del programa para apoyar misiones con drones contra el ISIS en Irak y Siria.

En marzo de 2018, Gizmodo publicó una serie de artículos de investigación incendiarios, en los que se revelaba que el Pentágono había contratado a Google para trabajar en el Proyecto Maven en septiembre de 2017 (Conger, 2018a). Según correos electrónicos internos de ejecutivos de Google, el contrato era de al menos 15 millones de dólares, y estaba previsto que ascendería a 250 millones de dólares (Statt, 2018).

En algunos correos electrónicos se detallaban reuniones entre ejecutivos de Google y el Subsecretario de Defensa Jack Shanahan (Conger, 2018b). Más de 10 empleados de Google fueron asignados al proyecto y la empresa se había asociado con otras, como DigitalGlobe, una compañía de imágenes geoespaciales, y CrowdFlower, una empresa de colaboración abierta. CrowdFlower (que desde entonces ha cambiado su nombre a Figure Eight) contrató a los denominados "trabajadores colaborativos" –personas que realizan tareas repetitivas

en línea, como identificar fotografías– para que etiquetaran miles de imágenes para el "aprendizaje profundo" algorítmico. Al parecer, estos trabajadores no sabían lo que estaban construyendo ni a quién beneficiaría (Conger, 2018b).

Algunos mensajes internos de Google daban a entender que la empresa tenía aspiraciones de ir más allá de lo que se había sugerido inicialmente en los anuncios del Pentágono. En un correo electrónico se hacía referencia a la creación de un sistema de espionaje "parecido a Google Earth" que diera a los usuarios la posibilidad de "hacer clic en un edificio y ver todo lo que está asociado a él", incluidas personas y vehículos.

A algunos funcionarios de Google les preocupaban las posibles repercusiones públicas de que se filtraba el Proyecto Maven: "Creo que deberíamos realizar una buena campaña de relaciones públicas sobre la colaboración entre el Departamento de Defensa y GCP desde una perspectiva de la tecnología en la nube (almacenamiento, redes, seguridad, etcétera)", escribió Fei-Fei Li, principal científico de inteligencia artificial de Google Cloud, "pero debemos evitar A TODA COSTA mencionar o hacer referencia a la inteligencia artificial" (Conger, 2018c).

Sin embargo, finalmente se filtró la información.

La revuelta de los ingenieros

En febrero de 2018, correos electrónicos internos sobre el Proyecto Maven se circularon ampliamente entre empleados de Google. Muchos de ellos se sorprendieron y alarmaron por lo que habían hecho los principales ejecutivos de la empresa. En unos meses, más de 4.000 investigadores de Google habían firmado una carta dirigida al director ejecutivo de la empresa, Sundar Pichai, para exigir la anulación del contrato del Proyecto Maven. La carta, firmada por varios ingenieros de alto nivel, comenzaba con la siguiente declaración: "Creemos que Google no debería participar en el negocio de la

guerra". También instaba a Google a elaborar "una política clara que establezca que ni Google ni sus contratistas construirían tecnología de guerra". Al final del año, alrededor de una decena de empleados renunció en protesta contra los contratos militares de la empresa y la falta de transparencia de los ejecutivos (Conger, 2018c).

Sorprendentemente, los empleados lograron su objetivo, al menos temporalmente. A principios de junio, Google anunció que la empresa dejaría de trabajar en el Proyecto Maven cuando venciera el contrato. Días más tarde, Google publicó un conjunto de directrices éticas o "principios de inteligencia artificial, en los que se afirmaba que la empresa "no diseñaría ni desplegaría inteligencia artificial" destinada a sistemas armamentísticos para "vigilancia que violara las normas internacionalmente aceptadas" o para tecnologías utilizadas en contravención del derecho internacional y los derechos humanos (Pichar, 2018).[1]

El compromiso de Google de no renovar su contrato con el Proyecto Maven era demasiado bueno para ser cierto. En marzo de 2019, *The Intercept* obtuvo un correo electrónico de Google en el que se señalaba que una empresa tercera seguiría trabajando en el Proyecto Maven utilizando "la Plataforma Google Cloud disponible (un servicio informático básico, en lugar de Cloud AI u otros servicios en la nube) para alivianar parte de la carga de trabajo". Walker añadió que Google estaba trabajando con el "Departamento de Defensa para realizar la transición de conformidad con los principios de inteligencia artificial y los compromisos contractuales" (Fang, 2019).

Otros informes revelaron que el Departamento de Defensa había adjudicado el contrato del Proyecto Maven a Anduril Industries, conocida por haber creado los anteojos de realidad virtual Oculus Rift. El año anterior, Anduril había puesto a prueba un sistema de vigilancia desarrollado para agentes de la Oficina de Aduanas y Protección Fronteriza de los Estados Unidos. El sistema utiliza inteligencia

[1] Pichar, S. (2018.) 'AI at Google: Our Principles', Google Blog [en línea], 7 de junio. https://blog.google/technology/ai/ai-principles/. (Consultado el 10 de diciembre de 2022.)

artificial para detectar la presencia de personas que intentan cruzar la frontera de los Estados Unidos.

Aunque los informes periodísticos daban a entender que Google (y posteriormente Anduril) eran las únicas empresas que habían participado en el Proyecto Maven, la realidad es mucho más compleja y preocupante. Un examen cuidadoso de la organización de investigación sin fines de lucro Tech Inquiry documenta la participación más profunda de numerosos contratistas y subcontratistas.[2] El Pentágono otorgó las "adjudicaciones principales" a ECS Federal y Booz Allen Hamilton, y las "subadjudicaciones" a una serie de empresas, como Microsoft, Clarifai, Rebellion Defense, Cubic Corporation, GATR Technologies, Technical Intelligence Solutions y SAP National Security Services, entre otras. Estos contratos nunca fueron ampliamente publicitados.

Aunque los empleados de Google que se opusieron al Proyecto Maven representaban tan solo un pequeño porcentaje de los 70.000 empleados de la empresa, lograron comenzar la discusión sobre los contratos militares en el sector tecnológico y generaron un debate más amplio sobre la ética en la inteligencia artificial.

La revuelta en Google se amplió a otras grandes empresas tecnológicas e inspiró a otras personas a seguir el ejemplo. En febrero de 2019, más de 200 empleados de Microsoft exigieron que la empresa cancelara un contrato de 480 millones de dólares con el Ejército de los Estados Unidos para abastecer a soldados con más de 100 mil anteojos de realidad aumentada HoloLens. El llamado a licitación del Pentágono establecía que se necesitaba una pantalla montada en la cabeza capaz de dar a los soldados visión nocturna, la búsqueda sigilosa de armas y la capacidad de reconocer amenazas automáticamente. Según el anuncio, idealmente otorgaría a los soldados "mayor letalidad, movilidad y percepción situacional" (Kelly, 2018).

[2] Tech Inquiry (10 de septiembre de2021). Easy as PAI [informe en línea]. https://techinquiry.org/EasyAsPAI/resources/EasyAsPAI.pdf

En una carta abierta al director ejecutivo de Microsoft, Satya Nadella, los trabajadores de la empresa expresaron preocupación de que si HoloLens caía en manos de las fuerzas armadas, podría "diseñarse para ayudar a personas a matar" y "convertiría a la guerra en un videojuego simulado". Los empleados añadieron que "no acordamos trabajar en el desarrollo de armas y exigimos que se tenga en cuenta nuestra opinión con respecto a cómo se utiliza nuestro trabajo" (Lecher, 2019). Los ejecutivos de Microsoft se negaron a anular el contrato. Nadella afirmó: "no vamos a retener tecnología de instituciones que hemos elegido democráticamente para que protejan nuestras libertades" (Riley y Burke, 2019).

A mediados de 2018, alrededor de 450 empleados de la gigante tecnológica Amazon firmaron una carta para exigir a la empresa que dejara de vender Rekognition –un programa de reconocimiento facial– a organismos de orden público (Conger, 2018d). La carta de los empleados también pedía a la división de Servicios Web de Amazon que dejara de alojar a Palantir, una empresa que brindaba programas informáticos de análisis de datos al Servicio de Inmigración y Control de Aduanas de los Estados Unidos, debido a que este organismo deportaba a niños no acompañados y sus familiares. El presidente de Amazon Jeff Bezos hizo caso omiso de la carta de los empleados. "Una de las tareas del equipo de dirección es adoptar la decisión correcta, aunque no sea la más aceptada", dijo en octubre de 2018. "Si las grandes empresas tecnológicas dan la espalda al Departamento de Defensa de los Estados Unidos, este país estará en problemas" (Leskin, 2018).

Cuando los trabajadores del sector tecnológico expresaron renuencia a participar en proyectos militares, los ejecutivos vendieron los productos de la empresa a funcionarios del Pentágono. Microsoft anunció Azure Government Secret, un servicio en la nube para el Departamento de Defensa y clientes de la comunidad de inteligencia, que implicaba "tareas clasificadas secretas de los Estados Unidos" (Keane,2021). Los sitios web de Oracle se jactaron de que sus productos "ayudan a organizaciones militares a mejorar su eficiencia,

preparación y ejecución de misiones".[3] Y Amazon creó un sofisticado video promocional de noventa segundos en agosto de 2018, titulado simplemente "Servicios web de Amazon para el combatiente de guerra".[4]

La oposición a la fusión de las grandes empresas tecnológicas y los grandes organismos de defensa

Las tecnologías de Silicon Valley demuestran las consecuencias impredecibles de desplegar nuevo hardware y software. La idea de que una invención pueda utilizarse tanto para fines pacíficos como militares, es decir, la noción de la tecnología de uso dual, se ha vuelto ampliamente aceptada en la sociedad estadounidense en los últimos 100 años.[5] La historiadora Margaret O'Mara nos recuerda que durante la Guerra Fría, "Silicon Valley construía pequeños dispositivos: microondas y radares para comunicación de alta frecuencia, transistores y circuitos integrados. Silicon Valley construía máquinas miniatura elegantes que podían alimentar misiles y cohetes, pero también podían ser utilizados con fines pacíficos –en relojes, calculadoras, electrodomésticos y computadoras–" (O'Mara, 2018).

Estas tecnologías siguen teniendo aplicaciones de uso dual. Google Earth puede utilizarse para trazar mapas y para la investigación geográfica, pero puede utilizarse también por equipos de las Fuerzas Especiales para atacar redes de electricidad, puentes y otro tipo de infraestructura (Tucker, 2015). En un principio Microsoft comercializó HoloLens como un dispositivo de realidad aumentada para jugadores de videojuegos, artistas y arquitectos, pero el consumidor más redituable probablemente sea la infantería. El programa de reconocimiento

[3] Oracle (2023). Oracle Cloud for the Defense Department. Oracle website. https://www.oracle.com/industries/government/us-defense/

[4] Amazon Web Services (9 de agosto 2018). Amazon Web Services for the Warfighter [video en línea].. https://www.youtube.com/watch?v=HHbBizyTet4

[5] Price, D. dual use.

facial de Amazon puede utilizarse para garantizar la seguridad de transacciones bancarias y de cajeros automáticos, pero también puede utilizarse como tecnología de vigilancia para organismos militares, de inteligencia o del orden público, como el Servicio de Inmigración y Control de Aduanas de los Estados Unidos. Las plataformas en la nube ofrecidas por Amazon, Oracle, Microsoft y Google tienen la capacidad de almacenar datos para investigadores científicos, funcionarios de salud pública y empresas comerciales. Pero también pueden aumentar la letalidad de las fuerzas militares.

Quizá haya quienes digan que los ingenieros y científicos disidentes de Google son ingenuos. ¿No sabían, acaso, en lo que se estaban metiendo? Si los científicos son conscientes de que cuando producen conocimientos probablemente no tienen control de cómo se utilizan esos conocimientos, entonces seguramente sepan que los dispositivos y aplicaciones que estaban creando en algún momento podían ser utilizados como armas. ¿O no?

Es posible que muchos científicos e ingenieros que ahora se oponen al trabajo militar de Silicon Valley nunca habrían imaginado que serían arrastrados al complejo militarindustrial-tecnológico. Quizá incluso decidieron trabajar para empresas tecnológicas porque pensaban que esas empresas no formaban parte del negocio de armas. A fin de cuentas, la carta de los manifestantes a Microsoft dice: "No acordamos trabajar en el desarrollo de armas".

Los investigadores quizá hayan tenido una fe ciega en los ejecutivos de las empresas. Los empleados de Google se sintieron engañados por decisiones secretas que dieron lugar al contrato del Proyecto Maven. Los periodistas suelen reconocer que la empresa tiene la mejor *cultura empresarial* de los Estados Unidos, no solo porque los empleados pueden llevar a sus mascotas al trabajo y tienen acceso a alimentos orgánicos preparados por chefs profesionales, sino también porque su organización tiene una reputación de valorar la colaboración de los empleados.

Cuando el Proyecto Maven salió a luz, la falsa conciencia de los trabajadores tecnológicos comenzó a evaporarse. Cuando se obtiene

un salario de seis dígitos como ingeniero o programador al salir de la universidad, es difícil considerarse proletario, especialmente cuando gozas de los beneficios que ofrece la industria –comidas gourmet gratuitas, gimnasio en la oficina y servicio de guardería gratuito, por nombrar algunos. Para miles de empleados, ser excluidos de las discusiones acerca de si la empresa debería colaborar en el desarrollo de armas de inteligencia artificial despertó un sentido de conciencia de clase latente.

Pero, había otro problema: Las relaciones de larga data de Silicon Valley con el Pentágono. Como explica el presente artículo y como ha observado Margaret O'Mara "Aunque sus empleados no se den cuenta, las gigantes tecnológicas hoy en día contienen algún elemento de la industria de defensa...Ello implica un reconocimiento más cabal de la larga y complicada historia de Silicon Valley y el negocio de la guerra" (O'Mara, 2018).

La separación entre el Pentágono y Silicon Valley es en gran medida un mito, nunca existió realmente, al menos no de manera significativa. Las diferencias son superficiales y estilísticas. Durante la mayor parte de un siglo, la economía y cultura regionales se han visto afectadas por lo que podría denominarse el complejo militar-industrial-universitario. Durante la Guerra Fría, el Pentágono ayudó a construir la industria informática al adjudicar contratos militares en campos como la electrónica de las microondas, la producción de misiles y satélites, y los semiconductores.

El historiador Thomas Heinrich nos recuerda que las representaciones populares de "ingeniosos inventores-empresarios e inversores de capital de riesgo que forjaron una economía dinámica de tecnología avanzada sin la intervención del Gobierno" alejaron la atención del papel fundamental de la "financiación del Pentágono para investigación y desarrollo, que contribuyó a sentar las bases tecnológicas para una nueva generación de empresas emergentes" en el siglo XXI (Heinrich, 2002). Desde la década del cincuenta hasta finales de la década del noventa, el mayor empleador del sector privado de Silicon Valley no era Hewlett Packard, Apple, Ampex o Atari. Era la gigante

de defensa Lockheed. Hoy en día, la región afronta un patrón conocido, aunque el tamaño y la influencia colosales de las empresas tecnológicas actuales eclipsan a las empresas informáticas de antaño.

Posiblemente ello tendrá grandes repercusiones en el futuro cercano. Jack Poulson, un ex científico de alto nivel de Google y cofundador de Tech Inquiry, me lo explicó de la siguiente manera: "Creo que estamos ante la transformación de las principales empresas tecnológicas de los Estados Unidos en contratistas de defensa y me atrevería a vaticinar que en los próximos años adquirirán a contratistas de defensa, algo similar a cuando Amazon compró Raytheon" (Poulson, J., Comunicación personal, 19 de junio de 2019).

La verdadera separación no es entre el Pentágono y Silicon Valley, sino que está en el seno de Silicon Valley, donde un modesto contingente de ingenieros y científicos políticamente comprometidos han ejercido presión en contra de militarizar su trabajo. Pero, ¿bajarán los brazos ante el ataque frontal de relaciones públicas, campañas sensibleras, discusión "colaborativa", más remuneración y privilegios, y quizá la amenaza tácita de perder sus empleos o de que estos sean externalizados?

Es muy pronto para saber lo que sucederá, pero el futuro de la guerra virtual y los campos de batalla digitales posiblemente esté en manos de esos empleados.

Bibliografía

Allen, Gregory C. (21 de diciembre de 2017). Project Maven Brings AI to the Fight against ISIS. Bulletin of the Atomic Scientists. https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/

Amazon Web Services (9 de agosto 2018). Amazon Web Services for the Warfighter [video en línea]. https://www.youtube.com/watch?v=HHbBizyTet4

Behrens, J. (28 de mayo de 2019). FY 20 Budget Request: DOD Science and Technology. *AIP*. https://www.aip.org/fyi/2019/fy20-budget-request-dod-science-and-technology

Conger, Kate (21 de mayo de 2018a). The Pentagon's Controversial Drone AI-Imaging Project Extends beyond Google. *Gizmodo*. https://gizmodo.com/the-pentagons-controversial-drone-ai-imaging-projectex-1826046321

Conger, Kate (1 de junio de 2018b). Google Plans Not to Renew Its Contract for Project Maven. *Gizmod*. https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620

Conger, Kate (14 de mayo de 2018c). Google Employees Resign in Protest against Pentagon Contract. *Gizmodo*. https://gizmodo.com/google-employees-resign-in-protest-against-pentagon-con-1825729300

Conger, Kate (21 de junio de 2018d). Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts with Law Enforcement. *Gizmodo*. https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-facerecognitio-1827037509

Cook, Cynthia R. (23 de noviembre 2016). DIUx: Capturing Technological Innovation. *The RAND Blog*. https://www.rand.org/blog/2016/11/diux-capturing-technological-innovation.html

Fang, Lee (14 de abril de 2016). The CIA Is Investing in Firms that Mine Your Tweets and Instagram Photos. *The Intercept*. https://theintercept.com/2016/04/14/in-undisclosed-cia-investments-social-media-miningglooms-large/

Fang, Lee (9 de marzo de 2019). Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Win Secretive Military AI Contract. *The Intercept*. https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/

Friedersdorf, Conor (24 de octubre de 2012). How Team Obama Justifies the Killing of a 16-Year-Old American. *The Atlantic*. https://www.theatlantic.com/politics/archive/2012/10/how-team-obama-justifies-the-killingof-a-16-year-old-american/264028/

Heinrich, Thomas (2002). Cold War Armory: Military Contracting in Silicon Valley. *Enterprise & Society*, 3(2), 247-284. https://www.jstor.org/stable/23699688

Hempel, Jessi (18 de noviembre de 2015). DOD Head Aston Carter Enlists Silicon Valley to Transform the Military. Wired. https://www.wired.com/2015/11/secretary-of-defense-ashton-carter/

Keane, Tom (16 de Agosto de 2021). Azure Government Top Secret Now Generally Available for US National Security Missions. *Microsoft Azure Blog*. https://azure.microsoft.com/en-us/blog/azure-governmenttop-secret-now-generally-available-for-us-national-security-missions/

Kaplan, Fred (19 de diciembre de 2016). The Pentagon's Innovation Experiment. Technology Review. https://www.technologyreview.com/2016/12/19/155246/the-pentagons-innovation-experiment/

Kastrenakes, Jacob (10 de noviembre de 2014). Google Signs 60-Year Lease on NASA Airfield and Hangars. The Verge. https://www.theverge.com/2014/11/10/7190057/nasa-leases-moffett-airfield-to-google60-years

Kehualani Goo, Sar y Klein, Alan (28 de febrero de 2007). Google Makes Its Pitch to Expand Federal Business. *Washington Post*. https://www.washingtonpost.com/archive/business/2007/02/28/

google-makesits-pitch-to-expand-federal-business/7d045b92-a5bb-44eb-bd6e-c85355210caf/

Kelly, Makena (28 de noviembre de 2018). Microsoft Secures $480 Million HoloLens Contract from US Army. *The Verge*. https://www.theverge.com/2018/11/28/18116939/microsoft-army-hololens-480-millioncontract-magic-leap

Lecher, Colin (22 de febrero de 2019). Microsoft Workers' Letter Demands Company Drop Army HoloLens Contract. *The Verge*. https://www.theverge.com/2019/2/22/18236116/microsoft-hololens-army-contractworkers-letter

Leskin, Paige (6 de noviembre de 2018). Amazon Employees Are Reportedly Gearing Up to Confront CEO Jeff Bezos at an All-Staff Meeting This Week about Selling Facial Recognition Software to Law Enforcement. *Business Insider*. https://www.businessinsider.com/amazon-workers-confront-jeff-bezos-facialrecognition-software-2018-11

Levine, Yasha (2018). Google Earth: How the Tech Giant is Helping the State Spy on Us. *The Guardian*. https://www.theguardian.com/news/2018/dec/20/googles-earth-how-the-tech-giant-ishelping-the-state-spy-on-us

Louie, Gilman (8 de mayo de 2017). Citado en una entrevista con Ernestine Fu en la Universidad de Stanford. https://www.youtube.com/watch?v=DfUm0RxXWxI

Mehta, Aaron (10 de junio de 2016). Carter Names Three to Innovation Board. *Defense News* [en línea], 10 de junio. https://www.defensenews.com/industry/techwatch/2016/06/10/carter-names-three-to-innovation-board/

Mitchell, Billy (9 de agosto de 2018). No Longer an Experiment—DIUx Becomes DIU, Permanent Pentagon Unit. *FedScoop*. https://fedscoop.com/diu-permanent-no-longer-an-experiment/

Myrow, Rachael (11 de abril de 2019). That Giant Structure off 101 once Housed a Flying Aircraft Carrier. *KQED Bay Curious* [podcast]. https://www.kqed.org/news/11738379/that-giant-structure-off-101-once-housed-a-flyingaircraft-carrier

O'Mara, Margaret (26 de octubre de 2018). Silicon Valley Can't Escape the Business of War. *New York Times.* https://www.nytimes.com/2018/10/26/opinion/amazon-bezos-pentagon-hq2.html

Oracle (2023). Oracle Cloud for the Defense Department. *Oracle website.* https://www.oracle.com/industries/government/us-defense/

Paletta, Damian (30 de agosto de 2016). The CIA's Venture-Capital Firm, Like Its Sponsor, Operates in the Shadows. *Wall Street Journal*. https://www.wsj.com/articles/the-cias-venture-capital-firm-like-its-sponsoroperates-in-the-shadows-1472587352

Pellerin, Cheryl (21 de julio de 2017). Project Maven to Deploy Computer Algorithms to War Zone by Year's End. *DOD News*. https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-todeploy-computer-algorithms-to-war-zone-by-years-end/

Pichar, Sundar (7 de junio de 2018). AI at Google: Our Principles. *Google Blog*. https://blog.google/technology/ai/ai-principles/

Reinert, John T. (2013). In-Q-Tel: The Central Intelligence Agency as Venture Capitalist. *Northwestern Journal of International Law & Business*, 33(3), 677-709. https://scholarlycommons.law.northwestern.edu/cgi/ viewcontent.cgi?article=1739&context=njilb

Riley, Charles y Burke, Samuel (25 de febrero de 2019). Microsoft CEO Defends US Military Contract That Some Employees

Say Crosses a Line. *CNN*. https://www.cnn.com/2019/02/25/tech/augmented-realitymicrosoft-us-military/index.html

Schachtman, Noah (18 de julio de 2010). Google, CIA Invest in "Future" of Web Monitoring. *Wired*. https://www.wired.com/2010/07/exclusive-google-cia/

Scahill, Jeremy y Greenwald, Glenn (9 de febrero de 2014). The NSA's Secret Role in the US Assassination Program. *The Intercept*. https://theintercept.com/2014/02/10/the-nsas-secret-role/

Statt, Nick (1 de junio de 2018). Google Reportedly Leaving Project Maven Military AI Program after 2019. *The Verge*. https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contractexpire

Szoldra, Paul (21 de septiembre de 2016). 14 Cutting Edge Firms Funded by the CIA. Business Insider. https://www.businessinsider.com/companies-funded-by-cia-2016-9

Tau, Byron (2021). Military Intelligence Agency Says It Monitored US Cellphone Movements without Warrant. *Wall Street Journal*. https://www.wsj.com/articles/military-intelligence-agencysays-it-monitored-u-s-cellphone-movements-without-warrant-11611350374

Taylor, Adam (23 de abril de 2015). The US Keeps Killing Americans in Drone Strikes, Mostly by Accident. *Washington Post*. https://www.washingtonpost.com/news/worldviews/wp/2015/04/23/the-u-s-keeps-killingamericans-in-drone-strikes-mostly-by-accident/

Tech Inquiry (10 de septiembre de2021). Easy as PAI [informe en línea]. https://techinquiry.org/EasyAsPAI/resources/EasyAsPAI.pdf

Tucker, Patrick (7 de enero de 2015). How US Special Forces Uses Google Maps. *Defense One*. https://www.defenseone.

com/technology/2015/01/how-us-special-forces-uses-google-maps/102396/

Wang, Maya (1 de mayo de 2019). China's Algorithms of Oppression. *Human Rights Watch Report* https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

Williams, Lauren (12 de febrero de 2018). DIUx Gets a Big Boost in FY19 Budget. FCW. https://fcw.com/acquisition/2018/02/diux-gets-a-big-boost-in-fy19-budget/198959/

Work, R.O. (2017). Memorando oficial de los Estados Unidos, 26 de abril. https://www.govexec.com/media/gbc/docs/pdfs_edit/establishment_of_the_awcft_project_maven.pdf

La frontera omnipresente

La infraestructura digital de control migratorio en las Américas

Mizue Aizeki, Laura Bingham y Santiago Narváez

Traducción al español por Nuria del Viso Pabón
Ilustración de Zoran Svilar

See you there.
OK

En 2021, José Eusebio Asegurado, agricultor de El Salvador, fue detenido por la Policía Nacional Civil salvadoreña por «promover la trata de personas». La base de la detención fue un chat de grupo de WhatsApp que Asegurado y otros migrantes utilizaban para coordinar una caravana, en la que se había infiltrado un agente de policía. Según las capturas de pantalla utilizadas para incriminarle, la única participación de Asegurado en el chat fue responder "OK" al mensaje de un migrante que le decía que estaría en un punto de encuentro sobre las cinco. La policía detuvo a Asegurado en el punto de encuentro, diciéndole que estaba "fichado" como organizador de la caravana (Cáceres y Gressier, 2021).

El mismo día, la policía salvadoreña también acusó a Fátima Pérez, cocinera, y a Juan Rufino Ramírez, guardia de seguridad privada, de promover la "trata de personas" basándose en los mensajes de un grupo de WhatsApp que habían creado para coordinar una caravana. En las capturas de pantalla del caso de Ramírez se le ve dando instrucciones al grupo de 55 miembros para reunirse en la estación de autobuses, así como los precios de los billetes a Guatemala. La policía detuvo a Ramírez y a Pérez la mañana en que planeaban partir.

Estas tres detenciones se produjeron en un lapso de cuatro horas. La entonces embajadora de Estados Unidos en El Salvador, Katherine Dueholm, felicitó rápidamente a la Fiscalía General y declaró: "Aplaudo a las autoridades salvadoreñas que están tomando medidas contra aquellos que quieren engañar a la ciudadanía con caravanas y falsas promesas. Solo promueven #UnViajeEnVano" (Johnson, 2021).

Las detenciones y los elogios de la embajadora Dueholm reflejan el papel fundamental que desempeñan la vigilancia encubierta y las tecnologías *inteligentes* basadas en datos en las prácticas estadounidenses de control migratorio que operan en países situados fuera de Estados

Unidos. En los últimos veinte años, Estados Unidos (y otros países ricos) han hecho grandes esfuerzos por externalizar los regímenes de control de fronteras más allá de su propio territorio. Esto implica a menudo la participación efectiva de organismos de otros países en la vigilancia, el control policial y la exclusión de los inmigrantes.

Sin embargo, la nueva infraestructura digital que permite la externalización de las fronteras es poco conocida. Esta infraestructura digital se basa tanto en la tecnología de grado militar construida por los principales fabricantes de armas como en la innovación de Silicon Valley: bases de datos interoperables que comparten huellas dactilares sin problemas entre los organismos policiales a través de las fronteras; dispositivos de recogida biométrica utilizados por las autoridades de detención mexicanas para rastrear a los migrantes para la Oficina de Aduanas y Protección Fronteriza de Estados Unidos (CBP); aplicaciones de medios sociales que sirven como redes de comunicación críticas para los migrantes y herramientas de vigilancia para la policía; sistemas de identificación digital que permiten el acceso a los servicios esenciales, pero también como dispositivos de seguimiento.

Las infraestructuras –digitales o materiales– tienen un verdadero poder de adhesión; de eso se trata. Una vez que una autopista parte una comunidad por la mitad, una nueva permanencia sofoca el estruendo de las protestas y la gente sigue adelante. Utilizamos el término *infraestructura digital* para describir el establecimiento de una base que será fundamental para la forma en que las potencias mundiales practicarán el control de la migración; y, a medida que se implante, cada vez más allá del desafío: una intervención estratégica unificada de los países poderosos, con Estados Unidos en la vanguardia. Aunque pueda parecer un experimento tecnológico (como los perros-robot dotados de inteligencia artificial en la frontera) o una captura de datos puntual y oportunista (como las redes de acuerdos internacionales de intercambio de datos), el crecimiento de la infraestructura fronteriza digital es *por diseño*. Esto es posible gracias a las tecnologías digitales integradas que se asientan en el tipo de permanencia rígida y *sin motivo* que se concede a otras infraestructuras, como los cables

de comunicaciones submarinos, los protocolos y los servidores que hacen funcionar Internet, una red eléctrica o una superautopista (De Goede y Westermeier, 2022).

Las profundas implicaciones de las nuevas infraestructuras persisten mucho tiempo después de su creación, como es el caso de la infraestructura digital desplegada para vigilar a los inmigrantes en el llamado *patio trasero* de Estados Unidos. Con frecuencia, sus repercusiones resultan invisibles. Los gobiernos promueven las tecnologías de vigilancia fronteriza como fundamentalmente seguras, humanas y no violentas, mientras que los defensores de los inmigrantes luchan por hacer visible la violencia al otro lado de estos *circuitos fronterizos* invisibles.[1]

Las implicaciones van desde la violencia desencadenada digitalmente y los asesinatos cometidos por la policía local en Centroamérica hasta las acciones de Estados Unidos, sus aliados y competidores en las contiendas geopolíticas por el control de la seguridad mundial. El gobierno estadounidense y la industria privada se han embarcado en un frenesí empresarial, en gran medida encubierto, para poseer y controlar la interfaz de vigilancia de la migración del futuro. Las capacidades de vigilancia y control –una parte rutinaria y de larga data de los paquetes de ayuda de Estados Unidos para luchar contra el crimen organizado– amplían el espionaje interno de los gobiernos socios para sus propios fines y sirven a los intereses de externalización fronteriza de Estados Unidos en el control del movimiento de personas y su desvío fuera de la frontera territorial estadounidense.

Este ensayo se centra principalmente en cómo la infraestructura digital sirve a los intereses estadounidenses. ¿Qué sabemos sobre esta estrategia y cómo está afectando ya a la movilidad y los derechos humanos en la región? ¿cuáles son sus fundamentos históricos? ¿qué

[1] Ver Muñiz, Ana (2022). *Borderland Circuitry: Immigration surveillance in the United States and beyond*. Oakland: University of California Press; ver también Mijente, Immigrant Defense Project, NIPNLG (2018). Who's behind ICE. https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling- Deportations_v4.pdf

retos nos aguardan? Es imposible responder a estas preguntas simplemente diseccionando la crudeza o la procedencia de una única tecnología, sistema o actor. Primero tenemos que entender las motivaciones transnacionales que impulsan estas dinámicas en ascenso, más observables, sobre el terreno. En otras palabras, debemos hacer visible la infraestructura digital invisible.

La infraestructura digital es clave para la externalización de fronteras y el aumento de la violencia irresponsable

Entender la externalización de las fronteras a través de la lente de la infraestructura digital capta la verdadera escala de las prácticas fronterizas previstas por Estados Unidos (y sus competidores y aliados), así como su permanencia prevista en el futuro orden mundial. La infraestructura fronteriza digital se alimenta de historias de dominación, control y atrocidades en nombre de proyectos transnacionales de *lucha contra el crimen*, preparando el terreno para unos elevados costes sociales.

En primer lugar, en lo que respecta a la escala, estamos asistiendo a una escalada del imperialismo fronterizo estadounidense y de la violencia en las fronteras, tanto en términos de alcance geográfico en territorios nacionales como de la ampliación de la *capacidad policial* a un número cada vez mayor de individuos y grupos a través de esta infraestructura digital.[2] Esto incluye a cualquier persona que un

[2] Esta lente también nos permite hacer hincapié en la conexión con antecedentes históricos como los proyectos de *modernización* de las infraestructuras físicas de tránsito y comercio, donde el vínculo con la violencia estatal es indiscutible (por ejemplo, los proyectos de construcción de ferrocarriles y el genocidio de los pueblos indígenas en Sonora entre 1880 y 1900). Ver Guidotti-Hernández, N. (2011). *Unspeakable Violence: remapping U.S. and Mexican national imaginaries*. Londres: Duke University Press. Insistimos en que esta escala no se aleja de las lógicas racializadas que han definido las prácticas fronterizas en esta región durante décadas. Ver Rosas, G. (2006). The managed violences of the borderlands: treacherous geographies, policeability, and the politics of race. *Latino Studies*, 4(4), 401–418. https://doi.org/10.1057/palgrave. lst.8600221

algoritmo considere *peligrosa*, a quienes puedan emigrar, así como a los agentes humanitarios, los grupos de defensa de los inmigrantes y las organizaciones de ayuda. La escalabilidad y el rápido crecimiento que engendra es una propiedad por excelencia de las tecnologías digitales, independientemente de su origen o aplicación. Los desplazamientos hacia nuevos objetivos en el marco de la infraestructura digital carecen de fricciones en comparación con las anteriores tácticas analógicas de vigilancia fronteriza. Asegurado, el agricultor que ayudaba a los inmigrantes en El Salvador, se vio envuelto en la red de externalización fronteriza de Estados Unidos con un simple "OK" en un chat de WhatsApp.

En segundo lugar, en cuanto a la permanencia, los defensores de las fronteras digitales en las capitales nacionales, la industria y las agencias de desarrollo adoptan el término *infraestructura pública digital* como una marca, para otorgar confianza (no merecida), normalización y la inevitabilidad de herramientas digitales cuestionadas como las identificaciones biométricas y los sistemas de pago.[3] Ceder el privilegio de definir la *infraestructura digital* a actores con intereses creados en las actuales prácticas de control de la migración es imprudente. Sin una contranarrativa que articule su disposición violenta, las herramientas digitales de externalización de fronteras –incluida la recogida generalizada de datos biométricos, la recopilación de datos de transacciones en tiempo real en los sistemas de pago y la confiscación de

[3] Ver, por ejemplo, Shivkumar, G., O'Neil, K. y Nordhaug, L. (30 agosto de 2021). How to bring digital inclusion to the people who need it most. https://www.weforum.org/agenda/2021/08/4-reasons-you-should-care-about- digital-public-infrastructure/ ("[Digital Public Infrastructure (DPI)] se refiere a soluciones digitales que permiten funciones básicas esenciales para la prestación de servicios públicos y privados, es decir, colaboración, comercio y gobernanza. Piénsese en nuestras actuales infraestructuras públicas compartidas, como carreteras y educación, pero en línea: eso es la DPI en pocas palabras"; Masiero, Silvia y Arvidsson, Viktor (2021). Degenerative outcomes of digital identity platforms for development. *Information Systems Journal*, 31(6), 903–928. https://doi.org/10.1111/isj.12351; Massally, K. y Frankenhauser, C. (3 agosto de 2022). The right way to build digital public infrastructure: 5 insights. https://www.weforum.org/ agenda/2022/08/digital-public-infrastructure/

teléfonos inteligentes en la frontera– pueden normalizarse fácilmente como *infraestructura pública digital*, en lugar de resistirse a ellas.

La escala y el impacto duradero del rápido endurecimiento de la infraestructura digital que alimenta la externalización fronteriza exigen una coordinación transnacional urgente. Como escritores y activistas, nos hemos unido para resistir el uso de la infraestructura digital en la política estadounidense de control migratorio en México, Centroamérica, Sudamérica y el Caribe. Solo tenemos rastros y no la imagen completa. Basándonos en el trabajo de otros, entretejemos todo esto para mostrar cómo la fusión del poder estatal y digital para construir una infraestructura fronteriza digital no es ni humana ni segura: más bien, está incrementando formas de violencia irresponsables.

Convergencia: guerra contra las drogas, externalización de fronteras, infraestructura digital y militarización de las regiones vecinas de EE.UU.

Desde la década del setenta, las iniciativas económicas y políticas han impulsado sin tregua las inversiones estadounidenses en prácticas de control de la inmigración más militarizadas, criminalizadoras y digitalizadas. Desde el 11 de septiembre, la convergencia estadounidense de la *seguridad nacional* con la migración no autorizada ha impulsado un régimen de externalización de fronteras cada vez más amplio –actualmente hay 23 oficinas de la CBP y 48 oficinas del ICE en todo el mundo–(Aizeki et al., 2021) y, en consecuencia, ha proporcionado un mercado especialmente lucrativo para las empresas de vigilancia digital.[4] A través de programas como la Iniciativa Mérida y la Iniciativa de Seguridad Regional Centroamericana, Estados Unidos ha vinculado

[4] Andersson, Ruben (2018). *Illegality, Inc.: clandestine migration and the business of bordering Europe*. Oakland: University of California Press; Miller, Todd (2019). *Empire of Borders: The Expansion of the U.S. Border around the World*. Londres, Nueva York: Verso..; Akkerman, Mark (2021). *Border Wars*. Amsterdam: Transnational Institute

la ayuda a países como México, El Salvador, Guatemala y Honduras al aumento de la militarización, la vigilancia policial, el encarcelamiento y el control de la migración.

Sin embargo, los patrones migratorios hacia Estados Unidos desde México, América Central y el Caribe no pueden disociarse de las prácticas y políticas que Estados Unidos ha empleado durante más de un siglo para dominar a los países de estas regiones. Décadas de prácticas y políticas estadounidenses han alimentado la inestabilidad económica, política y medioambiental, factores clave que impulsan la migración a Estados Unidos. En los últimos veinte años, el número de personas que emigran desde Centroamérica se ha más que duplicado, y los mayores aumentos se han producido en Guatemala, Honduras y México. La *guerra contra el narcotráfico* respaldada por Estados Unidos en México y Centroamérica ha aumentado drásticamente la violencia y la inestabilidad (Paley, 2014). En México, la lucha contra el crimen organizado ha provocado 350 mil muertes y más de 72 mil desapariciones entre 2006 y 2021. Según el Banco Mundial, el 60 % de la población rural centroamericana vive en la pobreza. Aunque los mayores contribuyentes a la crisis climática son los países ricos, estas poblaciones ya empobrecidas sufren los impactos más agudos del cambio climático. Durante décadas, las sequías prolongadas junto con catástrofes naturales como huracanes e inundaciones han afectado profundamente a Centroamérica. El número de personas que se enfrentan la inseguridad alimentaria se triplicó entre 2019 y 2021, afectando a 6,4 millones de personas. Asegurado, Pérez y Ramírez –como muchos otros– buscan alternativas a esta situación intolerable.

En lugar de reconocer estas causas subyacentes, la respuesta de Estados Unidos ha sido ampliar aún más su frontera. El general John Kelly, ex secretario del Departamento de Seguridad Nacional de Estados Unidos (DHS), declaró: "Creo que la defensa de la frontera suroeste comienza a 1.500 millas al sur". México ha sido durante mucho tiempo fundamental en el régimen de externalización de fronteras de EE.UU., y la infraestructura digital desempeña un papel cada vez más crítico. Tony Crowder, ex director de Operaciones Aéreas y Marítimas

de la CBP, compartía la opinión de Kelly: «Hemos enseñado a pescar a los mexicanos... [pero] aunque tenemos toda esta capacidad de vigilancia, no tenemos suficiente, necesitamos más" (Miller, 2019).

Aunque forma parte de los esfuerzos continuados de Estados Unidos por reclutar a México en apoyo de sus objetivos regionales, esta *asociación para la seguridad y el Estado de derecho* se aceleró tras el 11 de septiembre. En 2007, Estados Unidos desplazó el foco de su guerra contra las drogas de Colombia a México, América Central y el Caribe. En este marco de securitización, la guerra contra las drogas se fusionó con el régimen de control de la inmigración. En 2008, se puso en marcha la Iniciativa Mérida, una asociación bilateral entre Estados Unidos y México en nombre de la guerra estadounidense contra las drogas. Inicialmente proporcionó financiación para que México adquiriera equipamiento para sus fuerzas militares y policiales y para la recopilación de información de inteligencia. En 2013, Mérida fue renovada para incluir cuatro pilares, incorporando la creación de una "frontera estadounidense-mexicana del siglo XXI, mejorando al mismo tiempo la aplicación de las leyes de inmigración en México y la seguridad a lo largo de las fronteras meridionales de México". Desde 2008, unos 3.500 millones de dólares, prolongación de la política estadounidense, han contribuido a dar forma a la agenda de control migratorio de México.

En 2014, el Programa Frontera Sur reforzó aún más la seguridad de la frontera sur de México mediante el aumento de la policía de migración y el aparato de deportación. En consecuencia, México cuenta ahora con uno de los mayores sistemas de detención de inmigrantes del mundo. Entre 2014 y 2017, México deportó a más centroamericanos que la Patrulla Fronteriza de Estados Unidos. Doris Meissner, ex comisionada del Servicio de Inmigración y Naturalización (INS, el predecesor de ICE y CBP), subrayó la importancia del control migratorio mexicano, explicando en 2017 la necesidad de examinar tanto los datos estadounidenses como los mexicanos para evaluar la eficacia de la aplicación de la ley en la frontera estadounidense (Miller, 2019, p. 177).

En el marco de estos acuerdos, el Departamento de Defensa de EE.UU. ha proporcionado formación y ha vendido millones en equipamiento militar a México, incluida una serie de tecnologías de *fronteras inteligentes* proporcionadas por empresas como Dev Technology, General Dynamics, Amazon Web Services y NEC.[5] Un elemento clave del apoyo de EE.UU. a México ha sido el desarrollo de una infraestructura para recopilar y compartir datos –como información biométrica y biográfica, y antecedentes penales– de forma que interactúe sin problemas con las bases de datos estadounidenses.

La infraestructura digital que rastrea y cataloga a los migrantes es fundamental para la política migratoria estadounidense en México. La estrategia del Instituto Nacional de Migración (INM), respaldada por Estados Unidos, se basa en esta infraestructura como principal medio para controlar la migración en lugar de sellar la frontera sur de México con Guatemala. La recogida de datos biométricos es esencial para que los migrantes sean más legibles para el Estado. En 2011, Estados Unidos proporcionó cuatro quioscos biométricos a la frontera sur de México, y 117 escáneres biométricos adicionales al año siguiente. Entre 2018 y la primera mitad de 2022, el gobierno mexicano recopiló y compartió información sobre más de 360 mil migrantes en centros de detención.[6] La información de la CBP revela que las autoridades mexicanas compartieron información de 10 mil solicitudes de visado humanitario ante el DHS. La liberación de aproximadamente 1.800 migrantes no registrados de un albergue en Piedras Negras estaba condicionada al registro de sus datos.[7]

Un "entorno de intercambio de información" que incluya sistemas interoperativos de intercambio de datos es fundamental para lograr

[5] Immigrant Defense Project, Mijente, y NIPNLG (2018). Who's Behind ICE: The Tech and Data Companies Fueling Deportations. https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data- Companies-Fueling-Deportations_v4.pdf

[6] Ver FOIA: https://www.foia.gov/

[7] Watch CBP Intel (2019). Central American Caravans and Migration Crisis Flow - Update 32. *U.S. Customs and Border Protection.* https://r3d.mx/wp-content/uploads/Central-American-Caravans-and-Migration-Crisis-Flow- Update-32.pdf.

los objetivos del Estado de seguridad nacional (Meissner et al., 2013). La *interoperabilidad* permite una conectividad sin fisuras entre la policía, las agencias de inmigración, los gobiernos extranjeros, etc.[8] Las principales formas de la infraestructura digital iniciada por Estados Unidos se basan en la recopilación generalizada de información y el intercambio sin fisuras de datos para la vigilancia a través de las fronteras.

Este enorme volumen de recopilación e intercambio de datos se ha visto impulsado por el despliegue del poder del Estado carcelario –incluida la centralidad del "extranjero delincuente", el "miembro de una banda" y el "narcotraficante" como amenazas para la seguridad nacional– en todos los niveles geográficos del régimen estadounidense de control de inmigrantes. Por ejemplo, el Programa de Alerta Migratoria Transnacional de Identificación Biométrica (BITMAP) permite al DHS y a sus países socios saber dónde y cuándo llega una persona al hemisferio occidental y sus pautas de viaje antes de que llegue a la frontera suroeste de Estados Unidos. El BITMAP está desplegado actualmente en 18 países, incluido México. El DHS también cuenta con un programa de intercambio de información sobre antecedentes penales (CHIS) que permite compartir a escala mundial información biográfica, biométrica y descriptiva sobre las personas expulsadas de Estados Unidos (por ejemplo, presuntos antecedentes de inmigración, laborales, familiares y penales).

La criminalización estructural de la pobreza en ambos países se amplifica con el CHIS. Según la Encuesta Nacional de Población Privada de la Libertad en México, realizada por el Instituto Nacional de Geografía y Estadística (INEGI) en 2021, casi el 44 % de los encuestados declaró haber sido encarcelado por acusaciones o incriminaciones falsas. El 42 % afirmó haber sido obligado a declararse culpable o a incriminar a otra persona. Casi la mitad de las personas encarceladas

[8] Ver Woodward, John (2005). Using biometrics to achieve identity dominance in the Global War on Terrorism. *Military Review*; ver también Jacobsen, Annie (2021). *First Platoon: a story of modern war in the age of identity dominance*. Nueva York: Dutton.

no han sido condenadas (Angel, 2020), y casi la mitad de las condenas son por robos de menos de 100 dólares (Romero, 2014). Este es el tipo de datos que alimenta CHIS.

En otro ejemplo, el DHS está desarrollando el Sistema Avanzado de Tecnología de Reconocimiento Nacional (HART, por sus siglas en inglés) para sustituir a su actual base de datos biométricos centralizada, IDENT, mediante un contrato con Peraton (filial de Veritas Capital, una empresa de capital riesgo). Alojado en Amazon Web Services, HART permitirá al DHS agregar y comparar datos biográficos y biométricos de cientos de millones de personas en todo el mundo. Esto incluye los denominados datos de identificación procedentes de identificaciones policiales, reconocimiento facial, ADN, escáneres de iris e impresiones de voz, normalmente recopilados sin el conocimiento o consentimiento de la persona. La enorme base de datos HART se basa en la recopilación generalizada de datos biométricos en todos los ámbitos, por ejemplo, el desarrollo de bases de datos de ADN integradas en México y Centroamérica por parte del Departamento de Estado de EE.UU. en nombre de la lucha contra el tráfico de personas o la propuesta de un documento de identificación digital biométrica nacional en México. De este modo, se fusionan múltiples iniciativas estatales y crece exponencialmente el poder del Estado para vigilar, rastrear y controlar a los migrantes y a todas las personas bajo su vigilancia.

Aunque la Iniciativa Mérida terminó formalmente en 2019, su enfoque ha sido sostenido por el gobierno mexicano. En 2021, el gobierno mexicano aumentó el ejército en un 46 % y la Guardia Nacional dedicada a detener migrantes en un 300 %. En julio de 2022, el presidente López Obrador comprometió 1.500 millones de dólares en infraestructura fronteriza inteligente durante los próximos dos años.

Para los estados socios de EE.UU., cualquier canal tecnológico y de intercambio de datos que se financie y se exporte a ellos se convierte en un activo, no solo para vigilar a los migrantes, sino para impulsar múltiples agendas de construcción de poder coercitivo. Por tanto, esta infraestructura puede acabar alimentando la violencia

y la criminalización, socavando el derecho de asilo, exacerbando la desigualdad y ampliando el poder de los paramilitares y la policía, al tiempo que privilegia las prerrogativas corporativas y neoliberales securitizadas.

La naturaleza geopolítica de la infraestructura digital

En su investigación sobre los sistemas de pago digitales, Marieke de Goede y Carola Westermeier utilizan el término *geopolítica de infraestructuras* para subrayar la creciente centralidad de las infraestructuras en la geopolítica y el modo en que el poder económico estadounidense está arraigado en las infraestructuras financieras (que, como el control de la migración, se están digitalizando rápidamente) (De Goede y Westermeier, 2022).

La red mundial de mensajería financiera SWIFT es un ejemplo de infraestructura invisible para la mayoría de la gente y que, sin embargo, desempeña un papel fundamental, como describen los autores, en el refuerzo de las relaciones de poder del orden mundial de posguerra en el que surgió. Setenta años después de la Segunda Guerra Mundial y cincuenta desde la creación de SWIFT, las rutas de mensajería bancaria fluyen a través de antiguas capitales coloniales y se sitúan en un *núcleo* de países occidentales, dejando grandes franjas de América Latina, África y Oriente Medio en una periferia económica permanente, pero efectivamente invisible. Del mismo modo, las identificaciones digitales, el seguimiento y la infiltración en las redes sociales y las plataformas de intercambio de datos son esencialmente componentes, nodos o capas parcialmente visibles de proyectos de infraestructura digital geoestratégica más profundos y a más largo plazo.

La ampliación de las fronteras mediante infraestructuras digitales sirve a objetivos políticos y económicos de Estados Unidos que van mucho más allá de la vigilancia de la movilidad humana. La lucha geopolítica por el control de las infraestructuras se desarrolla en varios ámbitos. Los organismos militares codician el *dominio de la identidad*,

un objetivo que llevó a las fuerzas estadounidenses a recopilar almacenes masivos de datos biométricos en Afganistán e Irak como arma de guerra.[9] Los gigantes estadounidenses de los servicios digitales como Amazon y Google dominaron la *plataformización* construyendo infraestructuras de comercio electrónico (publicidad digital, búsquedas, redes sociales, etc.) para dominar la economía digital. A menudo convergen los intereses de los sectores público y privado, incluso en forma de asociaciones público-privadas (APP) para construir infraestructuras. En cada caso, la verdadera pugna entre estados y gigantes corporativos se centra en el control de la interfaz, o de los métodos infraestructurales más esenciales e invisibles de comunicación y control digitales. Como explica Michael Kwet, "las corporaciones transnacionales de las 'grandes tecnologías' con sede en Estados Unidos han amasado billones de dólares y han adquirido poderes desmesurados para controlarlo todo, desde los negocios y el trabajo hasta los medios sociales y el entretenimiento en el Sur Global. El colonialismo digital se está extendiendo por todo el mundo" (Kwet, 2021). La búsqueda de Estados Unidos de la dominación a través de infraestructuras externalizadas de vigilancia de la migración va de la mano de sus designios geopolíticos y corporativos de poder económico.

Estas formas de poder digital a través de las infraestructuras plantean retos únicos para la documentación y, en última instancia, para cualquier forma de cambio sistémico. Los retos incluyen líneas borrosas de responsabilidad, misión y función; los gobiernos y los actores corporativos son vistos o presentados como conductos pasivos o intermediarios en la infraestructura pública digital; y las infraestructuras pueden aparecer fácilmente como *ahist*óricas y sin motivación. En México y Centroamérica, el control de la migración converge con las operaciones policiales exteriores de Estados Unidos (como la guerra contra las drogas y las guerras entre bandas). Exploramos los diversos

[9] Ver Woodward, John (2005). Using biometrics to achieve identity dominance in the Global War on Terrorism. *Military Review.* https://www.rand.org/pubs/reprints/RP1194.html; ver también Jacobsen, 2021.

efectos simultáneos de esta compleja fusión: el giro hacia la infraestructura digital; su relación con la violencia y el sufrimiento humano; y su exclusión de la rendición de cuentas por estos daños.

Infraestructura digital de fronteras en su teléfono: las técnicas policiales de las Tecnologías de la Información y la Comunicación (TIC) en las rutas migratorias

La infraestructura de vigilancia es tangible en los centros físicos de detención de inmigrantes y en las detenciones policiales, con fichas policiales, frotis de mejillas y confiscación del teléfono móvil del detenido, entre otras. La creciente integración de la vida cotidiana, las telecomunicaciones y la informática abre amplias vías para una vigilancia más encubierta y oportunista de las comunicaciones y actividades privadas de los usuarios que recurren a las redes sociales, las comunicaciones móviles y las aplicaciones de mensajería. La vigilancia de los teléfonos móviles y las redes sociales abarca desde la obligación de revelar información para solicitar visados y prestaciones sociales hasta la elaboración de listas y el seguimiento por parte del gobierno de manifestantes y otros actores *indeseables*. La vigilancia de los migrantes está inmersa en estos sistemas de control, en los que la tecnología de vigilancia sirve de herramienta silenciosa para la violencia y la represión gubernamentales.

Esto ha repercutido en la forma en que los migrantes viajan y se mantienen a salvo, por ejemplo, mediante la seguridad en el número. Viajar en caravana se ha convertido, por tanto, en una estrategia tanto de supervivencia como de protesta: fuentes de seguridad tanto física como económica y de oposición a las políticas económicas que contribuyeron a su desplazamiento. Las redes sociales y las aplicaciones de mensajería son herramientas clave para la coordinación de las caravanas y para los migrantes en general. Los migrantes utilizan estas herramientas para identificar rutas, buscar refugio y alimentos, comunicarse con sus redes de apoyo, avisarse mutuamente de los riesgos y

coordinar los viajes. Tanto los gobiernos como la delincuencia organizada entienden esta dinámica y utilizan estas mismas herramientas para vigilar y extorsionar a los migrantes.

El 5 de junio de 2019, Irineo Mújica, de Sin Fronteras –una organización de la sociedad civil dedicada a la protección de los derechos humanos de los migrantes en México y Estados Unidos, y que ha apoyado a múltiples caravanas de migrantes– fue detenido en México, acusado falsamente de tráfico de personas. Mújica apareció en la base de datos de la lista de vigilancia de la CBP publicada en 2019 que contenía fotos, nombres, profesiones y otros detalles de periodistas, activistas y personas influyentes en las redes sociales, tanto de México como de Estados Unidos, con vínculos con la caravana de migrantes.

Un informe de la Oficina del Inspector General (OIG) del DHS sobre la base de datos y otras prácticas de vigilancia descubrió que la CBP estableció alertas electrónicas (vigías) sobre periodistas, abogados y defensores que estaban conectados a través de las redes sociales con las caravanas de migrantes.[10] Las personas etiquetadas por los vigías eran constantemente marcadas para un control secundario al entrar en Estados Unidos, e interrogadas sobre su trabajo, organización, familia, educación e inclinaciones políticas.

La militarización de esta información tuvo efectos nefastos en el lado mexicano de la frontera. Según Alex Mensing, activista de Sin Fronteras, después de que la CBP compartiera con el Gobierno mexicano la información recabada a través de los vigías, otros miembros de su organización que ayudaron a las caravanas de migrantes en el mismo periodo vieron aumentar el escrutinio fronterizo y las amenazas de muerte. Organizar y apoyar a los migrantes amenaza las operaciones lucrativas que dependen de la criminalización de la migración en toda la región. La ayuda de la sociedad civil hace que los migrantes sean menos propensos al secuestro y la extorsión, lo que por tanto

[10] DHS Office of Inspector General (2021) 'CBP Targeted Americans Associated with the 2018–2019 Migrant Caravan'. https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-62-Sep21.pdf

reduce los ingresos de la delincuencia organizada vinculada a estas actividades y, como efecto dominó, también disminuyen los sobornos a las autoridades, lo que enfrenta los intereses colectivos de estos grupos con los de los activistas y los que prestan ayuda humanitaria.

La vigilancia de cualquier persona que pueda suponer una amenaza para el sistema ha sido durante mucho tiempo una forma generalizada y sistemática de control gubernamental en México. Un documento filtrado de NSO Group, la empresa israelí que creó Pegasus, reveló que 50 mil personas eran posibles objetivos de vigilancia en México. La lista incluía a políticos de la oposición, periodistas que investigaban la corrupción gubernamental y las ejecuciones extrajudiciales, activistas que abogaban por gravar las bebidas azucaradas, jueces, académicos y expertos internacionales que investigaron el caso de la desaparición forzada y ejecución extrajudicial de los 43 estudiantes, entre otros.

En 2022, se descubrió que los teléfonos móviles de dos periodistas y un activista que investigaron los abusos cometidos por el ejército mexicano estaban infectados con el programa malicioso Pegasus. En 2020, el Gobierno mexicano pretendió crear un registro de tarjetas SIM que enlazaría con los datos biométricos y otros datos personales del propietario de la tarjeta. Esto habría intensificado la vigilancia digital del gobierno a través de la infraestructura de las TIC, y contó con la oposición de la sociedad civil.

Documentos internos de la CBP muestran que las agencias gubernamentales a través de la frontera comparten continuamente información sobre la ubicación de los migrantes, su origen y el número de personas en cada grupo, incluso antes de que comiencen a migrar. En 2018, agentes del DHS estadounidense se infiltraron en un grupo de WhatsApp de migrantes hondureños que viajaban en una caravana de unos 4.000. Estas prácticas policiales también están siendo reproducidas por el Gobierno mexicano.[11]

[11] LIS and R3D (2023). Uso de las tecnologías digitales en los contextos migratorios: necesidades, oportunidades y riesgos para el ejercicio de los derechos humanos de las

Impacto: violencia infraestructural y déficit de rendición de cuentas en la actuación policial globalizada en materia de migración

Roberto M., un joven de El Salvador, fue tiroteado y detenido por la policía poco después de ser deportado de Estados Unidos. Los policías rurales que dispararon a Roberto también amenazaron a punta de pistola a un testigo presencial, diciéndole que Roberto era miembro de una banda y que, si revelaba lo que había visto, le ocurriría lo mismo. La policía de El Salvador recibe de Estados Unidos datos sobre la afiliación de los miembros de las bandas, y comparte estas listas con la policía de los barrios donde tienen previsto vivir los deportados. Se ha comprobado que estas bases de datos son problemáticas y poco fiables.[12] Los departamentos de policía confirmaron que esta información se utiliza para perseguir a las personas: "Pensamos que si una persona no era buscada en Estados Unidos, debe ser porque la persona deportada es mala".

La violencia puede vincularse cada vez más a las tecnologías digitales fronterizas, sobre todo en combinación entre sí y con las realidades físicas y medioambientales que las rodean. Algunos estudios muestran los efectos de la vigilancia integrada por torres fijas en las tasas de mortalidad de los inmigrantes en el Valle de Altar, en Arizona. En este caso, la infraestructura digital se fusiona con la ineficaz, aunque antigua, política de disuasión estadounidense, que hace más peligrosas las rutas migratorias, con la teoría de que los migrantes no se arriesgarían a emprender el viaje. La fusión de tecnología y políticas que infligen un daño deliberado produce estos resultados predecibles del aumento de muertes de inmigrantes (Chambers et al., 2019).

personas migrantes, defensoras y periodistas [en prensa]. www.r3d.mx/publicaciones

[12] Open Society Justice Initiative (2019). Unmaking Americans: insecure citizenship in the United States. https://www.justiceinitiative.org/uploads/e05c542e-0db4-40cc-a3ed-2d73abcfd37f/unmaking-americans- insecure-citizenship-in-the-united-states-report-20190916.pdf

La historia de Roberto M. y del testigo de su tiroteo y desaparición tras la deportación en El Salvador refleja otra pauta de violencia vinculada al intercambio de información a través de infraestructuras digitales. La criminóloga Ana Muñiz documenta un "ciclo de actuación policial violenta, migración, actuación policial más violenta, detención, deportación, actuación policial violenta, migración, y así sucesivamente" (Muñiz, 2022), en el que las propias etiquetas ("extranjero criminal" o "miembro de una banda") se convierten en vectores ineludibles de precariedad. Tales etiquetas canalizan a los individuos hacia una *especie de apátridas* como chivos expiatorios constantes y cuantificables que proporcionan una distracción fácil para las fuerzas de seguridad del Estado y las corporaciones que producen y perpetúan las "causas estructurales de la violencia" (Rosas, 2006).

La infraestructura digital no se fusiona con un terreno físico, sino con factores sociales y políticos preexistentes que hacen de la violencia una conclusión inevitable. La infraestructura digital polivalente de hoy en día también permite la incorporación eficaz de nuevas categorías criminalizadas indeseables, incluidos los *organizadores de caravanas* o los *promotores de la migración*, como en el intento de El Salvador de reformar su código penal, criminalizando la *promoción de la migración* en las redes sociales.

Retos y perspectivas

Nos interesa desarrollar un conocimiento más profundo sobre los orígenes políticos de estas infraestructuras para desafiar la violencia de los sistemas globales de control de la migración. Este ensayo solo delimita el campo del objeto de estudio. Se necesita mucho más trabajo colectivo para documentar y diseñar modelos de resistencia que permitan hacer frente a estos desafíos.

La naturaleza difusa y estructural del poder que subyace a las características aparentemente ahistóricas y carentes de motivación de las infraestructuras digitales socava los enfoques clásicos de la rendición

de cuentas. Además, las conocidas vías judiciales nacionales e internacionales para responsabilizar a los autores de estas formas de violencia indirecta –por muy imperfectas o ineficaces que puedan ser– son excepcionalmente inadecuados para las condiciones que se dan en el contexto específico del seguimiento policial de la migración, y esto por varias razones.

En primer lugar, las tecnologías en uso, como las bases de datos biométricos, y los medios de utilizar tecnologías civiles como las redes sociales y otras TIC, simplemente no están diseñadas para respetar o someterse al escrutinio democrático; son de corte militar y convertidas para su uso en espacios cuasi-militarizados, por instituciones impregnadas de ideología militar. Casi un tercio del personal de la CBP sirvió anteriormente en el ejército estadounidense. Las tecnologías de vigilancia biométrica avanzaron a pasos de gigante en las operaciones militares estadounidenses antes de integrarse en la vigilancia fronteriza *civil*. Los contratistas militares del sector privado desempeñan un papel integral en esta transición.

Como documenta la periodista Annie Jacobsen, en el marco de la recopilación de datos biométricos por parte del ejército estadounidense en Afganistán, Palantir Technologies sirvió de enlace fundamental entre las operaciones de inteligencia estadounidenses para rastrear y matar a objetivos militares y las operaciones policiales cuasi civiles, como la prueba piloto de muestras rápidas de ADN de familias migrantes en la frontera estadounidense en 2019 (Jacobsen, 2020). Hoy en día, los kits biométricos utilizados en Afganistán, algunos de los cuales aún almacenan datos biométricos recopilados en el campo de batalla, están a la venta en eBay.

En segundo lugar, los organismos de justicia y supervisión están mal equipados para cumplir la función que les corresponde en este ecosistema. En los procedimientos e investigaciones penales, el uso de tecnologías que capturan y registran pruebas de actividades supuestamente delictivas o que pretenden cotejar biométricamente los registros son extremadamente difíciles de impugnar debido a su barniz científico y a la opacidad de sus métodos de recopilación y análisis

de datos, lo que no deja margen práctico para impugnar o excluir tales pruebas. El diseño de tecnologías que predeterminan factores de riesgo relacionados con conductas delictivas, incluida la migración, contraviene la presunción de inocencia. En el contexto civil, los mecanismos de justicia de ámbito nacional niegan la legitimación activa a los no nacionales situados fuera de Estados Unidos que son víctimas de violaciones vinculadas a la vigilancia digital.

Por último, existen enormes incentivos para que tanto el Estado como el poder empresarial oculten la violencia. El posicionamiento político de las *fronteras inteligentes* como más *humanas* oculta el papel del Estado en la violencia y aísla a las corporaciones de las relaciones públicas negativas o de las restricciones por participar en mercados repugnantes. Su tarea se ve facilitada por la abstracción del dolor físico en lugar de afectar a seres humanos reales (Guidotti-Hernandez, 2011; Woodward, 2005), y por características de la economía de datos como la forma en que las empresas han ayudado al movimiento hacia la gestión de las funciones gubernamentales como plataformas digitales privadas.

Las herramientas de *evaluación de riesgos* de mitigación, como la protección de datos o las evaluaciones de impacto sobre los derechos humanos proporcionan cobertura, favoreciendo la continuación de estas prácticas empresariales porque las empresas las llevan a cabo voluntariamente y se enfrentan a pocas o ninguna consecuencia por una mala evaluación de riesgos. Como era de esperar, estas herramientas dirigidas por la industria a menudo no proporcionan un medio real para la rendición de cuentas; revelan escasa información que sería procesable si y cuando los productos causan daño; y la carga de probar las violaciones de derechos y encontrar un remedio eficaz después de los hechos es asumida enteramente por las víctimas. Los intereses de actores poderosos convergen en torno a una red de intereses financieros en el sistema, lo que conduce al acoso agresivo y al posible silenciamiento de activistas, como ilustra el caso de Irineo Mújica y Sin Fronteras.

Necesitamos herramientas y métodos de cooperación transnacional para documentar, recopilar y compartir información de forma segura, y organizarnos. La fusión de nuevos conocimientos sobre cómo funciona el poder digital dentro de los movimientos de resistencia transnacionales existentes ofrece la posibilidad de cuestionar la infraestructura digital de la externalización de fronteras.

Estamos en las fases iniciales de nuestro esfuerzo colectivo por comprender y sacar a la luz esta infraestructura digital. A través de este análisis, podemos empezar a identificar las intervenciones para empezar a desmantelarla y romperla. La organización transnacional contra las corporaciones tecnológicas ofrece oportunidades para un entendimiento compartido y una solidaridad significativa. Este año, organizaciones de Francia y Kenia, con el apoyo de actores de otros países, demandaron al gigante de la biometría IDEMIA por no cumplir ni siquiera las normas mínimas de diligencia debida en materia de derechos humanos, ya que cosecha miles de millones en ventas secretas de tecnología de seguridad fronteriza a países de renta baja y media. Esta iniciativa surgió de la colaboración en la recopilación de pruebas y la organización transfronteriza.

Como reconoció el estamento militar estadounidense hace décadas: "quien domina el campo de las fronteras externalizadas define 'amigo y enemigo' en todas partes" (Woodward, 2005). Cuanto más rápido establezca Estados Unidos el dominio económico y político sobre la infraestructura digital de control de la migración, mayor será su seguridad para mantener el poder digital global. La infraestructura digital sirve a múltiples propósitos a la vez, pero la función geopolítica última es el poder bruto y generalizado sobre los asuntos mundiales. Las herramientas examinadas aquí *contendrán* la vida humana dentro de espacios de violencia catastrófica, por diseño (Muñiz, 2022; Rosas, 2006; Khan, 2019). Este efecto específico traiciona los compromisos más fundamentales de los derechos humanos internacionales y el derecho humanitario ante los desafíos sin precedentes para la supervivencia humana en la mayor parte del mundo. Pero este efecto pernicioso tampoco viene al caso.

En realidad, como facetas del poder infraestructural, las tecnologías que fijan el "cálculo de quién debe vivir y quién debe morir" (Rosas, 2006) no lo hacen como un fin en sí mismo, sino al servicio del poder y de su reproducción en esta era digital (McCoy, 2017). De este modo, la complicidad de los actores estatales y corporativos en la producción de violencia se pone de manifiesto con la mayor crudeza. Este análisis geopolítico es nuestro punto de partida para construir la resistencia y promover la transformación.

Bibliografía

Aizeki, Mizue et al. (2021). *Smart Borders or A Humane World*. https://www.tni.org/en/publication/smart-borders-or-a-humane-world

Akkerman, Mark (2021). *Border Wars*. Amsterdam: Transnational Institute.

Andersson, Ruben (2018). *Illegality, Inc.: clandestine migration and the business of bordering Europe*. Oakland: University of California Press.

Angel, Arturo (15 de diciembre de 2020). Población en cárceles crece a ritmo récord en 2020: hay 14 mil reos más que al inicio del año. *Animal Político*. https://www.animalpolitico.com/2020/12/poblacion-carceles-crece-record-2020#:~:text=Mientras%20que%20en%20diciembre%20de,de%20que%20cometieron%20un%20delito

Cáceres, Gabriela y Gressier, Roman (14 de mayo de 2021). Sting operation against migrant caravan arrests working-class migrants as human traffickers. *El Faro*.

https://elfaro.net/en/202105/el_salvador/25479/Sting-Operation-against-Migrant-Caravan-Arrests-Working

Chambers, Samuel et al. (2019). 'Mortality, surveillance and the tertiary "funnel effect" on the U.S.-Mexico border: a geospatial modeling of the geography of deterrence'. *Journal of Borderlands Studies*, 36(3), 443–468. https://doi.org/10.1080/08865655.2019.157086

De Goede, Marieke y Westermeier, Carola (2022). Infrastructural geopolitics. *International Studies Quarterly*, 66(3), 1–12. http://dx.doi.org/10.1093/isq/sqac033

DHS Office of Inspector General (2021). CBP Targeted Americans Associated with the 2018–2019 Migrant Caravan. https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-62-Sep21.pdf

Guidotti-Hernández, Nicole (2011). *Unspeakable Violence: remapping U.S. and Mexican national imaginaries*. Londres: Duke University Press

Immigrant Defense Project, Mijente, y NIPNLG (2018). Who's Behind ICE: The Tech and Data Companies Fueling Deportations. https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data- Companies-Fueling-Deportations_v4.pdf

Jacobsen, Annie (2021). *First Platoon: a story of modern war in the age of identity dominance*. Nueva York: Dutton.

Johnson, R. [@USAmbSV] (15 enero de 2021). Aplaudo a las autoridades salvadoreñas que están tomando acción contra quienes quieren engañar a los ciudadanos con caravanas y promesas falsas Solo promueven #UnViajeEnVano [Twit]. *Twitter*. https://twitter.com/FGR_SV/status/1350133335549501443

Khan, Jeffrey (2019). *Islands of Sovereignty: Haitian migration and the borders of empire*. Chicago: University of Chicago Press.

Kwet, Michael (2021). Digital Colonialism. https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire

Masiero, Silvia y Arvidsson, Viktor (2021). Degenerative outcomes of digital identity platforms for development. *Information Systems Journal*, 31(6), 903–928. https://doi.org/10.1111/isj.12351

Massally, K. y Frankenhauser, C. (3 agosto de 2022). The right way to build digital public infrastructure: 5 insights. https://www.weforum.org/ agenda/2022/08/digital-public-infrastructure/

McCoy, Alfred (2017). *In the Shadows of the American Century: The Rise and Decline of US Global Power*. Chicago: Haymarket Books.

Meissner, Doris et al. (2013). *Immigration Enforcement in The United States: a formidable machinery*. Washington, DC: Migration Policy Institute. https://www.migrationpolicy.org/pubs/ enforcementpillars.pdf.

Mijente, Immigrant Defense Project, NIPNLG (2018). Who's behind ICE. https://mijente.net/wp-content/uploads/2023/02/Who-is-Behind-ICE-The-Tech-and-Data-Companies-Fueling- Deportations_v4.pdf

Miller, Todd (2019). *Empire of Borders: The Expansion of the U.S. Border around the World*. Londres, Nueva York: Verso.

Muñiz, Ana (2022). *Borderland Circuitry: Immigration surveillance in the United States and beyond*. Oakland: University of California Press

Open Society Justice Initiative (2019). Unmaking Americans: insecure citizenship in the United States. https://www.justiceinitiative.org/uploads/e05c542e-0db4-40cc-a3ed-2d73abcfd37f/unmaking-americans- insecure-citizenship-in-the-united-states-report-20190916.pdf

Paley, Dawn (2014). *Drug War Capitalism*. Oakland, CA: AK Press.

Romero, Oscar A. (10 de febrero de 2014). La criminalización de la pobreza y el sistema de justicia penal. *Información Sididh*. http://centroprodh.org.mx/sididh_2_0_alfa/?p=31418

Rosas, Gilberto (2006). The managed violences of the borderlands: treacherous geographies, policeability, and the politics of race. *Latino Studies*, 4(4), 401–418. https://doi.org/10.1057/palgrave.lst.8600221

Shivkumar, G., O'Neil, K. y Nordhaug, L. (30 agosto de 2021). How to bring digital inclusion to the people who need it most. https://www.weforum.org/agenda/2021/08/4-reasons-you-should-care-about- digital-public-infrastructure/

Watch CBP Intel (2019). Central American Caravans and Migration Crisis Flow - Update 32. *U.S. Customs and Border Protection.* https://r3d.mx/wp-content/uploads/Central-American-Caravans-and-Migration-Crisis-Flow- Update-32.pdf.

Woodward, John (2005). Using biometrics to achieve identity dominance in the Global War on Terrorism. *Military Review.*

Ver el mundo como una Palestina

Luchas interseccionales contra las Big Tech y el aparheid de Israel

Apoorva PG

Traducción al español por Nuria del Viso Pabón
Ilustración de Anđela Janković

En mayo de 2021, mientras las fuerzas israelíes lanzaban una intensa oleada de ataques aéreos sobre la asediada Franja de Gaza –con el resultado de 256 víctimas palestinas y decenas de miles de heridos–, Google y Amazon Web Services (AWS) firmaron el Proyecto Nimbus, un contrato de 1.200 millones de dólares para proporcionar servicios en la nube al gobierno y al ejército israelíes. Las dos corporaciones proporcionarían de hecho la columna vertebral tecnológica de la ocupación israelí de los territorios palestinos. Ya están en marcha tres centros de datos para este proyecto. Amazon Web Services también proporcionó la plataforma en la nube para el programa espía Pegasus hasta que saltó la noticia sobre el Proyecto Pegasus, y sigue haciéndolo para la aplicación Blue Wolf, que permite a los soldados israelíes capturar imágenes de palestinos en toda la Cisjordania ocupada y luego cotejarlas con bases de datos militares y de inteligencia.

Este contrato, de un alcance y unas repercusiones sin precedentes, es solo una manifestación de los profundos vínculos entre Israel y las grandes empresas tecnológicas. Hewlett Packard Enterprise, por ejemplo, tenía un contrato exclusivo de 2017 a 2020 para suministrar servidores para la base de datos de población de Israel, que también se utilizó para determinar diversas formas de exclusión de los ciudadanos palestinos de Israel y los residentes de la Jerusalén Oriental ocupada. Las grandes tecnológicas han contribuido a sostener una ocupación basada en el control militar y la vigilancia perpetua, que los palestinos llevan décadas denunciando como una forma de *apartheid* y de *colonialismo de colonos*. Amnistía Internacional y otras organizaciones internacionales, el Relator Especial de la ONU sobre los derechos humanos en los Territorios Palestinos Ocupados (TPO) y un número creciente de gobiernos consideran que Israel está cometiendo el delito de *apartheid*.

La ubicuidad de la tecnología y el control digitales, junto con la monetización de los datos personales, han llevado a que los datos se conviertan en la nueva frontera del colonialismo. Comprender el papel de las grandes empresas tecnológicas en la consolidación de la violación de los derechos humanos de los palestinos por parte de Israel pone de relieve la urgente necesidad de hacer frente a este colonialismo global de los datos. Esto se debe tanto a que los métodos de represión probados contra los palestinos se están adoptando en todo el mundo como a que cuestionar a las grandes empresas tecnológicas, su connivencia con las agencias militares y de vigilancia y su robo de nuestros datos nos permite construir luchas interseccionales contra la matriz de opresión –militarización, capitalismo neoliberal y *apartheid* israelí– que las grandes empresas tecnológicas refuerzan y de la que se benefician.

Los profundos vínculos entre Israel y las grandes empresas tecnológicas han permitido un flujo bidireccional de beneficios, delitos y complicidad. Esto permite a Israel desplegar tecnología de rápida innovación desarrollada por empresas transnacionales e integrarla en su vigilancia, control y represión de la población palestina. Al mismo tiempo, la tecnología israelí desarrollada para controlar al pueblo palestino se pone a disposición de las empresas tecnológicas israelíes e internacionales para que la amplíen y exporten a otros países con fines represivos. Consideremos algunas de estas estadísticas recopiladas por la campaña palestina Stop the Wall en su informe *Digital Walls*:

- Durante las últimas décadas, más de 300 empresas multinacionales tecnológicas líderes establecieron centros de I+D en Israel, lo que representa alrededor del 50 % del gasto en I+D [investigación y desarrollo] de las empresas.
- Estas multinacionales han adquirido un total de 100 empresas israelíes. Algunas de ellas, como Intel, Microsoft, Broadcom, Cisco, IBM y EMC, han adquirido más de diez empresas locales durante el tiempo que llevan operando en Israel.

- Más de 30 unicornios tecnológicos –empresas emergentes valoradas en más de 1.000 millones de dólares– tienen su sede en Israel. Esto supone alrededor del 10 % de los unicornios del mundo.

Esta relación simbiótica impulsa la inversión de las grandes empresas tecnológicas en Israel y refuerza el crecimiento de la vigilancia y la tecnología digital militarizada, de la que Israel ha sido pionero, aunque no es el único.

'Big Tech' y guerras imperiales globales

El contexto específico de las grandes corporaciones tecnológicas y el *apartheid* de Israel forma parte de una estructura de poder global de dominación, racismo y estados coercitivos. La tecnología digital incluye sistemas de vigilancia utilizados por primera vez por los militares, como sostiene el informe Digital Walls:

Ambos procesos –la digitalización y la militarización– no son solo desarrollos parcialmente paralelos en el tiempo. Están profundamente entrelazados: los primeros ordenadores surgieron de la Segunda Guerra Mundial e Internet fue desarrollado en la Guerra Fría por el ejército estadounidense. No es de extrañar que la tecnología, la investigación y la industria militares estén obteniendo enormes beneficios del inicio de la economía digital.

El Proyecto Maven del Pentágono ilustra cómo estos procesos y sus interrelaciones siguen creciendo a la par que las guerras globales e imperiales. Desde principios de 2000, el ejército estadounidense ha utilizado aviones no tripulados para atacar objetivos en otros países, causando también víctimas civiles. El Proyecto Maven está orientado a fomentar los ataques con aviones no tripulados mediante el análisis de imágenes de vigilancia con el uso de Inteligencia Artificial (IA). Google fue contratado inicialmente para este proyecto, pero se retiró a raíz de las objeciones de sus propios empleados. El contrato pasó entonces

a AWS y Microsoft, y desde entonces se ha transferido a la Agencia Nacional de Inteligencia Geoespacial de Estados Unidos (NGA).

El proyecto Big Tech Sells War, que ha seguido la senda de connivencia entre las empresas tecnológicas estadounidenses y la violencia antimusulmana y la islamofobia, señaló que "la Ley [Patriota] autoriza amplios poderes al Gobierno para vigilar a los estadounidenses e incluso detener indefinidamente a inmigrantes que no están acusados de delitos. Su aprobación abrió las puertas para que las grandes tecnológicas se convirtieran, ante todo, en intermediarias de nuestros datos personales, vendiéndolos a agencias gubernamentales y empresas privadas dentro y fuera del país y desencadenando la era de la economía de datos". La Agencia de Seguridad Nacional de Estados Unidos (NSA), cuyo programa de vigilancia masiva sacó a la luz el ex contratista Edward Snowden, tuvo acceso a los servidores de Microsoft en septiembre de 2007; a los de Google en enero de 2009; a los de Facebook en junio de 2009; a los de YouTube en 2010; y a los de Apple en octubre de 2012, por mandato de las enmiendas a la Ley de Vigilancia de Inteligencia Extranjera, que desde entonces han sido reformadas.

Décadas de normalización de la vigilancia masiva, la introducción de ataques remotos con drones por parte del ejército estadounidense, y la construcción de muros y otros mecanismos de control fronterizo para impedir la entrada de inmigrantes han dependido de una tecnología en constante avance para clasificar, vigilar y atacar a las personas. Esta dinámica ha corrido paralela a la transformación de la gran tecnología en la industria multimillonaria que es hoy. Una cronología de ambas trayectorias –la evolución de las tecnologías de represión y el crecimiento de las grandes tecnológicas– puede encontrarse en la campaña Big Tech Sells War. En 2013, AWS consiguió su primer contrato en la nube en Estados Unidos con la CIA, la Agencia de Seguridad Nacional (NSA) y otras agencias de inteligencia estadounidenses. En abril de 2022, la NSA volvió a adjudicar a AWS un contrato (independiente) de 10.000 millones de dólares para servicios de computación en la nube. Microsoft protestó contra la obtención de este contrato por parte de AWS, sucesor del contrato Joint Enterprise

Defense Infrastructure (JEDI) IT, que Microsoft tenía en 2019. En marzo de 2021, Microsoft firmó para proporcionar gafas de realidad aumentada HoloLens al ejército estadounidense en un contrato por valor de unos 21.880 millones de dólares en 10 años.

Big Tech Sells War calcula que, en los últimos 20 años, los contratos de las grandes tecnológicas con el Pentágono y el Departamento de Seguridad Nacional (DHS) han ascendido aproximadamente a 44.000 millones de dólares. En el momento de escribir este artículo, Steve Pandelides, Director de Seguridad de AWS, había trabajado para el FBI durante más de 20 años, entre otras cosas en el Centro Nacional de Lucha contra el Terrorismo y en la División de Tecnología Operativa. Jared Cohen trabajó en Google, donde fundó Jigsaw, encargada de desarrollar herramientas antiterroristas para plataformas de medios sociales, entre otras cosas. Anteriormente fue personal de planificación de políticas del Departamento de Estado de Estados Unidos y ahora trabaja en Goldman Sachs.

En muchos sentidos, las grandes empresas tecnológicas se basan en el modelo del complejo militar-industrial para crear un nuevo complejo tecnológico-militar. Pero a diferencia de la naturaleza descarada de la industria armamentística tradicional, en la que las armas están obviamente diseñadas para matar y reprimir, la 'Big Tech' es más insidiosa porque pretende ser democrática y accesible al mismo tiempo. La difusa distinción entre uso militar y civil contribuye a normalizar su ubicuidad y embota nuestra respuesta a los urgentes desafíos que plantea.

La tecnología del apartheid israelí

Ver la situación desde la perspectiva de la ciudadanía palestina ayuda a despejar la niebla, dada la complicidad de las grandes tecnológicas en el sistema de *apartheid* de Israel. Desde antes de su establecimiento en 1948, mediante la limpieza étnica de cientos de miles de palestinos, Israel ha desplegado su aparato militar y de vigilancia para

desposeerlos, fragmentarlos y restarles aún más poder. El Cuerpo de Inteligencia de las Fuerzas de Ocupación Israelíes, Unidad 8200, se fundó en 1952. Desde entonces, se encarga de recopilar información y descifrar códigos. El espionaje y la vigilancia masiva de los palestinos es la fuerza motriz de gran parte del rápido desarrollo de nuevas tecnologías por parte de Israel. He aquí cómo la Autoridad de Innovación de Israel habla de la ciberguerra:

> La ciberguerra siempre ha estado a la vanguardia de la industria israelí de alta tecnología. [...] La combinación ganadora de graduados de las unidades tecnológicas de las FDI [Fuerzas de Defensa de Israel] y un entorno de innovación apoyado por la Autoridad de Innovación permite que la tecnología israelí de vanguardia dé forma al futuro a partir de hoy (Israel Innovation, s/f).

Israel exporta este paradigma de seguridad –de miedos fabricados que justifican respuestas autoritarias por parte de los estados para garantizar su *seguridad* y *supervivencia*– junto con sus armas y tecnologías. En el caso del régimen de apartheid de Israel, esta necesidad de seguridad se extiende solo a la población judía, mientras que los palestinos viven en diversos grados de privación de derechos, despojados de seguridad por las políticas de Israel.

La Unidad 8200 puede intervenir cualquier conversación telefónica en los Territorios Palestinos Ocupados. Hay cámaras de reconocimiento facial instaladas –una por cada 100 palestinos– en el Jerusalén Este ocupado. La información privada se utiliza para chantajear a los palestinos para que se conviertan en informantes (Mondoweiss, 2014). Las cámaras Hawk Eye, diseñadas para leer las matrículas, permiten a las fuerzas policiales israelíes obtener información y la ubicación de los vehículos en tiempo real. Los puestos de control israelíes tienen instalada tecnología de reconocimiento facial, inicialmente proporcionada por HP. La aplicación *Lobo azul*, apodada el *Facebook para palestinos* secreto del ejército israelí, capta imágenes de palestinos de toda Cisjordania ocupada y las coteja con la base de datos gestionada por los servicios militares y de inteligencia israelíes. Los soldados

israelíes son recompensados por capturar un gran número de fotografías de palestinos bajo ocupación (Abukhater, 2022).

Ni siquiera el panóptico de Jeremy Bentham capta esta situación, ya que solo pretendía vigilar para controlar, mientras que Israel y su aparato tecnológico pretenden vigilar, coaccionar, chantajear y violar, todo ello en el marco de su régimen de *apartheid*.

Al igual que la industria armamentística, la esfera de la tecnología digital israelí se despliega dentro de un sistema de *apartheid*, por el que las herramientas y aplicaciones se *prueban sobre el terreno* en palestinos antes de exportarlas. Jalal Abukhater, en el artículo citado anteriormente, señala:

> Para las empresas israelíes dedicadas al desarrollo de tecnologías de vigilancia y programas espía, los territorios ocupados no son más que un laboratorio donde probar sus productos antes de comercializarlos y exportarlos a todo el mundo con fines lucrativos. Para el Gobierno israelí, este régimen de vigilancia es tanto una herramienta de control como un negocio para hacer dinero (Abukhater, 2022).

De hecho, como reveló el Proyecto Pegasus, el programa espía Pegasus del Grupo NSO israelí se ha utilizado en todo el mundo para espiar a periodistas y activistas, así como a dirigentes gubernamentales y de la oposición. En India, por ejemplo, la lista de objetivos del programa espía Pegasus incluye a cualquiera que plantee un desafío serio al Gobierno derechista de Modi. Es bien sabido que las armas y tecnologías militares israelíes se utilizan como medio de represión en todo el mundo. Sin embargo, sigue estando oculto el papel de las grandes empresas tecnológicas en la producción y exportación de tecnologías represivas por parte de Israel.

Las grandes tecnológicas, beneficiarias del apartheid

Mientras que su régimen colonial de *apartheid* y de colonos es el *laboratorio* para la producción de armas y tecnología represivas, son las

grandes empresas tecnológicas las que proporcionan la inversión necesaria y apoyan la proliferación de la industria israelí de TI y ciberseguridad, de la que se beneficia ampliamente.

Los principales gigantes tecnológicos, desde Microsoft hasta Google y AWS, participan activamente en la industria tecnológica israelí. Microsoft habría adquirido dos empresas israelíes de ciberseguridad entre 2015 y 2017. Adallom, fundada por un veterano de la unidad especial de Inteligencia israelí, fue comprada en 2015 por 320 millones de dólares, y Hexadite por 100 millones en 2017.

En 2019, AWS, contratada junto con Google para construir la plataforma en la nube de Israel junto con Google, trabajó con centros de datos locales para establecer la infraestructura en la nube. Como parte del proyecto Nimbus, Google ha creado recientemente una región local de nube en Israel. Según el contrato, las dos empresas se han "comprometido a realizar compras recíprocas y a poner en marcha una cooperación industrial en Israel equivalente al 20% del valor del contrato" (Scheer, 2022). El segundo mayor centro de I+D de Facebook también tiene su sede en Israel.

Los estados que compran programas espía y tecnología digital israelíes para reprimir a sus ciudadanos están afianzando el régimen de *apartheid* de Israel, y, como tal, deben ser cuestionados, junto con la denuncia de la complicidad y la especulación de las grandes empresas tecnológicas con sede en Estados Unidos.

Praxis de la interseccionalidad: la campaña No Tech for Apartheid

La expansión del control y la complicidad de las grandes empresas tecnológicas en la represión militar se ha visto contrarrestada por diversos retos y por la resistencia popular. Desde la primera fase de denuncias de irregularidades hasta las campañas actuales que exponen cómo las grandes empresas tecnológicas se benefician de la guerra existe una demanda creciente para poner fin a la militarización de la tecnología.

En Estados Unidos, por ejemplo, una campaña popular, No Tech for ICE, destaca el papel clave desempeñado por Palantir y AWS al proporcionar la infraestructura para el Servicio de Inmigración y Control de Aduanas (ICE) junto con otras agencias policiales involucradas en la brutal política de separación familiar de la administración Trump. Palantir recopiló información sobre individuos, lo que permitió a las agencias estatales rastrear y construir perfiles de inmigrantes para ser deportados, mientras que AWS proporcionó servidores para alojar las herramientas de Palantir.

Los organizadores comunitarios están reconociendo y respondiendo rápidamente al modo digital de militarización y represión, que se observa no solo en las exportaciones de los gigantes tecnológicos a estados represivos, sino también en cómo la censura digital y el silenciamiento se utilizan para aplastar las voces de la resistencia y amplificar las ideologías regresivas de derechas. Esto también lo han puesto de relieve grupos de derechos digitales como 7amleh, el Arab Center for Social Media Development y Sada Social, que han demostrado cómo durante el asalto a Gaza de 2021 y en la lucha popular posterior plataformas de medios sociales como Facebook e Instagram censuraron el contenido relacionado con Palestina. Existe un discurso creciente sobre los derechos digitales que reúne a organizadores de base y expertos en tecnología que trabajan para que la esfera digital sea abierta y democrática en lugar de servir como herramienta de sometimiento.

A estas fuerzas se han unido varios empleados actuales (y antiguos) de empresas tecnológicas, en huelga contra el uso de sus productos para violar los derechos de los marginados y con fines militares. Destacaron las profundas implicaciones éticas de involucrarse de la manera que sea en la automatización de la guerra. En 2018, un año antes de su vencimiento, Google anunció que no renovaría su contrato con Project Maven. Como ya se ha dicho, Microsoft y AWS ganaron el contrato.

La campaña contra el Proyecto Nimbus presenta una oportunidad crucial para unir las luchas contra las 'Big Tech' desde varios ángulos: palestinos y activistas solidarios, trabajadores tecnológicos, derechos digitales y activistas sindicales y antimilitaristas.

Meses después de que se anunciara el contrato, noventa empleados de Google y trescientos de Amazon escribieron una carta abierta condenando y oponiéndose a la decisión de sus empleadores de "suministrar al Gobierno y al ejército israelí tecnología que se utiliza para dañar a los palestinos". Algunos de los manifestantes se enfrentaron a represalias, como Ariel Koren, a quien se le dio un ultimátum para trasladarse de Estados Unidos a Brasil, a pesar de las grandes peticiones públicas en contra de esta acción. Koren abandonó Google en agosto de 2022, señalando en su declaración de dimisión que "Google silencia sistemáticamente las voces palestinas, judías, árabes y musulmanas preocupadas por la complicidad de Google en las violaciones de los derechos humanos de los palestinos, hasta el punto de tomar represalias formales contra los trabajadores y crear un ambiente de miedo". Otros se unieron a ella para denunciar las represalias tomadas contra quienes apoyaban esta campaña.

Junto con la profunda complicidad de AWS en la industria de TI y ciberseguridad de Israel, y su apoyo a la represión en otros lugares como se ve en el ejemplo de ICE, se ha denunciado ampliamente su historial en el trato inhumano de los trabajadores y la represión sindical (Kantor, 2021). La formación del sindicato Amazon Labor Union en Staten Island fue, por tanto, un momento histórico en el movimiento sindical estadounidense. En conjunto, es probable que las acciones de estos empleados causen cierta preocupación entre los actuales directores ejecutivos de las grandes tecnológicas.

Más allá del apoyo a las agencias militares y de vigilancia, que en esencia contribuye a una militarización cada vez mayor de la vida cotidiana de las personas, también está la cuestión del control de las grandes tecnológicas sobre nuestros datos. Aspectos de nuestras vidas que dejan huellas en el mundo virtual –ahora casi inevitables– se entretejen en algoritmos que influyen profundamente en nuestras elecciones, opiniones políticas y decisiones. Los movimientos por los derechos digitales exigen la defensa de nuestra privacidad y seguridad y contra la comercialización de los datos personales, y en ningún lugar es más evidente que con Google. Existe un creciente desafío al control

de las grandes tecnológicas sobre las vidas individuales y las elecciones codificadas en datos. Las alternativas al colonialismo de los datos también han suscitado animados debates sobre el código abierto, la propiedad pública, etc.

En el extremo más agudo del colonialismo digital, Palestina es, por tanto, un signo de lo que está por venir y, por tanto, el punto en el que primero debemos resistir. En nombre de la reducción de la brecha digital, las grandes empresas tecnológicas están cada vez más arraigadas, extrayendo datos y lucrándose con ellos. La pandemia de COVID-19 exacerbó esta situación, ya que personas de todo el mundo tuvieron que trabajar y estudiar desde casa, en su mayoría sin acceso a tecnología y equipos digitales.

El creciente interés de estudiantes y académicos por cuestionar el control de las grandes empresas tecnológicas, como Google, en el ámbito de la educación, y su relación directa con la opresión de los palestinos, impulsó a la campaña mundial No Tech for *Apartheid* a elaborar un conjunto de herramientas para organizarse en los campus universitarios.

La campaña contra el Proyecto Nimbus se sitúa en la intersección de la solidaridad palestina y los movimientos contra el *apartheid*, los derechos laborales, los derechos digitales, la descolonización y la desmilitarización. En este movimiento en evolución, ofrece una visión clara de la matriz de opresión de la militarización, el capital neoliberal y el *apartheid* israelí, todo lo cual refuerza la gran tecnología y de lo que obtiene enormes beneficios. Se basa en la comprensión desarrollada por las campañas contra las grandes tecnológicas en la guerra, y reúne a muchas comunidades que luchan contra un contrato que tiene profundas implicaciones para todos. Los sistemas interconectados que nos oprimen exigen que nuestras formas de resistencia también se unan, para desafiar a las fuerzas que pretenden aislarnos. La solidaridad solo existe en la acción, y a través de su propia existencia como fuerza interseccional socava la violencia infligida por el colonialismo, el patriarcado, el racismo y el neoliberalismo. La tecnología no está diseñada para ser neutral, y mientras aspectos de nuestras vidas se adentran cada vez más

en esta esfera, y sus operaciones y mecanismos siguen estando lejos de ser democráticos, con la fuerza de la resistencia global sus herramientas básicas aún pueden democratizarse y hacerse accesibles.

Bibliografía

7amleh, the Arab Center for Social Media Development (2021). #Hashtag Palestine 2021. https://7amleh.org/storage/Hashtag%20 2021%20EN.pdf

Alys Samson Estapé (mayo de 2021). Israel: the model coercive state and why boycotting it is key to emancipation everywhere. *TNI Longreads*. https://longreads.tni.org/stateofpower/israel-the-model-coercive-state.

Abukhater, Jalal (2022). Under Israeli surveillance: Living in dystopia, in Palestine. *Aljazeera*. https://www.aljazeera.com/opinions/2022/4/13/under-israeli-surveillance-living-in-dystopia-in-palestine

Amnesty International (2022). Israel's apartheid against Palestinians. https://www.amnesty.org/en/latest/campaigns/2022/02/israels-system-of-apartheid/

Big Tech Sells War. Big Tech Sells War - How Big Tech Sells War on our Communities. https://bigtechsellswar.com/

Big Tech Sells War. Big Tech Sells War - How Big Tech Sells War on our Communities. https://bigtechsellswar.com/#timelines-home

Brewster, Thomas (2021). Project Maven: Amazon And Microsoft Scored $50 Million In Pentagon Surveillance Contracts After Google Quit. *Forbes*. https://www.forbes.com/sites/

thomasbrewster/2021/09/08/ project-maven-amazon-and-microsoft-get-50-million-in-pentagon-drone-surveillance-contracts-after- google/?sh=549483dc6f1e

Fung, Brian (2021). Amazon Web Services disables cloud accounts linked to NSO Group. *CNN Business.* https://edition.cnn.com/2021/07/19/tech/amazon-nso-group-pegasus-cloud-accounts/index.html.

Investigate & Dismantle Apartheid. (2022). Al Haq issues landmark report 'Israeli Apartheid: Tool of Zionist Settler- Colonialism'. https://antiapartheidmovement.net/updates/view/al-haq-issues-landmark- report-israeli-apartheid-tool-of-zionist-settler-colonialism/15

Israel Innovation. Attack is the Best Form of Defense. https://innovationisrael.org.il/en/reportchapter/attack-best-form-defense

Kantor, Jodi, Weise, Karen y Ashford, Grace (15 de junio de 2021). The Amazon That Customers Don't See. *The New York Times.* https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html

Khan, Azmat (18 de diciembre de 2021). Hidden Pentagon Records Reveal Patterns of Failure in Deadly Airstrikes. *The New York Times*. https://www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records- civilian-deaths.html

Middle East Eye (2021). Meet Blue Wolf, the app Israel uses to spy on Palestinians in the occupied West Bank. https://www.middleeasteye.net/news/israel-whats-blue-wolf-app-soldiers-use-photograph- palestinians

Nextgov.com (2021). NSA Awards Secret $10 Billion Contract to Amazon. https://www.nextgov.com/it-modernization/2021/08/nsa-awards-secret-10-billion-contract-amazon/184390/

Notechforice.com. About | #NoTechForICE. https://notechforice.com/about/

Novet, Jordan (31 de marzo de 2021). Microsoft wins U.S. Army contract for augmented reality headsets, worth up to $21.9 billion over 10 years. *CNBC*. https://www.cnbc.com/2021/03/31/microsoft-wins-contract-to-make-modified- hololens-for-us-army.html

Lunden, Ingrid (2017). Microsoft to buy Israeli security firm Hexadite, sources say for $100M. *TechCrunch*. https://techcrunch.com/2017/06/08/microsoft-confirms-its-acquired-hexadite-sources-say-for- 100m/?guccounter=2

Scheer, Steven (24 de mayo de 2021). Israel signs cloud services deal with Amazon, Google. *Reuters*. https://www.reuters.com/technology/israel-signs-cloud-services-deal-with-amazon- google-2021-05-24/

Scheer, Steven (20 de octubre de 2022). Google activates Israel's first local cloud region. *Reuters*. https://www.reuters.com/technology/google-activates-israels-first-local-cloud-region-2022-10-20/

Shulman, Sophie (8 de enero de 2021). Unit 81: The Elite Military Unit That Caused a Big Bang in the Israeli Tech Scene. *The algemeiner*. https://www.algemeiner.com/2021/01/08/unit-81-the-elite- military-unit-that-caused-a-big-bang-in-the-israeli-tech-scene/

Statt, Nick (2018). Google reportedly leaving Project Maven military AI program after 2019. *The Verge*. https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire

Stop The Wall (s/f). Digital Walls. https://stopthewall.org/digitalwalls/

Stop The Wall (s/f). Digital Walls. https://stopthewall.org/digitalwalls/#militarization

Strout, Nathan (2022). Intelligence agency takes over Project Maven, the Pentagon's signature AI scheme. *C4ISRNet*. https://www.c4isrnet.com/intel-geoint/2022/04/27/intelligence-agency-takes-over-project-maven- the-pentagons-signature-ai-scheme/

Theregister.com (2022). $10b US defense cloud contract re-awarded to AWS. https://www.theregister.com/2022/04/28/nsa_wands_aws/

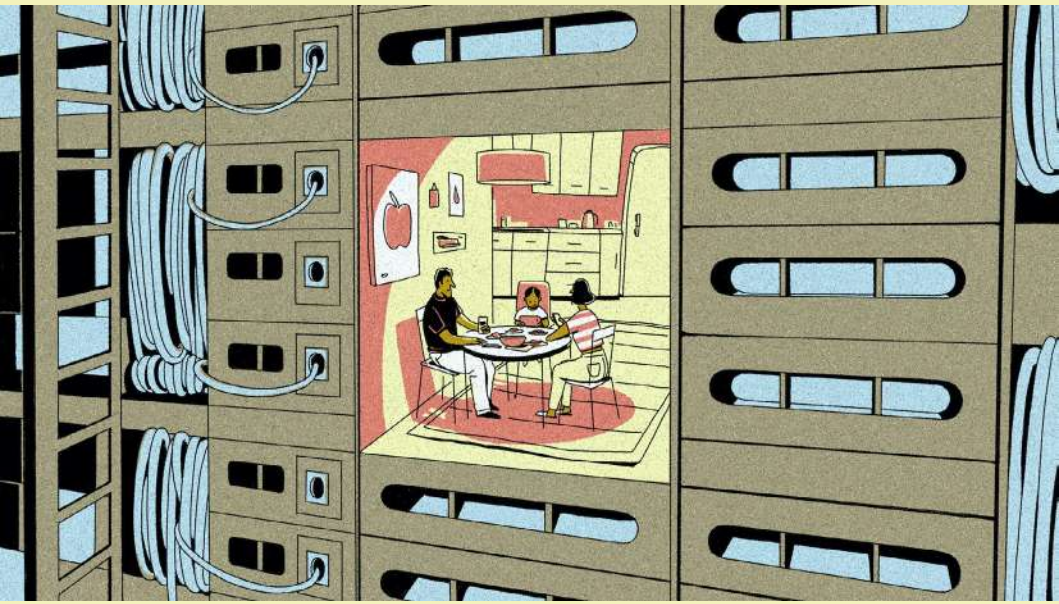
VentureBeat (2015). Microsoft confirms it has acquired cloud security platform Adallom. https://venturebeat.com/business/microsoft-confirms-it-has-acquired-cloud-security-platform-adallom/

Weiss, Philip (2014). Israel surveils and blackmails gay Palestinians to make them informants. *Mondoweiss*. https://mondoweiss.net/2014/09/blackmails-palestinian-informants/

WhoProfits (2021). Hewlett Packard Enterprise (HPE). https://www.whoprofits.org/company/ hewlett-packard-enterprise-hpe/

El capitalismo digital es una mina, no una nube

Explorando las bases extractivistas de la economía de datos



Maximilian Jung

Traducción al español por Nuria del Viso Pabón
Ilustración de Anđela Janković

El mayor centro de datos de la ciudad de Berlín (Alemania) se encuentra en un edificio anónimo y gris entre una oficina de pago de impuestos, dos negocios de venta de coches usados y un almacén de materiales en el barrio de Siemensstadt. Satisface su alta demanda energética a partir de la central térmica de carbón de Reuter West, que nutre de electricidad a más de un millón de hogares en Berlín, y que no está lejos del centro. Desde afuera, no se asemeja, ni mucho menos, a esa representación hipertecnológica de la nube como un espacio digital irreal y etéreo. Dentro del edificio, hay innumerables pilas de servidores, ronroneando y consumiendo grandes cantidades de agua y de electricidad de origen fósil para permitir la circulación de un flujo masivo de datos.

Parece improbable que este lugar, operado por la compañía japonesa de telecomunicaciones NTT, pudiera tener alguna conexión con la historia del barrio, que fue levantado por el gigante industrial Siemens para la producción y el alojamiento de sus trabajadores hace ya más de ciento veinte años. Y aun así, este edificio y la infraestructura que representa están detrás de las más ricas y poderosas compañías del mundo. Se trata de una manifestación de la explotación de las personas y del extractivismo que está devastando al planeta y que crecientemente intenta colonizar nuestras vidas y relaciones sociales en forma de datos.

A las grandes compañías tecnológicas, como Alphabet, Amazon, Apple, Microsoft o Meta, al igual que sus equivalentes chinas como Alibaba, Tencent y Weibo, les gusta decir que los datos son las nuevas *materias primas* que están ahí para extraerse. Una reserva que espera a ser descubierta por actores capaces de hacerlo, que aprovecharán todo su potencial para el beneficio de la humanidad. El último giro lingüístico del director de finanzas de Google, por ejemplo, ha sido el de

abandonar la metáfora de los datos como el nuevo petróleo y emplear, en su lugar, la de la radiación solar, implicando que los datos son un recurso "recargable, inagotable (especialmente en comparación con el petróleo finito) y sin dueño, que puede ser recogido de modo sostenible" (Couldry y Mejias, 2019b).

Esta narrativa naturaliza y oculta las omnipresentes infraestructuras que se construyen para generar los datos, y la aspiración empresarial de transformar potencialmente toda experiencia humana e interacción social en datos a ser extraídos. Esto no solo violaría nuestra privacidad, dejándonos sin medios para un consentimiento aceptado, sino que –como los datos son siempre relacionales– nos obligaría a relaciones en las que participaríamos en la opresión de unos por otros (Viljoen, 2021).

Esta narrativa también esconde la existencia de los actores que se apropian, agregan y venden estos datos para obtener beneficio económico y, de este modo, las decisiones subyacentes sobre los datos que merece la pena recolectar, cómo se almacenan, etiquetan y analizan. Esto minimiza la violencia implícita en la extracción de los materiales usados para la transformación digital, así como la explotación que hace que funcione, en la propia minería metálica, el manufacturado de partes, mediante la brutalización y desposesión de recursos vitales para las comunidades, el vertido de residuos tóxicos en vertederos o la descarga del peor trabajo de moderación en *trabajadores del click* traumatizados. Y, en última instancia, despolitiza aquellas decisiones que dieron lugar a la economía digital y pretende robarnos los medios para imaginar futuros diferentes.

Llevado al mercado, pero no producido para la venta

Más que concebir los datos como un recurso, deberíamos entender este fenómeno como experiencias humanas y relaciones sociales que han sido convertidas en datos (*datificadas*) y, de este modo, transformadas en una mercancía, que se puede vender. Esto no ocurre de modo natural, sino que requiere una gran cantidad de intervención política

y de violencia, y tiene graves consecuencias tanto para los individuos como para las sociedades. Retomemos las reflexiones de Karl Polanyi para guiar nuestras ideas sobre el proceso de mercantilización y sus consecuencias. En su clásico *La Gran Transformación,* describe la violencia histórica necesaria para asegurar que la tierra, el trabajo y el dinero se transformen en mercancías, así como para la creación de la sociedad de mercado como un sistema económico separado y *autorregulado*, dirigido y controlado por mecanismo de mercado. Esta lógica económica, sin embargo, colonizaría y dominaría pronto la lógica social.

La diferencia fundamental entre las *mercancías ordinarias* (como el petróleo o el maíz) y la tierra, el trabajo o el dinero es que el trabajo y el dinero son lo que Polanyi denomina *mercancías ficticias*, dado que son esenciales para la vida humana. Tratarlas como si fuesen mercancías ordinarias socaba las bases mismas de la producción de mercancías y es la causa de tres crisis interrelacionadas: la desintegración de las comunidades y la creciente presión sobre el trabajo de cuidados, el agotamiento de la naturaleza, y la financiarización de la economía, con su recurrente destrucción de los medios de vida en todo el mundo (Fraser, 2014).

Este desarrollo no hubiera sido posible sin procesos coloniales de apropiación, posesión, esclavización y extracción. Tales procesos fueron la base de la mercantilización del trabajo, la tierra y el dinero en Europa, y de la creación de la sociedad de mercado y su subsiguiente expansión (Bhambra, 2021). La expropiación violenta de la tierra en América fue la precursora de la privatización de los comunes. Sin la esclavitud, la racialización y la mercantilización de millones de personas negras, la mercantilización del trabajo es impensable (Ashiagbor, 2021). El trabajo esclavo en las plantaciones, el saqueo y las emergentes instituciones financieras íntimamente asociadas a la esclavitud fueron clave a la hora de proporcionar el capital para la industrialización y los procesos que Polanyi describe (Beckert y Rockman, 2016; Berry, 2017).

¿Cómo se mercantilizó el trabajo en Europa? Tomemos la descripción del trabajo de Polanyi. En esta argumenta que el trabajo es esencialmente otro nombre para una actividad que no se puede separar de la vida humana misma. Para mercantilizarlo, hubo que privatizar las

tierras comunes, desposeer violentamente a la población campesina, abolir las formas incipientes y locales de generación de bienestar, y obligar a hombres, mujeres y niños a una migración para trabajar en las fábricas de los emergentes centros urbanos. Solo cuando sus medios de subsistencia fueron robados, solo cuando fueron forzados violentamente a hacerlo, solo entonces las personas vendieron su trabajo en un mercado nacional de cambio institucionalizado por un salario escaso. El trabajo había sido finalmente mercantilizado.

La innovación tecnológica, pagada con el capital que venía de las colonias, necesitó esta forma de organización del trabajo para funcionar. El trabajo de cuidados en este sistema –limpieza, alimentación, y cuidado de los mayores y de los niños– se convierte en una actividad apropiada por el capital, transformándose en la acción de reproducir la fuerza de trabajo más que en la de sostener y nutrir la vida humana (Fraser, 2014).

Desde entonces, la lógica del mercado se ha expandido tanto en el mismo territorio como en todas las áreas de la sociedad. Tal y como Polanyi escribía: "Una economía de mercado puede existir solo en una sociedad de mercado" (Polanyi, 1957, p. 54). Aunque nuestra comunicación con los amigos y la familia, compartiendo nuestros pensamientos y experiencias íntimas, nuestras funciones corporales, o lo que hacemos en nuestro día a día no se conciban como una fuente de datos, bajo el capitalismo digital se han convertido en una mercancía, transformada a través de los procesos de extracción, abstracción y agregación. Estos datos se pueden vender y acaban volviendo a nosotros en forma de anuncios personalizados.

Las tres crisis interrelacionadas de trabajo, tierra y dinero se unen en ese proceso de mercantilización de los datos que habitualmente entendemos como digitalización. Más que suponer un alivio, la digitalización profundiza el agotamiento de la naturaleza, a través de la extracción de materiales. Se construye con trabajo explotado, a la vez que aumenta la vigilancia de sobre los trabajadores y eleva su precariedad. Y esto hace posible la financiarización de la economía, lo cual, a la vez, la financia.

La gran transformación, la sociedad de mercado en el siglo XXI, está encaminada a capturar la vida humana misma y a mercantilizarla hasta

el final. Este ensayo trata acerca de la historia de esa mercantilización, su relación con la crisis ecológica y las formas de salir de este proceso.

La generación de los datos y su mercantilización

La digitalización tiene una historia más larga de lo que habitualmente se conoce. Los primeros ordenadores –operados por mujeres– se usaron para gestionar el enorme volumen de datos que venían de los censos a principios del siglo XX. Los gobiernos querían conocer a sus ciudadanos y el entorno para gobernarlos. Los ciudadanos, cuyos datos habían sido recogidos, fueron convertidos por los burócratas en el término abstracto *población*, con atributos particulares que debían ser gestionados y administrados. Igualmente, los militares –ahora muy decisivos a la hora de configurar las tecnologías esenciales para capturar los datos– querían predecir el tiempo para la guerra o para el incremento los resultados de un sector agrícola en proceso de industrialización (Ensmenger, 2018).

Para comprender la mercantilización de los datos es crucial entender la historia de las tecnología de la información y la comunicación (TIC). Internet, y muchas otras tecnologías, desde los microprocesadores hasta los sistemas de geoposicionamiento global (GPS) o las pantallas táctiles que hacen *inteligentes* a nuestros teléfonos inteligentes, proceden de inversiones estatales e investigación del complejo militar-industrial de EEUU (y en menor extensión del de Reino Unido) (Mazzucato, 2013). El predecesor de internet, ARPANET, fue diseñado para cimentar la hegemonía estadounidense y anticipar las convulsiones sociales, externas e internas, que planteaba la feroz oposición del movimiento antiguerra.

Los esfuerzos por crear redes similares en la antigua Unión Soviética o en Chile muestran que había alternativas a este desarrollo, pero que esas redes fueron diseñadas y usadas para la planificación democrática o centralizada (Peters, 2016; Medina, 2011; Levine, 2018). Con el comienzo de las políticas neoliberales de los años ochenta y noventa, esta tecnología se comercializó a la vez que se construían muchas

dotaciones e infraestructuras públicas, con el apogeo de este proceso durante la administración Clinton y la privatización y comercialización de internet. El mantra de la autorregulación significaba que las compañías podían dar forma a las políticas iniciales de internet a su gusto. Mientras continuaba la vigilancia estatal, las compañías tendrían libertad para dar forma a internet durante las próximas décadas.

Esta aproximación desregulatoria prevaleció hasta la primera década de los dos mil, momento en el que los políticos en Norteamérica y, especialmente Europa, frente a las poderosas compañías tecnológicas y las amenaza a sus democracias, decidieron intervenir para frenar los principales excesos.

Desde los años setenta, la industria financiera se desarrolló paralelamente a la industria de la información y la comunicación. La digitalización hace posible la financiarización, proporcionándole un amplio abanico de aplicaciones a cambio de capital riesgo (Staab, 2019). Durante los años noventa, por ejemplo, un volumen sin precedentes de capital fue bombeado a las compañías de internet que prometían grandes oportunidades de negocio. La crisis de *las puntocom* a principios de los años dos mil frustró esos sueños, pero aquellos otros basados en el desarrollo de la publicidad se mantuvieron. Su modelo se basaba en la recolección de datos orientados a hacer los anuncios destinados a los usuarios más relevantes, de tal modo que estos gastarían más.

De esta forma, la recolección de datos estuvo presente en el corazón de internet desde el inicio. Además de la vigilancia del Estado, nació la vigilancia privada –destinada al beneficio–, permitiendo la generación y almacenaje digital de la actividad del usuario en forma de datos (Crain, 2021). Mientras que el público es muy crítico con la vigilancia del Estado (de manera acertada), la vigilancia privada destinada al beneficio se escapa con frecuencia de dicho escrutinio, a pesar de la actual cooperación entre las grandes empresas tecnológicas y el complejo militar-industrial (Levine, 2018). La participación activa del usuario en su propia vigilancia se busca mediante todo tipo de medios posibles, incluyendo estrategias como convertirla en juegos o la de generar adicción. Tal y como señalaba Blayne Haggart, investigador

en política digital de la Universidad de Brock en Canadá: "Hemos construido una economía y una sociedad dirigida por datos, en la cual la lista de lo que puede transformarse en datos y ser mercantilizado –pulsaciones, conversaciones, nuestras preferencias expresadas– está únicamente limitada por nuestra imaginación" (Haggart, 2018, s/p).

Palimpsestos de infraestructura

En la percepción popular, las innovaciones tecnológicas y los avances en informática son una historia de desmaterialización creciente –una historia que permite la creencia en la digitalización como la salvación ecológica. Tecnologías como *la nube* hacen de su ubicuidad o su desconexión del medio ambiente físico, una seña de identidad. La invisibilidad es una característica central de sistemas de infraestructuras a gran escala –se supone que no se ven. Descubrir estas historias nos ayudará a entender mejor cómo es posible la mercantilización de los datos, el coste ecológico de los mismos, y cómo estos se relacionan con el extractivismo y las relaciones coloniales.

Volviendo al período en el cual el telégrafo comenzó a unir a las metrópolis y sus colonias, particularmente a través de cables submarinos, se visibilizaba la naturaleza material de las redes de comunicación. Aunque persiste la desigualdad inherente a estas infraestructuras globales, el cambio experimentado en los actores involucrados en la financiación de los cables que yacen sobre el fondo oceánico muestra también las discontinuidades de aquellos que ostentan el poder sobre las comunicaciones globales y su infraestructura. Hace 120 años, estos cables eran financiados por imperios, que pensaban que esto les llevaría a una tutela más eficiente y a un sistema de dirección más inmediato en su tarea colonizadora, y se usaban recursos coloniales para construirlos.

Una ventaja importante de las compañías de cables británicas para controlar el mercado durante el siglo XIX fue su capacidad de aislar cables submarinos a través de la goma de gutapercha –látex natural–, similar al caucho, que procedía de las colonias de la península malaya.

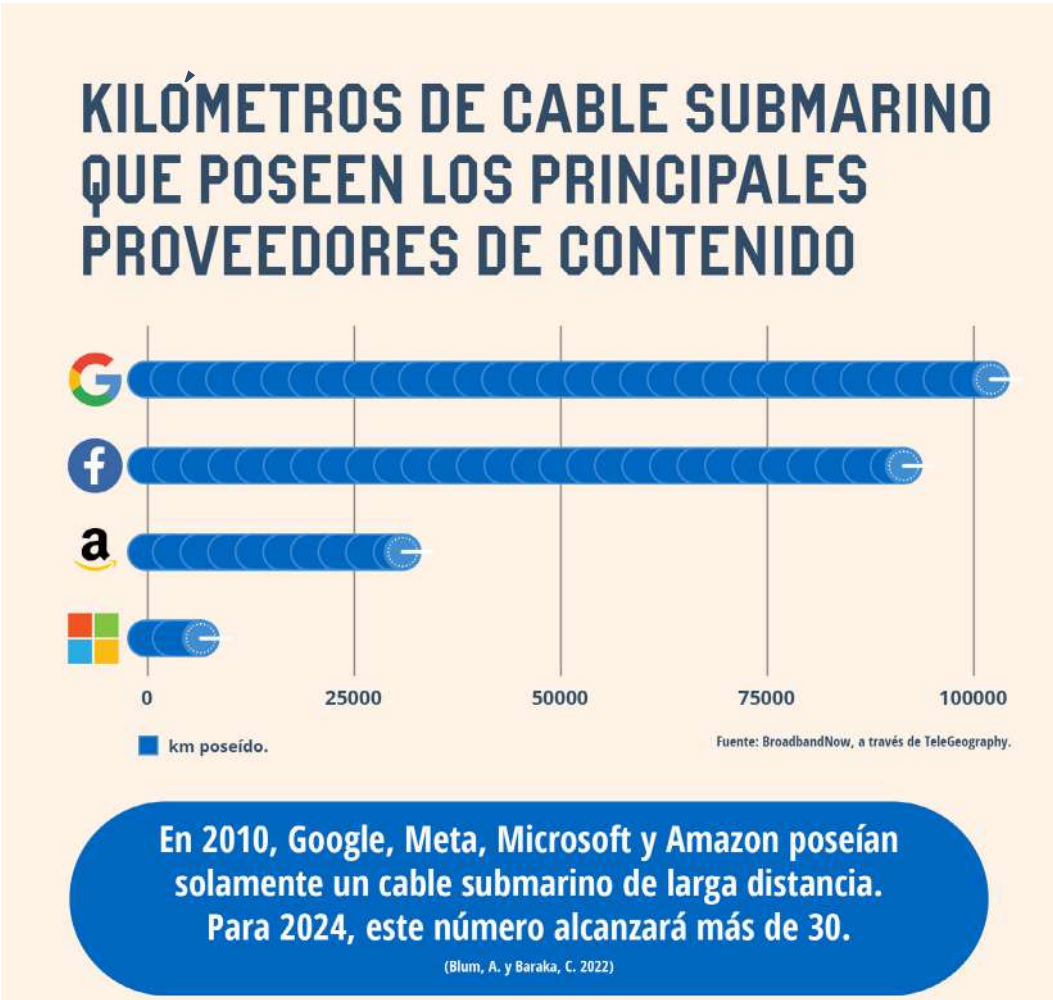
Los malayos compartieron con los oficiales coloniales británicos los conocimientos indígenas sobre su medio ambiente y esta particular savia del árbol y sus propiedades, y todo ello se transformó en algo imprescindible para el inicio de la historia de internet. Su extracción pronto se convirtió en un desastre ecológico. El primer cable transatlántico, colocado en 1857 entre el oeste de Irlanda y la zona de Terranova y Labrador, en Canadá, se aisló con 250 toneladas de goma de gutapercha, y sabemos que un árbol talado podía producir una media de 312 gramos de este material. Cuando los británicos impusieron la prohibición de tala en 1883, este árbol ya se había extinguido de muchas regiones de la actual Malasia. A principios del siglo XX, cerca de 200 mil millas náuticas (370 mil km) de cables cruzaban los fondos marinos, aislados mediante una cantidad de goma equivalente a unos 88 millones de árboles (Tully, 2009).

Hoy día, los antiguos países y personas colonizadas se tratan en primer lugar y principalmente como recursos que pueden ser aprovechados en lugar de considerarlos por sí mismos. Muchos cables de fibra óptica submarina todavía siguen las rutas establecidas durante la época colonial. Los grandes gigantes tecnológicos globales financian, construyen y controlan cada vez más nuevos cables. En 2012, Amazon, Google, Meta y Microsoft solamente eran dueños de un cable submarino de larga distancia. Para 2024, habrá más de 30. Este número incluye proyectos como el cable Equiano de Google que conectará toda la costa de África Occidental o el cable 2Africa de Meta que rodeará todo el continente y se ramificará hacia los estados del Golfo Pérsico, Paquistán y la India, dando servicio a 3.000 millones de personas con una capacidad todavía sin parangón. La construcción de sus propios cables da a las grandes compañías tecnológicas un control técnico y operativo sin precedentes –qué tráfico de datos va a dónde y a qué velocidad– y un acceso privilegiado a los datos y la posibilidad de dar servicio a 1.400 millones de potenciales usuarios de internet (Blum y Baraka, 2022).

Meta y Google se pueden permitir las grandes inversiones de capital necesarias para desplegar estos cables incluso sin tener que vender el ancho de banda, dado que los retornos de beneficio potenciales de

un nuevo usuario son considerados como una amortización suficiente a su inversión. Nanjira Sambuli, un abogado de derechos digitales con sede en Nairobi, remarca:

> Lo que es más interesante en la tecnopolítica es la *carrera para conectar a los desconectados* y retenerlos en una cierta plataforma [...] puesto que todo tiene que ver con los datos. Cuántos datos puede obtener de una persona, de tal modo que pueda vender anuncios, para crear predicciones que los tengan enganchados a lo que ofrezco (Al Jazeera, 2019).



Extractivismo (de datos)

La naturaleza colonial de la economía digital se visibiliza mejor en los viejos y en los nuevos campos del extractivismo a lo largo y ancho del globo. El extractivismo se presenta en diversas formas: la fabricación de un creciente volumen de aparatos electrónicos y digitales se basa no solo en la explotación de tierras raras, otros metales y trabajo humano, sino también en la logística de su transporte impulsada por combustibles fósiles. Es más, su producción y desecho genera residuos, contaminación y toxicidad.

La minería a menudo es el sector más letal para los personas y para los defensores de los derechos de la naturaleza, con frecuencia pertenecientes a comunidades indígenas. Los informes de la asociación Global Witness señalan que 1.733 defensores de los derechos ambientales han sido asesinados en los últimos 10 años, con muchos más que nunca fueron contabilizados, tratando de defender sus tierras de la explotación. Tanto la transición *verde* como la digital están incrementando la naturaleza extractiva de la economía.

El metal del diablo

Gran parte de la atención pública acerca de los metales necesarios para la economía digital se ha preocupado por la minería del litio en Bolivia, el trabajo esclavo e infantil en la minería artesanal del cobalto en la República Democrática del Congo, o los conflictos geopolíticos alrededor de las tierras raras. El estaño se asocia habitualmente a las latas más que a los ordenadores, pero la mitad de la oferta mundial de esta sustancia la utiliza la industria electrónica; y el 30 % es extraído en las *islas del estaño* de Bangka y Belitung en la costa de Sumatra, donde la minería ilegal convierte ricos ecosistemas de bosque tropical húmedo en vertederos tóxicos. Desde que los holandeses colonizaron las islas en la década del setenta del siglo XIX, la administración colonial ha tratado de intensificar e industrializar las práctica mineras

pre-existentes (Ross, 2014). La minería actual de baja tecnología, muy intensiva en trabajo y peligrosa ha destruido los ecosistemas costeros, que son la fuente de sustento de los pescadores locales, ha creado piscinas de agua estancada que son el nido de los vectores del dengue y la malaria, y se han convertido en una fuente de muerte para los mineros.[1]

Pequeños chips, grandes tóxicos

Incluso tras de la extracción del recurso, la producción con alta tecnología contamina y envenena a los trabajadores y sus comunidades. La producción de microchips, por ejemplo, que ha sido externalizada desde California o Nueva York a lugares más económicos y con una regulación más laxa y globalizada como *Silicon Island* (Taiwan) o *Silicon Paddy* (China), lo que implica un empleo intensivo de insumos químicos para extraer las menas. En 2002, para ensamblar un microchip se empleaba 630 más masa que la que tenía el peso final del producto en forma de insumos, en un proceso que suponía hasta 300 pasos de procesado. Esto requiere grandes cantidades de electricidad, agua y productos químicos. La compañía Taiwan Semiconductor Manufacturing Company (TSMC), por ejemplo, consume un 7,2 % de la electricidad de la isla de Taiwan, y en medio de las sequías causadas por la crisis climática, las instalaciones de TSMC consumen cerca de 63 mil millones de litros de agua cada año (Zhong y Chang Chien, 2021).

En la ciudad de Endicott, en el estado de Nueva York, miles de litros de disolventes cancerígenos como el tricloroetileno (TCE) y el percloretileno (PERC) acaban vertidos en el suelo, envenenando las aguas subterráneas y generando un incremento en las tasas de cáncer y enfermedades congénitas. Durante toda una serie de procedimientos legales emprendidos por unos 1.000 habitantes de Endicot, IBM tuvo que desclasificar el contenido de un *archivo de mortalidad corporativa*,

[1] Ver Friends of the Earth, 2012 y Simpson, 2012.

en el cual había hecho el seguimiento de los datos demográficos y la causa de muerte de 33.730 antiguos empleados. Los datos mostraban el incremento de las tasas de cáncer de pecho, intestinal y respiratorio al menos desde 1969. IBM trató de extraer las aguas contaminadas, pero a la compañía le llevó 24 años y una orden del Departamento de Conservación Ambiental del Estado de Nueva York controlar la calidad del aire e instalar sistemas de mitigación en las casas y los edificios públicos. La contaminación en Endicott no es un caso aislado (Gaydos, 2019). El valle de Santa Clara, en California, con frecuencia conocido como Silicon Valley, tiene 23 lugares catalogados como sitios *contaminados* –con sustancias peligrosas– más que ningún otro condado de EE.UU. Y, dada la situación, no está claro que una limpieza eficaz de los suelos vaya a producirse alguna vez. Muchos más lugares afrontan problemas parecidos a lo largo y ancho de todo el mundo.

Enfriamiento de los servidores, calentamiento del agua y clima

El acceso al agua juega un papel decisivo no solo en la producción de semiconductores, sino también la localización geográfica de las grandes granjas de servidores, insaciables en su hambre de poder y agua para asegurar su funcionamiento y constante refrigeración. Las empresas frecuentemente se aseguran de llegar a buenos tratos con las administraciones municipales o estatales para satisfacer su sed de agua durante décadas. Los efectos de esto se hacen visibles cada vez con más frecuencia bajo situaciones de estrés hídrico inducidas por la sequía. Por ejemplo, el Centro de Datos de la Agencia Nacional de Seguridad (NSA) en Utah (uno de los estados más secos de EE.UU.), en el momento de su construcción el tercer mayor sistema de servidores del mundo, usa cerca de 6,5 millones de litros de agua al día, que se sustraen al uso de las comunidades y los hábitats locales. Inicialmente, la NSA incluso se negó a desclasificar este dato, aludiendo a "cuestiones de seguridad nacional". Las protestas por esta situación no han

tenido mucho éxito ya que la ciudad de Bluffdale ha garantizado a la NSA agua a precios bajos durante los próximos años (Hogan, 2015).

La *efímera* nube se localiza frecuentemente en áreas rurales como Utah o las colinas de Guizhou, y países *fríos* como Finlandia, Islandia, Irlanda o Suecia. La imaginación imperial y los anuncios empresariales presentan estas localizaciones como remotas o *naturales*, lo que oculta su impacto ambiental a la vez que la intervención política que facilita su construcción. Como de costumbre, la imagen abstracta y desmaterializada de la nube oculta lo contrario.

Tierra desechable, personas desechables

Últimamente, los aparatos electrónicos y digitales, especialmente por su baja vida útil, acaban en vertederos. Cada año, el mundo desecha casi 50 millones de toneladas de residuos electrónicos. La gran mayoría de los que proceden del Norte Global acaban siendo exportados al *resto del mundo*, desde Norteamérica y Europa a Nigeria o Ghana, desde Japón y China, hasta Singapur o la India. La mayor parte de los residuos acaban en vertederos, donde los metales pesados, como el plomo, el mercurio, el cadmio y otras sustancias tóxicas se infiltran en el suelo y contaminan el agua subterránea y la cadena alimentaria. En estos lugares el reciclaje y la recogida tienen lugar en condiciones precarias a través de métodos perjudiciales y fuertemente tóxicos, incluidos el desmenuzado, la quema al aire libre y el baño electrónico en ácidos para la recolección de pequeños fragmentos de materiales preciosos que puedan ser vendidos. La exposición a humo tóxico es peligrosa para los trabajadores, con frecuencia niños, e inhibe el desarrollo del cerebro, el sistema nervioso y el sistema reproductivo. Muchas personas no alcanzan los treinta años y son víctimas de enfermedades, heridas no tratadas, enfermedades respiratorias o cáncer (Adjei, 2014).

Zygmunt Bauman dice que esta forma de colonialismo tóxico se caracteriza por la existencia de tierra y personas desechables (Bauman, 2004). Además, se extiende al mundo virtual. Los trabajadores

del sector digital en las Islas Filipinas o la India tienen que afrontar contenido pornográfico, extremadamente violento o abusivo en su trabajo para los gigantes de las redes sociales. La visión una y otra vez de videos de suicidas, decapitaciones, masacres o abusos sexuales a niños causan un trauma severo y otros daños mentales, hasta el punto de que los mismos trabajadores tratan de suicidarse. A diferencia de los moderadores que se encuentran en los EE.UU., los trabajadores de la mayoría del mundo no disponen de una asistencia psicológica adecuada ni son compensados cuando llegan a obtener sentencias legales favorables en los EE.UU. La regulación legal exime con frecuencia a las grandes firmas tecnológicas de gran parte de sus responsabilidades respecto a sus empleados, dejando a esa otra reserva global de trabajadores en esos países y dejándoles claro que son intercambiables y desechables (Dwoskin, Whlen y Cabato, 2019; Elliott y Tekendra, 2020).

La extracción de datos

Solo cuando observamos el capitalismo (digital) a través de las lentes coloniales somos capaces de entender esos procesos de extracción y desposesión, así como la frontera contemporánea de la expansión capitalista. En el impulso por abrir nuevos mercados, generar nuevo crecimiento y aprovechar cada vez más lo que está *afuera*, el capitalismo se ha dirigido *hacia el interior*. Las compañías digitales que maximizan sus beneficios han penetrado en cada vez más capas de la vida humana englobando y colonizando tiempo y espacio privado previamente no mercantilizado (Couldry y Mejias, 2019a).

Volviendo a Polanyi, esta transformación tiene toda su lógica. Si mientras que, con la mercantilización de la tierra, el trabajo y el dinero, la economía de mercado naciente podría existir solo en una sociedad de mercado, la mercantilización de los datos también requiere su propia transformación social violenta y disruptiva hacia una sociedad *datificada*. Esta transformación se expresa mediante las distintas formas que se han discutido aquí.

Más relevante aún, las relaciones sociales ya no están solamente incorporadas a un sistema económico, sino que "se transforman en sistema económico, […] la vida humana se convierte en la materia prima para el capital a través de los datos" (Polanyi, 1957, p. 117). La experiencia humana y las relaciones sociales se reducen a un insumo productivo y se transforman de modo que generan más datos, que pueden ser extraídos, abstraídos, agregados y vendidos.

Este es el fin último de las grandes tecnológicas: convertir todo en datos que finalmente generen un beneficio. Incluso si la violencia de la recolección misma de los datos no es tan evidente y grosera como lo fue durante el colonialismo histórico, la masa de datos capturados y mercantilizados, particularmente a través de su procesado automático y los algoritmos, tiene profundos efectos sobre las actuales formas de opresión racial, de género y de clase. Todo se justifica bajo la ideología de *conocer* el mundo a través de la *objetividad* de los datos.

El doble movimiento: gobernanza de datos emancipatorios y desmercantilización

Ninguna transformación a gran escala ni nuevo orden social o económico emergente ha estado libre de formas de contestación. Polanyi describe esto como un doble movimiento: las sociedades no esperaron sentadas a la mercantilización del trabajo, la tierra y el dinero. Las personas colonizadas resistieron contra la violencia colonial. La mercantilización del trabajo, la tierra y el dinero dio lugar a una reacción de creación de instituciones y reglas que protegían a la sociedad de los efectos de una mercantilización desenfrenada. Gran parte de esta regulación, como es el caso de la protección de los trabajadores o los estados de bienestar, están volviendo a ser atacadas por la mercantilización de la información y la transformación de la sociedad a través del colonialismo de los datos (Cohen, 2019). Igualmente, las comunidades que se encuentran en la línea de este frente, en la actualidad resisten diariamente a las empresas que tratan de destruir su medio ambiente

y transformarlo en zonas sacrificables. Los políticos y activistas por los derechos digitales de todo el mundo luchan continuamente contra el poder de las grandes empresas tecnológicas. Que el futuro digital sea social, ecológico y justo significa afrontar la mercantilización de los datos, y también las crisis derivadas de la mercantilización del trabajo, la tierra y el dinero.

¿Cómo podemos encontrar formas de dirigir los datos y su infraestructura material de un modo más democrático? Una respuesta legal muy popular es el reforzamiento del derecho a la privacidad como, por ejemplo, en la Unión Europea con el Reglamento General de Protección de Datos (RGPD), o la prohibición de la recolección de datos y publicidad dirigida, con la Ley de Servicios y Mercados Digitales.

Sin embargo, concebir la mercantilización de los datos simplemente como un problema que afecta a los individuos frente a las empresas no es verdaderamente emancipatorio. Salomé Viljoen, profesora de la Facultad de Derecho de Michigan, propone reconceptualizar la gobernanza de los datos de un modo más democrático, de tal forma que se considere el conocimiento generado a nivel de población, porque, incluso si hubiera formas de retirar el consentimiento individual a la extracción de los datos por parte de empresas o estados, el conocimiento sobre aquel individuo podría seguir siendo inferido de los datos agregados recolectados a partir de personas categorizadas dentro del mismo grupo demográfico.

Ser conscientes de estas relaciones entre datos y entender la gobernanza de los datos de este modo abre la puerta a concebir los datos como un bien común o de utilidad pública. Los datos tendrían que ser recopilados y usados solo por instancias que tengan una legitimidad democrática previa y cuando beneficien a los ciudadanos. Esto permitiría construir un contrapoder y reducir drásticamente la extracción de datos (Viljoen, 2021). Esto permitiría un modelo de propiedad de los datos a través de fideicomisos públicos o propiedad común, formas que están emergiendo de abajo hacia arriba (Micheli et al., 2020). Los datos existentes y los datos que están siendo recolectados por parte de las empresas privadas deberían ser transferidos al dominio y las

instituciones públicas, igual que cuando finalizan los derechos de propiedad intelectual antes de que se extingan completamente (Sadowski, Viljoen y Whittaker, 2021). Un fideicomiso como este actuando en nombre de las personas dueñas de los datos, si existe una cierta pluralidad, aseguraría el empoderamiento social frente a las poderosas empresas bajo el sistema actual.

Las aproximaciones al tratamiento de los datos como un bien común –que implica una contribución, acceso, uso y empoderamiento del ciudadano– se están implementando de modo exitoso en Barcelona (España), donde los funcionarios públicos subrayan la necesidad de transparencia, medición y confianza, y podría ser escalado (hacia arriba) a escala nacional a través de la propiedad común, instituciones públicas sujetas a vigilancia científica y fiscalización democrática que actúen independientemente de las instituciones judiciales o militares (Bria, 2018; Hind, 2019; Delacroix y Lawrence, 2019). Este empuje hacia regulaciones diferentes y creación de estructuras comunitarias para la participación en la gobernanza de los datos puede complementarse con "experiencias utópicas actuales" ("nowtopias"), espacios donde el futuro deseable esté siendo ya implementado, tales como proyectos subversivos de "comunes digitales" o a través de "una política contenciosa de activismo digital" (Beraldo y Milan, 2019).

El problema con la economía digital no reside exclusivamente en la capacidad de ciertas empresas poderosas de extraer información para su beneficio, sino más bien en la lógica colonial y extractiva sobre la cual descansa el capitalismo. Así pues, la respuesta de cualquier movimiento radical y transformador tiene que ser más amplia, más exhaustiva, y desafiar las relaciones de poder inherentes a la economía digital y al capitalismo en general, a la vez que representa también la pluralidad y la heterogeneidad de toda la realidad.

Esto requerirá luchas en áreas muy distintas. Los trabajadores de todo el mundo ya han expresado esta resistencia a través de huelgas, buscando y construyendo la solidaridad y el poder de la clase trabajadora a través de los sindicatos, pero también mediante un amplio abanico de estrategias (Piasna y Zwysten, 2022; Qadri y Raval, 2021).

Desde esos movimientos de oposición emergen nuevos modelos de propiedad en la economía digital, tales como el de las plataformas cooperativas. Más que dar apoyo a estas florecientes cooperativas locales a pequeña escala, los legisladores deberían tratar de socializar las plataformas existentes (Kwet, 2022). Esto último también incluye a (la infraestructura de) internet, que tiene que ser orientada a servir como bien público y para el bien público en lugar de tener una columna vertebral financiada con publicidad.

Aunque estas propuestas no supondrían un fin inmediato del fenómeno de la mercantilización de la información, nos situarían en el camino hacia su desmercantilización. Esta desmercantilización tiene que realizarse junto con la reducción del consumo material de la economía (digital), una reorientación hacia la suficiencia en lugar de hacia la eficiencia. Las propuestas decrecentistas identifican acertadamente la imposibilidad de desacoplar la intensidad de recursos (y emisiones) del crecimiento de la economía y la necesidad de asegurar un bienestar global (Hickel y Kallis, 2019). Es necesario establecer objetivos vinculantes para reducir la extracción de recursos. Las comunidades indígenas y locales deberían tener una verdadera capacidad de participación en las consultas sobre los proyectos extractivos que les afectan.

Los partidarios de la desmercantilización de la información deberían buscar alianzas entre ellos y aprender de los grupos de justicia climática y ambiental que se encuentran a la cabeza de las luchas locales contra los proyectos extractivistas y por un modelo posextractivista que afronte la lógica colonial que requiere la economía digital y que está devorando el medio ambiente a lo largo y ancho del planeta, con el objetivo de llegar a un futuro solidario en el que sea posible la sostenibilidad de los ecosistemas globales.

Bibliografía

Adjei, Asare (19 de abril de 2014). Life in Sodom and Gomorrah: The world's largest digital dump. *The Guardian*. https://www.theguardian.com/global-development-professionals-network/2014/apr/29/agbogbloshie-accra- ghana-largest-ewaste-dump

Al Jazeera [Al Jazeera English] (2019). Is Big Tech colonising the internet? | All Hail The Algorithm [Video]. YouTube. https://www.youtube.com/watch?v=_fC7acShZkg

Ashiagbor, Diamond (2021). Race and colonialism in the construction of labour markets and precarity. *Industrial Law Journal*, 50(4), 1–26. https://doi.org/10.1093/indlaw/dwab020

Beckert, Sven y Rockman, Seth (eds.) (2016). *Slavery's Capitalism: A new history of American economic development*. Filadelfia: University of Pennsylvania Press.

Beraldo, Davide y Milan, Stefania (2019). From data politics to the contentious politics of data. *Big Data & Society*, 6(2). https://doi.org/10.1177/2053951719885967

Berry, D. R. (2017). *The Price for Their Pound of Flesh: The value of the enslaved, from womb to grave, in the building of a nation*. Boston: Beacon Press.

Bhambra, Gurminder K. (2021). Colonial global economy: Towards a theoretical reorientation of political economy. *Review of International Political Economy*, 28(2), 307–322.

Blum, Andrew y Baraka, Carey (10 de mayo de 2022). 'Sea change', Rest of World. https://restofworld.org/2022/google-meta-underwater-cables/

Boyd, Danah y Crawford, Kate (2012). Critical questions for big data. *Information, Communication & Society*, 15(5), 662– 679. https://doi.org/10.1080/1369118X.2012.678878

Bria, F. (2018). A new deal on data. En McDonnell, John (ed.), *Economics for the many (*pp. 164– 171). London: Verso.

Cohen, Julie E. (2019). *Between Truth and Power: The legal constructions of informational capitalism.* Oxford: Oxford University Press.

Couldry, Nick y Mejias, Ulises (2019a). *The Cost of Connection: How data is colonizing human life and appropriating it for capitalism*. Stanford: Stanford University Press.

Couldry, Nick y Mejias, Ulises (2019b). Making data colonialism liveable: How might data's social order be regulated? *Internet Policy Review*, 8(2). https://doi.org/10.14763/2019.2.1411

Crain, Matthew (2021). Profit over Privacy. How surveillance advertising conquered the internet. Minneapolis: University of Minnesota Press.

Delacroix, Silvie y Lawrence, Neil D. (2019). Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance. *International Data Privacy Law*, 9(4), 236–252. https://doi.org/10.1093/idpl/ipz014

Dwoskin, Elizabeth, Whlen, Jeanne y Cabato, Regine (25 de julio de 2019). Content moderators at YouTube, Facebook and Twitter see the worst of the web—and suffer silently. *The Washington Post*. https://www.washingtonpost. com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation- workers-is-paying-price/

Elliott, Vittoria y Tekendra, Parmar (22 de julio de 2020). The despair and darkness of people will get to you. *Rest of World*. https://restofworld.org/2020/facebook-international-content-moderators/

Ensmenger, Nathan (2018). The environmental history of computing. *Technology and Cutlure*, 59(4), S7–S33. https://doi.org/10.1353/tech.2018.0148

Fraser, Nancy (2014). Can society be commodities all the way down? Post-Polanyian reflections on capitalist crisis. *Economy and Society*, 43(3), 541–558. https://doi.org/10.1080/03085147.2014.898822

Friends of the Earth (26 de noviembre de 2012). Mining for smartphones: The true cost of tin. https://www.foe.co.uk/sites/ default/files/downloads/tin_mining.pdf

Gaydos, Ellyn (7 de diciembre de 2019). In the shadow of big blue: The birthplace of IBM is struggling to live in its shadow. *Logic*, 9. https://logicmag.io/nature/in-the-shadow-of-big-blue/

Global Witness (2022). A deadly decade for land and environmental activists—with a killing every two days. https://www.globalwitness.org/en/press-releases/deadly-decade-land-and-environmental-activists- killing-every-two-days/

Haggart, Blayne (2018). The government's role in constructing the data-driven economy. *Center for International Governance Innovation*. https://www.cigionline.org/articles/governments-role-constructing-data-driven- economy/

Hickel, Jason y Kallis, Giorgos (2019). Is green growth possible? *New Political Economy*, 25(4), 469–486. https://doi.org/10.1080/13563467.2019.1598964

Hind, Dan (20 de septiembre de 2019). The British digital cooperative: A new model public sector institution. *Common Wealth* [en línea]. https://www.common-wealth.co.uk/reports/the-british-digital-cooperative-a-new-model-public- sector-institution

Hogan, Mél (2015). Data flows and water woes: The Utah data center. *Big Data & Society,* 2(2). https://doi.org/10.1177/2053951715592429

Kwet, Michael (2022). The digital tech deal: A socialist framework for the twenty-first century. *Race and Class*, 63(3), 63–84. https://doi.org/10.1177/03063968211064478

Levine, Yasha (2018). *Surveillance Valley: The secret military history of the internet*. Nueva York: Public Affairs.

Mazzucato, Mariana (2013). *The Entrepreneurial State: Debunking public vs. private sector myths*. Londres: Anthem Press.

Medina, Edén (2011). *Cybernetic Revolutionaries: Technology and politics in Allende's Chile*. Cambridge, MA: MIT Press.

Micheli, Marina et al. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, 7(2). https://doi.org/10.1177/2053951720948087

Peters, Benjamin (2016). *How Not to Network a Nation: The uneasy history of the Soviet internet*. Cambridg: MIT Press.

Piasna, A. y Zwysten, W. (2022). New wine in old bottles; organizing and collective bargaining in the platform economy. *International Journal of Labour Research*, 11(1-2), 36-46. https://www.ilo.org/actrav/ international-journal-labour-research/WCMS_856837/lang–en/index.htm

Polanyi, Karl (1957 [1944]). *The Great Transformation: The political and economic origins of our time*. Boston: Beacon Press. Existe versión en español: Polanyi, Karl (1989). *La Gran Transformación*. Madrid: La Piqueta. https://traficantes.net/sites/default/files/Polanyi,_Karl_-_La_gran_transformacion.pdf

Qadri, Rida y Raval, Noopur (2021). Mutual aid stations. *Logic 13*. https://logicmag.io/distribution/mutual-aid-stations/

Ross, Corey (2014). The tin frontier: Mining, empire, and environment in Southeast Asia, 1870s-1930s. *Environmental History*, 19, 454-479. http://dx.doi.org/10.1093/envhis/emu032

Sadowski, Jathan, Viljoen, Salomé y Whittaker, Meredith (2021). Everyone should decide how their digital data are used—not just tech companies. *Nature*, 595, 169–171. https://doi.org/10.1038/d41586-021-01812-3

Simpson, C. (24 de Agosto de 2012). The deadly tin inside your smartphone. *Bloomberg*. https://www.bloomberg.com/news/articles/2012-08-23/the-deadly-tin-inside-your- smartphone

Staab, Philipp (2019). *Digitaler Kapitalismus*. Berlín: Suhrkamp.

Starosielski, Nicole (2015). *The Undersea Network*. Londres: Duke University Press.

Tully, John (2009). A Victorian ecological disaster: Imperialism, the telegraph, and gutta-percha. *Journal of World History*, 20(4), 559–579. https://www.jstor.org/stable/40542850

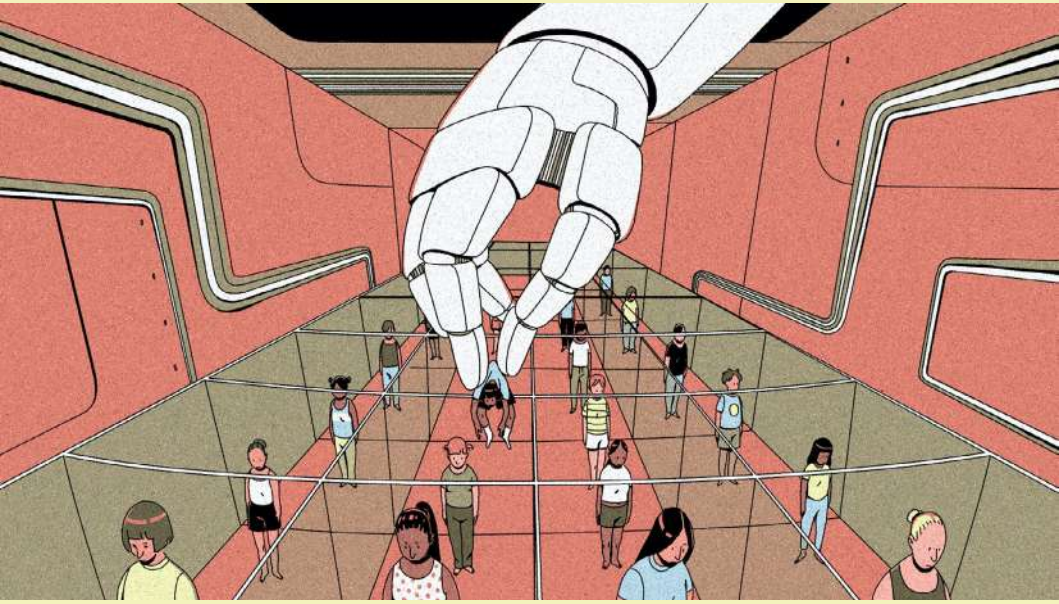
Viljoen, Salomé (2021). A relational theory of data governance. *The Yale Law Journal*, 131(2), 370–781.https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance

Zhong, Raymond y Chang Chien, Amy (8 de abril de 2021). Drought in Taiwan pits chip makers against farmers. *The New York Times*. https://www.nytimes.com/2021/04/08/technology/taiwan-drought-tsmc-semiconductors.html

Bauman, Zygmunt (2004). *Wasted Lives: Modernity and its outcasts*. Cambridge: Polity.

Lo que oculta la inteligencia artificial

Microsoft y las niñas vulnerables del norte de Argentina



Tomás Balmaceda, Karina Pedace y Tobías Schleider

Traducción al español por Mercedes Camps
Ilustración de Anđela Janković

Bajo el ropaje de la neutralidad valorativa y el deslumbramiento que nos produce la novedad, la tecnología está consolidando la opresión de las naciones centrales sobre los países periféricos a través de grandes empresas que ocupan espacios en comunidades vulnerables

En 1939 se estrenó la película *El Mago de Oz*. Uno de sus protagonistas estelares fue el perro adiestrado Terry (en el rol de Toto), que en el momento era considerado "el animal más inteligente del planeta". La cuestión de la inteligencia animal ocupó a buena parte de los pensadores de la época mientras en paralelo crecía el interés por entender si una máquina podía pensar, un claro desafío al sentido común del momento, que lo descartaba de plano, y que fue cuestionado de manera concreta 10 años después de que la cinta debutara en el cine por el trabajo del matemático británico Alan Turing.[1] Durante gran parte del siglo XX, la idea de que los animales o las máquinas pudieran pensar era absolutamente descabellada ¡cuánto ha cambiado desde entonces!

A comienzos de 2016, *El Mago de Oz* fue el libro escogido por el gobernador de Salta, en Argentina, para distribuir entre estudiantes de su provincia que estaban aprendiendo a leer. Las niñas descubrieron en el texto firmado por L. Frank Baum que detrás de la *magia* siempre hay un hombre. Cuando pasaron a la adolescencia, ese aprendizaje se extendió a otros órdenes más concretos de sus vidas: que no hay magia, sino hombres, detrás de la pobreza, de las promesas, de los desengaños y de los embarazos.

En ese entonces la inteligencia artificial había dejado de ser el desafío de Turing para convertirse en el área de conocimiento favorita de las empresas más poderosas e influyentes del mundo y, gracias a

[1] Wikipedia, la enciclopedia libre (2023). https://es.wikipedia.org/wiki/Alan_Turing

aplicaciones atractivas en dispositivos personales como teléfonos celulares y plataformas de *streaming*, logró popularizarse entre muchas personas.

Hasta hace unos pocos años solo escuchábamos la frase "inteligencia artificial" para hacer referencia a HAL 9000[2] de *2001. Odisea del espacio* o al androide Data de *Star Trek*, pero hoy pocos se sorprenden de su uso cotidiano. El consenso en los medios de comunicación y en cierta bibliografía académica es que nos encontramos frente a una de las revoluciones tecnológicas más importantes de la historia.

Sin embargo, el deslumbramiento que esta tecnología –que parece salida de un cuento de hadas o de una película de ciencia ficción– genera, esconde su verdadera naturaleza: se trata de una creación tan humana como los mecanismos que el supuesto mago de Oz quería hacer pasar como eventos divinos y sobrenaturales. En manos del aparato estatal y de grandes corporaciones, la *inteligencia artificial* puede ser un instrumento eficaz de control, vigilancia, dominación y consolidación del *statu quo*, tal como quedó de manifiesto cuando el gigantesco Microsoft se alió al gobierno de Salta con la promesa de que un algoritmo podría ser la solución a la crisis de deserción escolar y embarazo adolescente de aquella región argentina.

Algoritmos que predicen embarazos adolescentes

Un año después de que entregara copias de *El mago de Oz* a las escuelas de su provincia, el gobernador de Salta, Juan Manuel Urtubey, anunció un convenio con la filial nacional de Microsoft para la aplicación de una plataforma de inteligencia artificial destinada a la prevención de lo que calificó como "uno de los problemas más urgentes" de la región. Se estaba refiriendo al alza en el número de embarazos adolescentes. Según las estadísticas oficiales, en 2017, más del 18 % de los

[2] Wikipedia, la enciclopedia libre (2023). https://es.wikipedia.org/wiki/HAL_9000

partos totales de la provincia fueron de gestantes menores de diecinueve años: 4.914 hijos e hijas, a razón de más de trece por día.

En la promoción de su iniciativa, el gobernador manifestó: "Lanzamos un programa para prevenir el embarazo adolescente utilizando inteligencia artificial de la mano de una reconocidísima empresa de software del mundo. Con la tecnología vos podés prever cinco o seis años antes, con nombre, apellido y domicilio, cuál es la niña, futura adolescente, que está en un 86 % predestinada a tener un embarazo adolescente" (Página 12, 2018).

Casi con la misma fanfarria con la que el mago de Oz recibía a los visitantes que lograban recorrer el camino empedrado de ladrillos dorados, Microsoft daba el anuncio del acuerdo como una "iniciativa innovadora, única en el país y un gran paso en el proceso de transformación digital de la provincia".[3]

La alianza entre la gigante tecnológica y el gobierno tenía un tercer actor, la Fundación CONIN, presidida por Abel Albino, médico activista en contra de la legalización del aborto y del uso de preservativos (Perfil, 2018).

Es esta alianza la que explica los intereses políticos, económicos y culturales detrás de este programa: una consolidación de la noción de *familia* en la que el sexo y los cuerpos de las mujeres están al servicio de la reproducción, supuestos fines últimos y sagrados que deben ser protegidos a toda costa. Es una visión conservadora conocida desde hace siglos en América Latina, pero que aquí se viste de ropajes vistosos gracias a la complicidad de una compañía de capitales estadounidenses como Microsoft y la utilización de términos como *inteligencia artificial* que, como explicaremos en la siguiente sección, parece ser suficiente para garantizar eficacia y modernidad.

[3] Ver Microsoft News Center LATAM (2017). Microsoft y el gobierno de Salta firman un acuerdo para aplicar la inteligencia artificial en la prevención de los problemas más urgentes. https://news.microsoft.com/ es-xl/microsoft-gobierno-salta-firman-acuerdo-aplicar-la-inteligencia-artificial-la-prevencion-los-problemas-masurgentes/

En esos anuncios, se informó, además, parte de la metodología de trabajo. Por ejemplo, se comunicó que la información de base "es entregada voluntariamente por las personas" y permite "trabajar en la prevención del embarazo adolescente y la deserción escolar. Los algoritmos inteligentes permiten identificar características en las personas que podrían derivar en alguno de estos problemas y advierten al gobierno". El Coordinador de Tecnología del Ministerio de Primera Infancia de Salta, Pablo Abeleira, declaró que "a nivel tecnológico, el modelo que desarrollamos tiene un nivel de precisión de casi un 90% de una prueba piloto realizada en Salta capital" (Alonso, 2018).

Pero ¿qué se escondía detrás de los artificios?

El mito de una inteligencia artificial objetiva y neutral

Aunque ya está instalada no solo en el discurso público sino también en nuestra vida cotidiana, en ocasiones nos parece que todas las personas saben a qué nos referimos cuando hablamos de *inteligencia artificial* (IA). Sin embargo, el término está lejos de ser unívoco. No solo porque suele ser utilizada como una noción paraguas bajo la que aparecen conceptos vinculados y muy cercanos pero que no son sinónimos, como *aprendizaje automatizado* (*machine learning*), *aprendizaje profundo* (*deep learning*) o *computación cognitiva*, entre otros. Sino porque un análisis más pormenorizado revela que la misma noción de inteligencia en este contexto es polémica.

En este texto, usaremos IA para hacer referencia a sistemas o modelos de algoritmos que pueden procesar grandes volúmenes de información y datos a la vez que pueden *aprender* y mejorar en su tarea más allá de cómo fueron programados originalmente. Por ejemplo, es un caso de IA un algoritmo que, luego de procesar cientos de miles de fotos de gatos, puede extraer lo que necesita para poder reconocer a un gato en una nueva imagen, sin confundirlo con un juguete o un almohadón. A medida que se le entregan más y más fotografías, en general más aprenderá y menos errores cometerá.

Estos desarrollos de IA se están dando en todo el mundo y ya están presentes en tecnologías cotidianas como el reconocimiento de voz de asistentes virtuales como Siri y Alexa o en proyectos más ambiciosos como automóviles que no necesitan conductor o estudios para poder detectar de manera temprana enfermedades como el cáncer. El campo de aplicación de estos desarrollos es vastísimo y afecta a muchas industrias y sectores de la sociedad, como la economía, con el auge de algoritmos que prometen sugerir las mejores inversiones en la bolsa de valores; la política, con campañas en redes sociales a favor o en contra de un candidato creadas para interpelar a distintos individuos en particular a partir de sus preferencias y conductas en la web, o en la cultura, con recomendaciones personalizadas en plataformas de *streaming* de series, películas o música.

El suceso de estas aplicaciones de la tecnología y las promesas de beneficios que hasta hace algunos años sólo existían en la ciencia ficción consiguieron sobredimensionar la percepción de lo que realmente puede hacer la IA. Hoy es considerada en vastísimos espacios como el punto máximo de la actividad racional, libre de prejuicios, pasiones y cualquier error humano.

Sin embargo, esto no es más que un mito. No existe algo tal como una *IA objetiva* o libre de valores humanos. Es inexorable el impacto de nuestra condición humana –quizás demasiado humana– sobre la tecnología.

Una manera de dejar en claro esto es quitar ciertos velos tras los que se esconde un término como *algoritmo*. Desde la filosofía de la tecnología, podemos distinguir entre al menos dos modos de caracterizarlo conceptualmente. En sentido *estrecho*, un algoritmo es un constructo matemático que se selecciona dada su eficacia pasada en la resolución de tareas similares a las que plantea el problema que ahora se pretende resolver (como las redes neuronales profundas, las redes bayesianas o las cadenas de Markov). [4] En sentido *amplio*, por su

[4] Ver Wikipedia (2023). https://es.wikipedia.org/wiki/Aprendizaje_profundo ; https://es.wikipedia.org/wiki/Red_bayesiana; https://es.wikipedia.org/wiki/Cadena_de_M%C3%A1rkov

parte, un algoritmo es un sistema tecnológico que comprende varios insumos como los datos de entrenamiento, que producen un modelo estadístico diseñado, ensamblado e implementado para resolver un problema práctico formulado previamente.

Todo comienza con la concepción ingenua en torno a los datos. Estos surgen de un proceso de selección y abstracción y, en consecuencia, no son nunca una descripción objetiva del mundo, sino que son inexorablemente parciales y sesgados en la medida en que resultan de decisiones y elecciones humanas. Así, por ejemplo, se decide incluir ciertos atributos y dejar de lado otros.

Lo mismo sucede con la noción misma de predicción que surge de los datos, ya que una cuestión clave para el uso gubernamental de la ciencia de datos en general y del aprendizaje automatizado en particular estriba en decidir qué medir y cómo medirlo a partir de una definición del problema que se pretende abordar, lo que lleva a elegir el algoritmo, en sentido estrecho, que se evalúa como más eficiente para esa tarea, sin perjuicio de que pueda tener consecuencias letales (Brunet, Font y Rodríguez, 2022). Por consiguiente, la gravitación humana es crucial para establecer qué problema se quiere solucionar.

Así, queda claro que hay un vínculo inextricable entre la IA y una secuencia de decisiones humanas. Allí donde el aprendizaje automatizado nos provee las ventajas del rápido procesamiento de una voluminosa cantidad de datos y la capacidad de extraer patrones a partir de ellos, hay una serie de instancias donde la supervisión humana no solo es posible, sino necesaria.

Desnudando a la IA

Cuando Dorothy, el Hombre de Hojalata, el León y el Espantapájaros logran conocer al mago de Oz quedan fascinados por la voz grave y sobrenatural de este ser, que en la versión fílmica de 1939 tiene el timbre de Frank Morgan y se presenta como un altar de fuego y humo místico. Sin embargo, Toto, el perro de la niña, no parece quedar

tan impresionado y muerde una cortina hasta dejar al descubierto el engaño: hay alguien al mando de una serie de palancas y botones conduciendo todo lo que sucede en el escenario. Muerto de miedo y vergüenza, el supuesto mago intenta mantener la farsa: "No le presten atención al hombre detrás del telón". Pero, acorralado por los protagonistas, debe confesar su engaño: "Solo soy un hombre normal", le confiesa a Dorothy y a sus amigos. El Espantapájaros, sin embargo, lo corrige al instante: "Eres más que eso: ¡eres una estafa!".

Cuando le quitamos los ropajes y vestidos lujosos a la IA la podremos ver tal y como realmente es: un producto del accionar humano que, por lo tanto, lleva en su seno las marcas de sus creadores. En ocasiones, incluso, se la considera como similar en sus procesos al pensar humano pero carente de errores o prejuicios. Así, frente a la extendida y persuasiva retórica acerca de su neutralidad valorativa y la objetividad que le sería concomitante, debemos analizar la ineludible gravitación de intereses humanos calificados en diferentes etapas de esta supuesta tecnología mágica.

La promesa que Microsoft y el gobierno salteño de poder predecir "cinco o seis años antes, con nombre, apellido y domicilio, cuál es la niña, futura adolescente, que está en un 86 % predestinada a tener un embarazo adolescente" terminó siendo solo una promesa incumplida.

Y el fiasco comenzó con los datos: se utilizaron bases reunidas por el gobierno provincial y organizaciones de la sociedad civil en barrios de bajos ingresos de Salta capital durante 2016 y 2017. La encuesta llegó a poco menos de 300 mil personas, de las cuales 12.692 eran niñas y adolescentes entre 10 y 19 años. En el caso de las menores de edad, la información fue recogida luego de obtener el consentimiento de "los jefes de hogar" (sic).

Estos datos nutrieron un modelo de aprendizaje automático que, según sus implementadores, permite predecir, con un grado cada vez mayor de precisión, qué niñas y adolescentes cursarán un embarazo en el futuro. Se trata de un absoluto absurdo: Microsoft estaba vendiendo un sistema que prometía algo técnicamente imposible (Eubanks, 2018). Esto es, se obtiene un listado de personas a las cuales les

fue asignada una probabilidad de embarazo. Los algoritmos, lejos de autoejecutar políticas, brindaban la información al Ministerio de Primera Infancia para que abordara los casos identificados.

No se precisó desde el Estado salteño en qué consistiría ese abordaje, ni los protocolos empleados, ni las acciones de seguimiento previstas, ni el impacto de las medidas aplicadas –ni si ese impacto se ha medido de algún modo–, ni los criterios de selección de los organismos no gubernamentales o fundaciones involucrados, ni el rol de la iglesia.

El proyecto también tuvo fallas técnicas graves: según una investigación de la World Web Foundation (Ortiz Freuler e Iglesias, 2018), no existe información accesible sobre las bases de datos empleadas, ni sobre la hipótesis que sirve de apoyo para el diseño de los modelos, ni sobre el proceso de diseño de los modelos finales, criticando la opacidad del proceso. Además, se ha sostenido que la iniciativa omite evaluar cuáles son las inequidades que se pueden producir y prestar especial atención a los grupos minoritarios o vulnerables que pueden verse afectados, amén de las dificultades de trabajar con un rango de edad tan amplio en los relevamientos y el riesgo de discriminación o aun criminalización inherente al sistema.

Los especialistas coincidieron en que hubo una contaminación sutil de los datos de evaluación ya que los datos sobre los cuales se evalúa el sistema no son distintos de los datos que se usan para entrenarlo. Por otra parte, los datos son inadecuados para el fin que se persigue. Estos datos provinieron de una encuesta a adolescentes que residían en la provincia de Salta, que indagaba información sobre su persona (edad, etnia, país de origen, etc.), su entorno (si contaba con agua caliente en su vivienda, con cuántas personas cohabitaba, etc.) y sobre si había cursado o estaba cursando un embarazo. Ahora bien, la pregunta que se intentaba responder a partir de estos datos *actuales* era si una adolescente podía cursar un embarazo *en el futuro*, algo que, más que una predicción, tiene el aspecto de una premonición. Eran, además, informaciones sesgadas porque los datos sobre embarazos

adolescentes, por la sensibilidad inherente a esta clase de temas, tienden a estar incompletos o, directamente, ocultos.

Los investigadores del Laboratorio de Inteligencia Artificial Aplicada del Instituto de Ciencias de la Computación de la Universidad de Buenos Aires determinaron que, además de utilizar estos datos poco confiables, la iniciativa de Microsoft adolece de desaciertos metodológicos serios. Además, plantean el riesgo de tomar medidas incorrectas a los responsables de políticas públicas: "Las técnicas de inteligencia artificial son poderosas y demandan responsabilidad por parte de quienes las emplean; son solo una herramienta más, que debe complementarse con otras, y de ningún modo reemplazan el conocimiento o la inteligencia de un experto", especialmente en un área tan sensible como la salud pública y los sectores vulnerables.[5]

Y es que este es uno de los nudos conflictivos graves: aun si fuera posible (lo cual no parece ser el caso) *predecir* el embarazo adolescente, no queda claro *para qué* se haría: la *prevención* permanece ausente en todo el proceso. Considerar un riesgo alto de estigmatización de niñas y adolescentes por esta causa es, entonces, inevitable.

La IA como herramienta del poder contra las poblaciones vulnerables

Desde el inicio, la alianza entre Microsoft, el gobierno salteño y la Fundación CONIN se fundó en preconceptos que no solo son cuestionables sino que se enfrentan a principios y normas amparadas por la Constitución argentina y las convenciones internacionales incorporadas al sistema nacional. Así, se parte, de manera incontestable, de la idea de que el embarazo (infantil y adolescente) es una catástrofe que, en ciertos casos, sucederá indefectiblemente si no se

[5] Laboratorio de Inteligencia Artificial Aplicada (2018). Sobre la predicción automática de embarazos adolescentes. https://liaa.dc.uba.ar/es/sobre-la-prediccion-automatica-de-embarazos-adolescentes/

interviene de manera directa para evitarla. Esta premisa apareja, de manera correlativa, una postura muy difusa respecto de la atribución de responsabilidades.

Por un lado, quienes planearon y desarrollaron el sistema parecen ver al embarazo como un suceso que se da sin responsabilidad de nadie. Por otro, colocan su responsabilidad en las niñas o adolescentes embarazadas. Esta anfibología, en una u otra de sus alternativas, conduce en primer lugar a la objetivación de las personas involucradas y a la invisibilización de los responsables; para empezar, los hombres (o adolescentes, o niños, pero principalmente hombres) que contribuyeron de manera necesaria al embarazo (suele afirmarse, con un burdo giro eufemístico, que la niña o adolescente "se embarazó"). Pero, en segundo término, también soslaya que, en gran parte de los casos de embarazo de jóvenes, y en todos los de niñas, el consentimiento de la persona gestante no solo no puede presuponerse, sino que debe descartarse. Dicho en pocas palabras, esta posición oculta un aspecto del fenómeno que no podría ser más relevante: todos los embarazos de niñas y muchos de los de jóvenes son el producto de una violación.

En otro plano, y ya reparando en el aspecto menos atendido del sistema, esto es, la predicción de la deserción escolar, se presupone (y se concluye en) que un embarazo de una estudiante apareja de manera inexorable el abandono de la escolaridad. Si bien no puede ignorarse que, de hecho, el embarazo y la maternidad tempranas importan un costo de oportunidad para las mujeres, lo cierto es que la interrupción o el abandono de la trayectoria educativa no es una consecuencia inevitable, y existen programas y políticas inclusivas que han demostrado ser exitosos para contribuir a su evitación o su merma.

Desde una visión más general, el sistema y sus aplicaciones afectan derechos que forman parte del espectro de los derechos sexuales, considerados como derechos humanos. La sexualidad es un aspecto nuclear en el desarrollo de las personas, con independencia de si deciden o no reproducirse. Cuando se trata de menores de edad, han de marcarse diferencias de acuerdo con sus capacidades evolutivas, aunque siempre teniendo en cuenta que la orientación de las niñas y

los niños por parte de los padres u otras personas responsables deben priorizar sus capacidades para ejercer derechos en su propio nombre y beneficio. En lo que hace a los derechos sexuales en particular, esas consideraciones son específicas. Por ejemplo, deben respetarse las circunstancias particulares de cada niña, niño o adolescente, su nivel de comprensión y madurez, su salud física y mental, el vínculo con sus familiares y, eventualmente, la situación concreta que le toca enfrentar.

Este uso de la IA afecta de manera concreta derechos de las niñas o jóvenes (también potenciales) gestantes. En primer término, hay una afectación del derecho a la autonomía personal de las niñas y jóvenes que fueron materia prima del proyecto. Ya se hizo mención a su objetivación, al trato indiferente respecto de sus intereses particulares en pos de un supuesto interés general. Las niñas y adolescentes no son si quiera consideradas sujetos de derecho y sus deseos y preferencias personales son desconocidos por el Estado.

En este proyecto de Microsoft la IA fue utilizada como una herramienta de poder contra niñas y jóvenes, que fueron catalogadas sin su consentimiento (ni, aparentemente, su conocimiento). Las consultas pertinentes fueron evacuadas, según los promotores del sistema, por los *jefes de familia* (en especial, sus padres), sin siquiera invitarlas a participar. Y, además, los cuestionarios tratan sobre cuestiones personalísimas (su intimidad, su vida sexual, etc.) sobre cuyos detalles sus padres, por lo habitual, no estarían en condiciones de responder sin invadir su esfera de privacidad o –algo que parece también muy grave– basarse en suposiciones o en prejuicios que el Estado asumirá como verdaderos y legítimos.

También se vulneraron otros derechos, como el de intimidad, privacidad y libertad de expresión u opinión mientras que los derechos a la salud y educación corren riesgo de ser desconocidos, a pesar de las manifestaciones de las autoridades y de la multinacional respecto de su intención de cuidar a las niñas y adolescentes. Finalmente, merece mención un derecho conexo que, en el contexto especial del proyecto, cobra una relevancia singular: el derecho a la libertad de pensamiento, de conciencia y de religión.

No nos animamos a sugerir que el episodio tuvo, como en El Mago de Oz, un final feliz. Pero sí que el proyecto de Microsoft no duró mucho. Aunque su interrupción no aconteció por las críticas de los activismos sino por un motivo mucho más mundano: en 2019 se desarrollaron elecciones nacionales en la Argentina y Urtubey no logró ser reelegido. La nueva gestión descontinuó varios programas, incluyendo el de uso de algoritmos para predecir embarazos, y degradó al Ministerio de Primera Infancia, Niñez y Familia al rango de secretaría.

Lo que oculta la IA

Los efectos de humo y luces de la retórica de los desarrollos de inteligencia artificial valorativamente neutrales y objetivos parecen desmoronarse cuando se enfrenta a aquellas voces que aseguran mostrar su imposibilidad por principio, tal como señalamos en la primera sección, como cuando se exhibe la participación de analistas humanos en numerosas etapas del desarrollo de los algoritmos. Son hombres y mujeres quienes determinan el problema al que hay que dar respuesta, quienes los diseñan y preparan los datos, seleccionan qué algoritmos de aprendizaje automático son los más apropiados, interpretan críticamente los resultados del análisis y planifican la acción adecuada a tomar en función de las ideas que el análisis ha revelado.

El avance de esta tecnología no está acompañado por una suficiente reflexión y discusión abierta acerca de sus consecuencias no deseadas. Parece prevalecer en la sociedad la noción de que la aplicación de algoritmos en diferentes ámbitos no sólo es garantía de eficiencia y rapidez sino también de la no intervención de los prejuicios humanos, que pueden *ensuciar* el prístino accionar de los códigos que son el núcleo de los algoritmos. Así, se da por sentado que la IA fue creada para mejorar a la sociedad en su conjunto o, con más modestia, a ciertos procesos y productos. Sin embargo, no solo no se problematiza lo más elemental, esto es: para quién representaría esto una mejora, quién se beneficiaría, quién evalúa la mejora –¿los ciudadanos?, ¿el Estado?,

¿las empresas?, ¿las adolescentes salteñas?, ¿los adultos que abusaron de ellas?– sino que no parece haber una real conciencia de la dimensión de su impacto social o de la necesidad de discutir si tal cambio es evitable.

Las continuas novedades sobre la inserción de la IA en nuevos ámbitos son recibidas como un dato que no sorprende más que por lo novedoso, y que, inexorable como el avance del propio tiempo, no puede ser impedido o revisado. La creciente automatización de procesos que antes eran realizados por humanos puede generar alarma y desazón, pero no el interés por tratar de detenerlo o preguntarse cuál es el futuro del trabajo o el de las personas una vez que la IA se haga cargo de nuestras tareas laborales. Se impone una serie de preguntas que raramente se formulan: ¿es eso algo deseable?, ¿para qué sector de la sociedad?, ¿quién se beneficiará de esta transformación y quién saldrá perdiendo?, ¿qué podemos esperar de un futuro en el que gran parte de las ocupaciones tradicionales serán llevadas adelante por máquinas? No parece haber tiempo ni espacios para discutir sobre eso: la automatización simplemente ocurre y solo nos resta quejarnos por el mundo perdido o maravillarnos por lo que es posible lograr hoy.

Esta pasividad frente al continuo avance de la tecnología en nuestra vida privada, pública, laboral y cívica parece posible gracias a la confianza generada por la creencia de que estos desarrollos son *superiores* a lo que se podría conseguir a través del mero esfuerzo humano. De acuerdo con esto, ya que la IA es mucho más poderosa, es *inteligente* (la etiqueta *smart* hoy se aplica a teléfonos celulares, aspiradoras y cafeteras, entre otros objetos que harían sonrojar a Turing) y está libre de sesgos e intencionalidades. Sin embargo, como hemos señalado, es imposible por principio plantear una IA valorativamente neutra. Dicho en pocas palabras y de manera clara: los sesgos están presentes en todas las etapas del diseño, las pruebas y la aplicación de los algoritmos y, por eso mismo, son muy difíciles de identificar y más arduos aún de corregir. Sin embargo, es una tarea necesaria para desenmascarar su supuesto carácter aséptico, carente de los valores y errores humanos.

Un enfoque centrado en los peligros de la IA, junto con el optimismo sobre su potencial, puede conducir a una dependencia excesiva de la IA como una solución a nuestras preocupaciones éticas, a un enfoque en que la IA deba responder a los problemas generados por la IA. Si los problemas se consideran únicamente tecnológicos, deberían requieren únicamente soluciones tecnológicas. En cambio, tenemos decisiones humanas disfrazadas de decisiones tecnológicas. Necesitamos un enfoque diferente.

El caso de algoritmos que predicen embarazos adolescentes en Salta deja al descubierto la inviabilidad de la imagen de pretendida objetividad y neutralidad de la inteligencia artificial. Al igual que Toto, no podemos dejar de ver al hombre detrás del telón: el desarrollo de algoritmos no es neutral, sino que se realiza a partir de una decisión en medio de muchas posibles elecciones. En este sentido, como el diseño y la funcionalidad de un algoritmo reflejan los valores de sus diseñadores y de sus usos pretendidos, los algoritmos inexorablemente conducen a decisiones sesgadas. Hay decisiones humanas en la definición del problema, el diseño y la preparación de datos, la selección del tipo de algoritmo, la interpretación de los resultados y la planificación de acciones a partir de su análisis. Sin una supervisión humana calificada y activa, ningún proyecto de algoritmo de inteligencia artificial podrá lograr sus objetivos y ser exitoso. Los mejores resultados de la ciencia de datos se producen cuando la experiencia humana y la potencia de los algoritmos trabajan de forma conjunta.

Los algoritmos de inteligencia artificial no son mágicos, pero tampoco tienen que ser, como sostenía el Espantapájaros, una estafa. Basta con reconocer que son humanos.

Bibliografía

Alonso, Alejandro (28 de marzo de 2018). Microsoft democratiza la IA y los servicios cognitivos. *It.sitio*. https://www.itsitio.com/es/microsoft-democratiza-la-ia-y-los-servicios-cognitivos/

Brunet, Pere, Font, Tica y Rodríguez, Joaquín (2022). Robots asesinos: 18 preguntas y respuestas. https:// centredelas.org/publicacions/robots-asesinos-18-preguntas-y-respuestas/?lang=

Eubanks, Virginia (2018). *Automating Inequality; How high-tech tools profile, police and punish the poor*. Nueva York: St Martin's Press.

Laboratorio de Inteligencia Artificial Aplicada (2018). Sobre la predicción automática de embarazos adolescentes. https://liaa.dc.uba.ar/es/sobre-la-prediccion-automatica-de-embarazos-adolescentes/

Microsoft News Center LATAM (2017). Microsoft y el gobierno de Salta firman un acuerdo para aplicar la inteligencia artificial en la prevención de los problemas más urgentes. https://news.microsoft.com/ es-xl/microsoft-gobierno-salta-firman-acuerdo-aplicar-la-inteligencia-artificial-la-prevencion-los-problemas-masurgentes/

Ortiz Freuler, Juan e Iglesias, Carlos (2018). *Algoritmos e Inteligencia Artificial en Latinoamérica: Un Estudio de implementaciones por parte de Gobiernos en Argentina y Uruguay*. World Wide Web Foundation. https://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Spanish_Screen_AW.pdf

Página 12 (2018). La inteligencia artificial de Urtubey. https://www.pagina12.com.ar/107412-lainteligencia-artificial-de-urtube

Perfil (2018). Albino dijo que el preservativo no protege porque "el virus del SIDA atraviesa la porcelana" https://www.perfil.

com/noticias/politica/albino-dijo-que-el-preservativo-no-protege-del-vih-porque-atraviesala-porcelana.phtml

Wikipedia, la enciclopedia libre (2023). https://es.wikipedia.org/wiki/Alan_Turing

Wikipedia, la enciclopedia libre (2023). https://es.wikipedia.org/wiki/HAL_9000

Creatividad abolicionista

Cómo la propiedad intelectual puede piratear el poder digital

Julia Choucair Vizoso y Chris R. Byrnes

Traducción al español por Nuria del Viso Pabón
Ilustración de Zoran Svilar

La empresa inmobiliaria más influyente de la historia no posee muchos inmuebles. Ha hecho que la vivienda sea menos asequible (Barron, Kung y Proserpio, 2020), ha creado crisis inmobiliarias en destinos turísticos populares, ha vaciado comunidades (Bernardi, 2018) y ha alcanzado una valoración de 113 mil millones de dólares (Griffith, 2020), todo ello sin poseer la propiedad física.

Sin embargo, Airbnb posee una gran cantidad de propiedades. Lo que la empresa carece de propiedad física lo compensa con propiedad intelectual (PI), los códigos jurídicos y económicos que rigen la creatividad, la información, la marca y la reputación en la economía mundial. Si usted es uno de los 500 millones de usuarios de Airbnb, cuando busca anuncios, hace una reserva, paga o se pone en contacto con el servicio de atención al cliente, está interactuando con diversos tipos de propiedad intelectual, como código de *software* protegido por derechos de autor, algoritmos protegidos por secretos comerciales y cientos de patentes de la empresa. A medida que Airbnb se expande a nuevos mercados, explica a sus inversores que el crecimiento a largo plazo de la empresa procederá de la red de propiedad intelectual que rodea al mercado de alquiler y alojamiento (Airbnb, 2021).

El imperio intangible de Airbnb dista mucho de ser único. La propiedad física, las materias primas, los recursos, los productos –las cosas que se pueden tocar– tienen un valor de mercado cada vez más marginal. El cambio ha sido tectónico: hace cincuenta años, el 80 % del valor de las mayores empresas del mundo estaba en activos físicos; ahora, el 90 % está en intangibles (Tang, 2022). El valor de los intangibles se ha multiplicado por diez en los últimos siete años, hasta alcanzar los 65 billones de dólares, es decir, más del 75 % de la economía mundial (WIPO, 2017 y 2021). Ninguna cadena de suministro, ningún acuerdo

comercial existiría sin que lo atravesara la propiedad intelectual. El poder digital no sería posible sin ella.

No podemos entender el capitalismo digital actual y sus muchas desigualdades sin comprender cómo ha transformado cada acto de la imaginación humana, cada punto de datos, pasado y presente, en una mercancía potencial. Una nueva generación de empresas tecnológicas *disruptivas* ha encontrado formas de utilizar la propiedad intelectual como una parte importante de su arsenal para controlar y explotar el trabajo y los datos de los trabajadores digitales y los consumidores por igual en la llamada economía colaborativa.

Sin embargo, quizá ninguna otra clase de activos esté tan madura para la revolución. A pesar de todo su poder en la economía, la propiedad intelectual también es especialmente vulnerable. Podemos ocupar las vulnerabilidades del sistema actual, desvincular la creatividad y los datos de la exclusión y la posesión personal, y forjarlos en su lugar como una práctica de construcción de comunidad radicalmente imaginativa, generativa y socialmente productiva.

Creatividad abolicionista

"La abolición es presencia, no ausencia. Se trata de construir instituciones que afirmen la vida".

Ruth Wilson Gilmore, geógrafa abolicionista

Hoy en día, se intercambian billones de dólares imaginarios por derechos a propiedades imaginarias, pero carecemos de la imaginación necesaria para transformar la economía en algo que pueda ayudar a que florezca la vida. Ahora, más que nunca, la creatividad es la vía para salir de los callejones sin salida a los que nos enfrentamos. Pero para que prospere, primero debemos abolir los códigos económicos y jurídicos que la encadenan.

La creatividad entra en la economía como propiedad intelectual, el régimen jurídico surgido de la Europa del siglo XVII, que formalizó la expresión creativa y la invención en derechos exclusivos individuales. La propiedad intelectual, término que engloba los derechos de autor, las patentes, las marcas y los secretos comerciales, está en todas partes. La tecnología del *smartphone* que puede estar utilizando para leer esto podría tener tantas como 250 mil patentes.[1]

El informe del que es capítulo este ensayo lleva un aviso de *copyright* –en forma de licencia Creative Commons– en la primera página. Incluso el garabato que haya hecho en una servilleta está automáticamente protegido por derechos de autor, lo quiera o no (e independientemente de su valor estético).

A la ley de derechos de autor no le importa si lo que hemos creado es bueno desde el punto de vista artístico. Para que un trabajo esté protegido por los derechos de autor, debe ser *original* y *creativo*, pero el umbral es muy bajo: un poco más creativo y original que organizar una guía telefónica por orden alfabético.

La propiedad intelectual, basada en los conceptos de trabajo e individualismo desarrollados por los filósofos de la Ilustración, se impuso en todo el mundo a través de los proyectos coloniales europeos y los acuerdos comerciales. A día de hoy, el sistema de propiedad intelectual sigue siendo rígidamente eurocéntrico, sin medios acordados para reconocer y respetar epistemologías o concepciones del individuo no europeas.

El régimen está reforzado por instituciones poderosas y legalmente vengativas cuya jurisdicción se extiende a todos los miembros de la Organización Mundial del Comercio (OMC). Bajo la bandera de la vigilancia de la *infracción de la propiedad intelectual*, las leyes de propiedad intelectual pueden bloquear cualquier bien en la frontera e impedir que incluso las innovaciones más esenciales se pongan a disposición del público. Y su poder no parece sino aumentar. Bajo la

[1] Ver Patent Progress. Too Many Patents. https://www.patentprogress.org/systemic-problems/too-many-patents/

presión de un amplio abanico de grupos de presión empresariales, los derechos exclusivos que en su día se extinguieron se han convertido en perpetuos y expansivos, erosionando el dominio público.

Naturalmente, un sistema así inspira resistencia. Las voces críticas se oponen a la visión colonial capitalista de los derechos de propiedad que sustenta el sistema. Los piratas y los defensores de la cultura libre insisten en que "la información quiere ser libre", estableciendo plataformas alternativas para compartir la cultura. Incluso los defensores liberales de los regímenes de propiedad intelectual admiten a regañadientes que, aunque la configuración inicial era acertada –promovería "el ideal de progreso, un mercado transparente, un acceso fácil y barato a la información, una producción cultural descentralizada e iconoclasta, una política de innovación autocorrectiva"–, el sistema se ha visto corrompido por la influencia empresarial, lo que ha socavado la cultura de compartir y remezclar (Boyle, 2008).

¿Qué hay que hacer? ¿eliminar por completo la propiedad intelectual? ¿reformarla mediante políticas públicas? ¿desarrollar tecnologías legales que permitan a los creadores excluirse? ¿promover campañas contra la piratería y las infracciones en línea? Aunque estos debates son importantes (algunos más que otros), frenan peligrosamente nuestra imaginación. Al limitar nuestra mirada al mundo interior de lo que constituye la propiedad intelectual –si las obras creativas deben protegerse y cómo, qué debe considerarse propiedad intelectual–, no estamos haciendo el trabajo radical: situar la propiedad intelectual en la economía política más amplia, cuestionar qué papel desempeña en las estructuras más amplias de explotación y opresión.

Cuando nos alejamos de las guerras culturales que han dominado los debates sobre la propiedad intelectual en sí, nos vemos obligados a enfrentarnos más seriamente a la materialidad de la creatividad, a cómo atraviesa todas las cadenas de suministro mundiales y todos los acuerdos comerciales internacionales que se puedan imaginar, a cómo hace posible y omnipresente el poder digital. El capitalismo reconoce este poder y se mueve para estrechar su control. Vaqueros capitalistas que acaparan titulares como Jeff Bezos, Nathan Myhrvold y Martin

Shkreli están innovando en torno a las incongruencias de esta poderosa clase de activos.[2] Los anticapitalistas han estado dormidos al volante.

La falta de atención no es sorprendente. La mención de la propiedad intelectual puede hacer que hasta los ojos más brillantes se nublen. Es una de las muchas cuestiones que deliberadamente se hacen parecer oscuras, demasiado técnicas, legalistas e irrelevantes para las crisis a las que nos enfrentamos. No hace falta ser licenciado en Derecho para entender las condiciones en las que la creatividad entra en la economía. Liberar a la propiedad intelectual de su andamiaje legalista y despertar a su poder revela que se trata de un régimen singularmente vulnerable.

He aquí la laguna fundamental: la propiedad y el control de la propiedad intelectual siempre pertenecen, en primera instancia, a los artistas, inventores, académicos y creadores que la han creado. En la actualidad, este poder permanece latente. La mayoría de los productores de propiedad intelectual ceden sin concesiones su PI a las empresas (tanto con ánimo de lucro como sin él) mediante contratos de trabajo, condiciones de contratación y licencias de PI que permiten a estas instituciones dar rienda suelta a la comercialización de la PI en cadenas de suministro explotadoras y opresivas. Otros simplemente ceden su poder utilizando licencias Creative Commons o de código abierto, pero tampoco hacen nada para impedir que las empresas comercialicen la propiedad intelectual de forma agresiva y opresiva.

¿Podríamos imaginar un camino diferente? ¿y si los creadores se apoderaran de sus derechos de propiedad intelectual, los ocuparan y dieran la vuelta a su lógica? ¿y si tomáramos la esencia de la PI –el derecho económico y legal a excluir a otros de un intangible– y optáramos por excluir únicamente la opresión y la explotación? ¿podemos aprovechar nuestros derechos legales como creadores para poner

[2] Ver Blumberg, Alex y Sydell, Laura (22 de julio de 2011). When Patents Attack. *This American Life* [Podcast]. https://www.npr.org/sections/money/2011/07/26/138576167/when-patents-attack; Owles, Eric (22 de junio de 2017). The making of Martin Shkreli as "pharma bro". *The New York Times*. https://www.nytimes.com/2017/06/22/business/dealbook/martin-shkreli-pharma-bro-drug-prices.html

trabas al capitalismo? ¿y si los creadores no se limitaran a protestar contra los regímenes que encarcelan la imaginación, sino que crearan, aquí y ahora, sistemas, estructuras e instituciones de base para sustituirlos?

Con estos fines, no nos preocupa principalmente la cuestión abstracta de si debe existir la propiedad intelectual. Para nosotros, la creatividad abolicionista no consiste en eliminar los derechos de los creadores o las protecciones otorgadas a las creaciones; consiste en garantizar que la creatividad entre en la economía como una herramienta contra la opresión. En palabras de la geógrafa abolicionista Ruth Wilson Gilmore, "la abolición tiene que ver con la presencia, no con la ausencia" (Gilmore, 2020). Pedimos a los creadores que aparezcan y estén presentes en los derechos que se nos han concedido, que los ocupen y los pongan juntos al servicio de los mundos que queremos crear. Que utilicemos nuestra creatividad para construir instituciones que afirmen la vida.

Inspirándonos en las preguntas formuladas por los abolicionistas Mariame Kaba y Dean Spade en su reflexión sobre las "reformas no reformistas" (término acuñado originalmente por el economista y filósofo francés André Gorz en la década del sesenta), pedimos a los creadores que se pregunten: ¿cuál es la finalidad de la creatividad, de la información, del conocimiento? ¿supone un alivio material para los oprimidos y explotados dentro de las cadenas de suministro en las que se comercializa la creatividad? ¿crea poder, movilizando la lucha continua entre los afectados por las obras creativas? ¿deja fuera a los grupos marginados? ¿legitima el sistema? (Duda, 2017).

La mirada abolicionista ve la creatividad, tal y como se interpreta en nuestra economía, como un hilo que teje a través de sistemas de opresión entrelazados. Nos invita a tirar de ese hilo.

El régimen mundial de propiedad intelectual también es vulnerable por otra razón. Precisamente porque está torpemente modelado a partir de las leyes de la Edad Moderna temprana relacionadas con la propiedad física, la PI está llena de contradicciones y absurdos, que ofrecen oportunidades sugerentes para la experimentación

transgresora, la imaginación radical y el juego subversivo. He aquí algunas de ellas.

Tramas del futuro abolicionista

Trama nº 1. La protesta como actuación protegida por derechos de autor

La protesta está cada vez más criminalizada en todas las democracias. Durante manifestaciones pacíficas contra la inacción climática, la injusticia racial, la brutalidad policial o la guerra, los servicios de seguridad detienen y reprimen violentamente a manifestantes, periodistas y observadores de derechos humanos. Los mandos policiales envían órdenes de "recuperar las calles", transformando a las personas que ejercen un derecho democrático fundamental, el derecho a protestar, en delincuentes.[3] Cada vez más países están introduciendo leyes para responsabilizar penal y civilmente a los manifestantes por los daños a la propiedad que se produzcan durante las protestas.

La digitalización se ha convertido en un componente crucial de la mayor vigilancia y capacidad coercitiva de los estados, que la despliegan con escasa regulación o transparencia. Periodistas, defensores de los derechos civiles y manifestantes han documentado el uso que hace el gobierno de la vigilancia, el control de las redes sociales y otras herramientas digitales, advirtiendo de que pueden pasar años desde la celebración de una protesta hasta que se conozcan todas las formas en que las fuerzas de seguridad vigilaron a los organizadores. Los gobiernos también se coordinan con fuerzas de seguridad privadas expertas en tecnología que empezaron como contratistas en la *guerra contra el terrorismo*. El "solapamiento de los intereses del gobierno y la industria que utilizan la vigilancia, el mantenimiento del orden y el encarcelamiento como soluciones a problemas económicos, sociales

[3] Ver International Network of Civil Liberties Organizations (2013). "Take back the streets": Repression and criminalization of protest around the world. https://www.aclu.org/sites/default/files/field_document/global_ protest_suppression_report_inclo.pdf

y políticos" es lo que los abolicionistas denominan el complejo industrial penitenciario.[4]

Durante las protestas contra el oleoducto Dakota Access en Standing Rock, por ejemplo, documentos filtrados revelaron que fuerzas militares estatales y federales trabajaban junto a un contratista militar privado, TigerSwan, contratado por los propietarios del oleoducto, Energy Transfer Partners (Brown, 2020). En colaboración con la policía de al menos cinco estados para atacar al movimiento indígena Water Protector, TigerSwan utilizaba medidas antiterroristas de tipo militar y vigilancia digital para vigilar los movimientos de los manifestantes, incluida la transmisión de vídeo en directo desde un helicóptero de seguridad privado de Dakota Access.

Aquí es donde entra en juego la propiedad intelectual. ¿Qué pasaría si protegiéramos legalmente la creatividad inherente a las protestas como arte escénico susceptible de derechos de autor? Las protestas incorporan habitualmente innovaciones performativas a su repertorio, desde Standing Rock hasta México, pasando por Irak y el Reino Unido (Cadena-Roa y Puga, 2021; Reuters, 2019; Brown, 2015).[5] Sabemos que para las comunidades en resistencia, "los rituales, danzas, protocolos y canciones que caracterizan estas luchas no son meras efemérides culturales del activismo; son una parte íntima y constitutiva de la creación del mundo indígena, un medio para coordinar y alinear el imaginario colectivo con el fin de facilitar y enriquecer la cooperación de los implicados" (Haiven, 2017). Los académicos llevan mucho tiempo reconociendo la performatividad de la protesta, estudiando el uso de la visualización y el espacio o argumentando que "la coreografía, el movimiento y el gesto no son periféricos, sino centrales en la política de la protesta". ¿Qué pasaría si los manifestantes reconocieran que

[4] Ver Critical Resistance. What is the PIC? What is Abolition? https://criticalresistance.org/mission-vision/not-so- common-language/

[5] Ver también Mural Arts Philadelphia. *Standing Rock: Decolonizing Creative Practice in the Environmental Justice Movement*. [video en línea]. https://www.youtube.com/watch?v=z5A2Xf5B7Lc

estas características clave de la protesta también tienen derechos legales que pueden ayudarles a desafiar al complejo carcelario-industrial?

Imaginemos que los manifestantes llevaran el © "Todos los derechos reservados" en el cuerpo o se adornaran con códigos de barras que enlazaran con las condiciones de sus derechos de autor, especificando que las imágenes y el audio no pueden utilizarse para fines comerciales, incluida la vigilancia contratada de forma privada. Imaginemos que los manifestantes exigieran ante los tribunales saber cómo utilizan las fuerzas de seguridad privadas cualquier grabación de su arte, visual o sonora. Imaginemos que la proposición de prueba (el procedimiento previo al juicio en el que cada parte puede obtener pruebas de la otra mediante la solicitud de documentos) revelara los intereses comerciales secretos entre los departamentos de policía y las empresas de seguridad privada, o entre una empresa mercenaria privada y su empleador, una compañía petrolera. Imagina que estas empresas tuvieran que indemnizar a los manifestantes por violar los derechos de autor, o que los tribunales desestimaran las pruebas porque las empresas las habían obtenido ilegalmente infringiendo los derechos de autor. La legislación sobre derechos de autor no va a sacar a los manifestantes de la cárcel por cargos penales, pero puede ayudar a garantizar que el complejo industrial penitenciario no pueda lucrarse con la vigilancia policial.

¿Cómo querrían los creadores de una actuación protegida por derechos de autor de Extinction Rebellion, Black Lives Matter, BP or not BP, #NoDAPL y otros innumerables e intrépidos activistas condicionar el uso de su actuación? ¿qué tipo de exclusiones jurídicamente exigibles favorecerían los objetivos de su acción directa o respuesta comunitaria? ¿deberían los manifestantes permitir que los departamentos de policía (y las empresas de seguridad privada con las que trabajan cada vez más) utilicen grabaciones de vídeo y sonido de una actuación guionizada (es decir, una protesta) o de arte visual como el graffiti –y cualquier otro material sujeto a derechos de autor– sin ninguna condición? ¿qué indemnización debería pagar quien incaute o destruya una instalación artística?

Habitamos sistemas que ofrecen más protección jurídica a la indignación ante la injusticia que a la reivindicación de la justicia como derecho; sistemas que valoran más la inviolabilidad de la propiedad que la inviolabilidad de las vidas de las personas e indígenas, más que la protección de la biodiversidad. No existe un régimen internacional de derechos humanos que pueda aplicarse de forma fiable, pero sí un poderoso régimen jurídico internacional asociado a la propiedad intelectual. Podemos reconvertir radicalmente este poder. Podemos liberar los códigos y la tecnología jurídica de la propiedad intelectual de su uso previsto.

Las posibilidades son intrigantes. ¿Podríamos ser más capaces de ocupar la propiedad física ocupando la propiedad intelectual, remodelando los absurdos poderes otorgados a la propiedad intangible para fomentar nuestra capacidad de controlar el espacio físico? ¿puede la protección de los derechos de autor complicar la forma en que el poder digital oprime cada vez más la protesta o los actos de preservación, ya se trate de cuestiones medioambientales o de una vida digna?

Cualquiera puede participar. Todo manifestante es un artista de la *performance*. Para aquellos que ya se identifican como artistas socialmente comprometidos o artivistas, esta es una oportunidad para repensar la agencia política de su arte. ¿Puede una obra de arte tener agencia política directa, no a través de debates sobre la rectitud de su estética o contenido político, sino a través de artistas que ocupan el andamiaje legal y económico que la rodea?

Trama nº 2. Ocupar los contratos de trabajo con cláusulas morales de PI

Los contratos de trabajo son el lugar en el que, como productores de PI, más a menudo cedemos nuestros derechos. Cedemos a las empresas lo que legalmente nos pertenece a través de la cláusula de cesión de PI: una cláusula contractual que otorga a nuestros empleadores plena propiedad y control para utilizar y comercializar nuestra PI. Dado el enorme valor de la propiedad intelectual para los resultados de una empresa, no es de extrañar que las empresas hayan intentado que sus

reivindicaciones sobre la creatividad de los empleados sean lo más amplias posible.

Las leyes que rigen las cláusulas de cesión de propiedad intelectual a los empleados varían según la jurisdicción, pero las cláusulas más comunes exigen que los empleados renuncien a todos los derechos morales: derechos legales que facultan a los creadores a oponerse a usos de su trabajo que perjudiquen su honor o reputación. Otras cláusulas comunes conceden a los empleadores la propiedad de cualquier idea registrada en cualquier pieza de propiedad corporativa, incluida la idea de un empleado para un proyecto personal si por casualidad la grabó en un ordenador portátil del trabajo.

¿Qué pasaría si ocupáramos nuestras cláusulas de cesión de propiedad intelectual? ¿qué pasaría si nos organizáramos colectivamente como productores de PI y pusiéramos condiciones a los derechos de nuestros empleadores sobre nuestra PI? Una tecnología jurídica existente que podemos utilizar es la cláusula de moralidad: una cláusula contractual que da derecho a rescindir un contrato, o a tomar otras medidas correctivas, si la parte infractora tiene un comportamiento inmoral. ¿Qué podrían estipular las cláusulas morales de la PI abolicionista cocreada?

¿Qué pasaría si nuestros empleadores ya no pudieran utilizar nuestra PI en cadenas de suministro con trabajos forzados y devastación ecológica, o al servicio de ejércitos, vigilancia y policía?

La propiedad intelectual tiene un enorme poder para interrumpir toda una cadena de suministro. Si los productores de PI de una parte de la cadena de suministro utilizaran cláusulas morales, podrían desencadenar un litigio de PI siempre que estas cláusulas morales se infringieran en cualquier punto de la cadena de suministro en la que se utilizara la PI.

He aquí un ejemplo de las grandes empresas tecnológicas, cuyas cadenas de suministro tienen un apetito insaciable de cobalto. La minería del cobalto es famosa por sus abusos de los derechos humanos, la corrupción, la destrucción del medio ambiente y el trabajo infantil (Kelly, 2019). Una cláusula moral de PI utilizada por los productores de

PI a lo largo de estas cadenas de suministro –por ejemplo, por la Coalición de Trabajadores de la Tecnología– podría utilizarse para aplicar las propuestas realizadas por los activistas de derechos humanos, según las cuales "cualquier empresa que se abastezca de cobalto procedente de la RDC debe establecer un sistema independiente de terceros para verificar que todas las cadenas de suministro de minerales están limpias de explotación, crueldad, esclavitud y trabajo infantil. Deben invertir todo lo necesario para garantizar una remuneración decente, unas condiciones de trabajo seguras y dignas, la atención sanitaria, la educación y el bienestar general de las personas de cuya mano de obra barata dependen" (Ochab, 2020). Si estas condiciones se incluyeran en una cláusula moral de PI, capaz de paralizar las cadenas de suministro dependientes del cobalto al desencadenar un litigio de PI en caso de infracción, todo el poder de mercado de la PI podría utilizarse como zanahoria y garrote para aplicar estas propuestas.

Los académicos, periodistas, artistas y músicos también pueden esgrimir poderosas cláusulas morales de PI. Los editores dependen del papel, la tinta y el pegamento, o de los ordenadores, el *software*, Google y Amazon para difundir sus obras protegidas por derechos de autor. Sin embargo, la industria de la *pulpa y el papel* sigue beneficiándose de la deforestación de la selva amazónica, los fabricantes de tinta violan los derechos laborales y vierten residuos peligrosos, y las encuadernaciones de libros no son reciclables (Vermeer, 2020; Ro, 2021).[6] Por su parte, la edición digital alimenta cadenas de suministro que vierten habitualmente residuos electrónicos en todo el Sur Global.[7] Estas condiciones pueden coexistir con las condiciones de concesión de licencias de acceso abierto que permiten a cualquier persona

[6] Ver también China Labor Watch (13 de diciembre 2021). Abuse in the printing supply chain: An investigation into two cartridge manufacturers. *China Labor Watch.* https://chinalaborwatch.org/zh/abuse-in-the-printing-supply-chain-an- investigation-into-two-cartridge-manufacturers/

[7] Ver Good Electronics (25 de marzo de 2021). Global South: The dumping ground for the world's electronics waste. *Good Electronics*. https://goodelectronics.org/topic/health-safety/

acceder libremente a contenidos protegidos por derechos de autor, al tiempo que prohíben a los editores ofrecer contenidos de acceso abierto a través de cadenas de suministro poco éticas.

Mediante cláusulas morales de propiedad intelectual, podemos poner en práctica ideas sobre abolición, sostenibilidad o derechos humanos a través de las cadenas de suministro en las que se comercializan estas ideas. También podemos aprovechar el poder de la PI para profundizar en la solidaridad de los trabajadores a través de las cadenas de suministro. En este proceso, podemos experimentar con la PI no como un derecho individual exclusivo, sino como una herramienta colectiva. ¿Podemos imaginar sindicatos de PI organizados en torno a una moral colectiva de PI?

Por qué el acceso abierto no es abolicionista

La creatividad abolicionista puede estar reñida con los movimientos contraculturales de mayor éxito del mundo de la propiedad intelectual, como el movimiento del software libre, el movimiento del código abierto y el movimiento Creative Commons. Aunque heterogéneos y enzarzados en animados debates entre sí, estos movimientos comparten una preocupación común: ¿cómo resuelve la sociedad el desajuste entre lo que teóricamente permite la tecnología digital –la oportunidad de acceder, compartir y colaborar en la creatividad a una escala sin precedentes y con un coste marginal cercano a cero– y lo que restringe la ley de derechos de autor?

Las respuestas de los movimientos de acceso abierto han logrado construir una comunidad, una cultura y una práctica alternativas en relación con los derechos de autor. Mediante mensajes creativos y recursos educativos accesibles, estos movimientos han llevado los derechos de autor a la esfera pública y los han liberado de su arcano andamiaje. Sus licencias estándar, fáciles de usar, permiten a los creadores salirse del marco por defecto de "todos los derechos reservados" y ejercer una mayor autonomía sin necesidad de convertirse en

expertos en leyes de derechos de autor. Estos movimientos también han facilitado el acceso a la información a quienes no pueden permitirse muros de pago y han permitido la acción colectiva para crear *software* más seguro y respetuoso con la privacidad.

La creatividad abolicionista se basa en las aportaciones de los movimientos contemporáneos de acceso abierto, pero cambia fundamentalmente el quid del problema. Los movimientos de acceso abierto se centran en cómo compartir ideas y cultura más libremente; cómo facilitar la libertad de expresión y el libre acceso al tiempo que se mantiene la innovación. Estas preocupaciones son producto de la ubicación y el momento histórico del que surgieron. En la década del noventa, los informáticos y estudiosos del ciberderecho de Europa y Estados Unidos que participaron en el auge del *software* e internet como herramientas de masas (la llamada Era de la Información) trataron de resolver un reto concreto: cómo hacer realidad el potencial y la esperanza de internet mientras la legislación sobre derechos de autor se vuelve cada vez más restrictiva y punitiva.

En lugar de ello, comenzamos nuestro análisis examinando el sistema global más amplio en el que operan el conocimiento y la información: un sistema colono-colonial que extrae riqueza, conocimiento y cultura de las comunidades económicamente marginadas y redistribuye de forma desigual sus frutos económicos entre los más ricos y poderosos. Este enfoque está en consonancia con las críticas que activistas y académicos críticos llevan mucho tiempo haciendo a los movimientos de acceso abierto (Vats y Keller, 2018): que el enfoque central en los valores de la libertad ignora las preocupaciones sobre la igualdad; que una noción romántica del *dominio p*úblico como un paisaje neutral en el que todo el mundo puede cosechar sus riquezas ignora su papel real en la explotación del trabajo y los cuerpos de las personas de color, las mujeres, las personas del Sur global y los empobrecidos (Chander y Sunder, 2004). Ahora sabemos que el *dominio público* de los conocimientos indígenas sobre la flora y la fauna locales, las medicinas tradicionales, el folclore o las expresiones culturales tradicionales ha permitido a las grandes farmacéuticas apropiarse de los

conocimientos indígenas, transformarlos en propiedad intelectual y convertirse en propietarias exclusivas de esos conocimientos: un fenómeno conocido como biopiratería.

La creatividad abolicionista tampoco está de acuerdo con una creencia ideológica que recorre algunos segmentos destacados de los movimientos de acceso abierto, a saber, que el sistema funcionó bien en su día, pero que "desgraciadamente, nuestros regímenes de PI se han desviado mucho de sus propósitos originales" (Electronic Frontier Foundationd). Para los colonizados, para los pueblos indígenas cuyo conocimiento colectivo ha sido saqueado, para las comunidades obligadas a aceptar acuerdos comerciales opresivos (por ejemplo, los ADPIC), para el creciente número de esclavos modernos que trabajan en cadenas de suministro globales impulsadas por intangibles, es difícil ver cómo el sistema de PI ha funcionado alguna vez para ellos, o qué han conseguido décadas de intentos reformistas dentro de la legislación de PI en Estados Unidos.[8]

Para los abolicionistas, el sistema no está roto ni necesita reformas, ajustes y retoques. Funciona tal y como fue diseñado, como una estructura jurídica y económica colonial de colonos. Y se nos está acabando el tiempo y el pensamiento mágico esperando que las políticas públicas se vuelvan favorables de alguna manera en una oligarquía dominada por las corporaciones (Gilens y Page, 2014).

Los movimientos de acceso abierto también deben enfrentarse a un hecho incómodo: las grandes empresas tecnológicas están de su lado. La creencia generalizada de que las grandes empresas siempre prefieren regímenes de propiedad intelectual más estrictos para bloquear a los nuevos competidores, o que la aplicación celosa de la ley de propiedad intelectual favorece a los poderosos, no se ve confirmada por la historia. Con la excepción de la industria farmacéutica, los monopolios de las industrias intensivas en tecnología se han resistido a lo

[8] Ver ILO/OIT (12 de septiembre de 2022). 50 million people worldwide in modern slavery. https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_855019/lang–en/index.htm

largo de la historia a una fuerte protección de las patentes: la industria ferroviaria en el siglo XIX, IBM en la industria informática de los años sesenta y setenta del siglo XX, las grandes tecnológicas en la actualidad (Barnett, 2021). Google, Facebook (Meta) y Twitter están tratando de aplicar selectivamente la observancia de la PI, gastando millones de dólares en grupos de presión para garantizar la menor fricción posible con la PI dentro de los mercados en los que ya tienen un poder de mercado dominante, para tener un control sin restricciones sobre los datos y el conocimiento, para seguir obteniendo "beneficios publicitarios colosales de los contenidos producidos gratuitamente por los usuarios" (Riekeles, 2022) y para evitar la temida disputa por la PI (Michel, 2022; Schiffner, 2022; Pegoraro, 2015) .

Si los actores más poderosos son los verdaderos ganadores en un mundo de acceso abierto, ¿no deberíamos replantearnos la afirmación de que *la información quiere ser libre*? Si el libre acceso significa seguir ignorando las súplicas de las comunidades indígenas para detener la biopiratería, la expropiación cultural y el *dominio público* de los colonizados, ¿por qué seguimos sosteniéndolo como un valor absoluto?

A diferencia de los movimientos de acceso abierto, la creatividad abolicionista reconoce que la economía global en la que liberamos nuestra creatividad no es un campo de juego neutral e igualitario. Renunciar o limitar los derechos existentes a la creatividad en nuestro sistema actual no hace nada para interferir en la estructura de opresión. Simplemente cede la capacidad de acción a actores más poderosos, una capacidad que debería cederse hacia abajo, no hacia arriba. En lugar de renunciar a nuestros derechos en nombre de una especie de libertarismo para la Era de la Información, deberíamos abrir los ojos a las formas materiales en que nuestra creatividad entra en la economía y reifica las estructuras de poder digital (y de otros tipos).

Como ilustran nuestras tramas para un futuro abolicionista, existen interesantes experimentos y ejercicios para reconocer y reutilizar el poder de lo que se clasifica como *propiedad intelectual*. Al apoderarnos de los medios de producción imaginativa, podemos transformar

la creatividad en una herramienta de liberación colectiva que perturbe y anule los propios regímenes de poder digital que la encierran y explotan. Al mismo tiempo, lejos de cosificar el propio sistema de propiedad intelectual, la creatividad abolicionista pone de relieve sus contradicciones, sacude su equilibrio y crea crisis internas. Si existe un futuro para la propiedad intelectual, lo descubriremos, colectivamente, en nuestros actos de resistencia e imaginación.

Bibliografía

Airbnb, Inc. (11 de febrero de 2021). Annual Report for the fiscal year ended Dec. 31, 2020. 10-K, United States Securities y Exchange Commission. https://www.sec.gov/Archives/edgar/data/1559720/000155972021000010/ airbnb-10k.htm

Barnett, Jonathan M. (2021). *Innovators, Firms, and Markets: The organizational logic of intellectual property*. Nueva York: Oxford University Press. https://academic.oup.com/book/33492

Barron, Kyle, Kung, Edward, y Proserpio, Davide (2020). The effect of home-sharing on house prices and rents: Evidence from Airbnb. *Marketing Science* 40(1), 23–47.

Bernardi, Monica (2 de octubre de 2018). The impact of AirBnB on our cities: Gentrification and 'disneyfication' 2.0. *The Urban Media Lab*. https://labgov.city/theurbanmedialab/the-impact-of-airbnb-on-our-cities-gentrification-and- disneyfication-2-0/

Blumberg, Alex y Sydell, Laura (22 de julio de 2011). When Patents Attack. *This American Life* [Podcast]. https://www.npr.org/sections/money/2011/07/26/138576167/when-patents-attack

Boyle, James (2008). *The Public Domain: Enclosing the commons of the mind*. New Haven & London: Yale University Press. https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=5385&context=faculty_scholarship

Brown, Alleen (15 de noviembre de 2020). In the mercenaries' own words: Documents detail TigerSwan infiltration of Standing Rock. *The Intercept*. https://theintercept.com/2020/11/15/standing-rock-tigerswan-infiltrator- documents/

Brown, Mark (3 de septiembre de 2015). Activists plan oil protest at British Museum. *The Guardian.* https://www.theguardian.com/culture/2015/sep/03/art-not-oil-plan-protest-british-museum

Cadena-Roa, Jorge y Puga, Cristina (2021). Protest and Performativity. En Rai, Shirin et al. (eds.), *The Oxford Handbook of Politics and Performance (*pp. 101–116). Nueva York: Oxford University Press.

Chander, Anupam y Sunder, Madhavi (2004). The romance of the public domain. *California Law Review*, 92, 1331. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=562301

China Labor Watch (13 de diciembre 2021). Abuse in the printing supply chain: An investigation into two cartridge manufacturers. *China Labor Watch.* https://chinalaborwatch.org/zh/abuse-in-the-printing-supply-chain-an- investigation-into-two-cartridge-manufacturers/

Critical Resistance. What is the PIC? What is Abolition? https://criticalresistance.org/mission-vision/not-so- common-language/

Duda, John (9 de noviembre de 2017). Towards the horizon of abolition: A conversation with Mariame Kaba. *The Next System Project.* https://thenextsystem.org/learn/stories/towards-horizon-abolition-conversation-mariame-kaba

Electronic Frontier Foundation. Creativity and Innovation. https://www.eff.org/issues/innovation

Gilens, Martin y Page, Benjamin (18 de septiembre de 2014). Testing theories of American politics: Elites, interest groups, and average citizens. *Perspectives on Politics*, 12(3), 564–581. https://doi.org/10.1017/S1537592714001595

Gilmore, Ruth Wilson (10 de junio de 2020). What are we talking about when we talk about "a police-free future"? *MDP150*. https://www.mpd150.com/what-are-we-talking-about-when-we-talk-about-a-police-free-future/

Griffith, Erin (10 de diciembre 2020). Airbnb tops $100 billion on first day of trading. *The New York Times.* https://www.nytimes.com/2020/12/10/technology/airbnb-tops-100-billion-on-first-day-of-trading-reviving-talk-of- a-bubble.html

Haiven, Max (2017). Monsters of the Financialized Imagination: From Pokémon to Trump. En N. Buxton y D. Eade (eds.), *State of Power 2017*. Amsterdam: Transnational Institute. http://longreads.tni.org/state-of-power/age-of- monsters/

International Network of Civil Liberties Organizations (2013). "Take back the streets": Repression and criminalization of protest around the world. https://www.aclu.org/sites/default/files/field_document/global_ protest_suppression_report_inclo.pdf

ILO/OIT (12 de septiembre de 2022). 50 million people worldwide in modern slavery. https://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_855019/lang–en/index.htm

Kelly, Annie (16 de diciembre de 2019). Apple and Google named in US lawsuit over Congolese child cobalt mining deaths. *The Guardian.* https://www.theguardian.com/global-development/2019/

dec/16/apple-and-google-named-in-us- lawsuit-over-congolese-child-cobalt-mining-deaths

Michel, Paul R. (5 de Agosto de 2022). Big Tech has a patent violation problem. *Harvard Business Review*. https://hbr.org/2022/08/big-tech-has-a-patent-violation-problem

Mural Arts Philadelphia. *Standing Rock: Decolonizing Creative Practice in the Environmental Justice Movement*. [video en línea]. https://www.youtube.com/watch?v=z5A2Xf5B7Lc

Ochab, Ewelina U. (13 de enero de 2020). Are These tech companies complicit in human rights abuses of child cobalt miners in Congo? Centre de Ressources sur les Entreprises et les Droits de l'Homme. https://www.business-humanrights. org/fr/derni%C3%A8res-actualit%C3%A9s/are-these-tech-companies-complicit-in-human-rights-abuses-of-child- cobalt-miners-in-congo/

Owles, Eric (22 de junio de 2017). The making of Martin Shkreli as "pharma bro". *The New York Times*. https://www.nytimes.com/2017/06/22/business/dealbook/martin-shkreli-pharma-bro-drug-prices.html

Patent Progress. Too Many Patents. https://www.patentprogress.org/systemic-problems/too-many-patents/

Pegoraro, Rob (30 de junio de 2015). Why the tech industry hates patent trolls, and you should too. *Yahoo Tech.* https://finance.yahoo.com/news/why-the-tech-industry-hates-patent-trolls-and-you-121628489339.html

Reuters (4 de enero de 2019). Basra youth adopt new tactic for peaceful protest. https://uk.movies.yahoo.com/ basra-youth-adopt-tactic-peaceful-131430647.html

Riekeles, Georg (28 de junio de 2022). I saw first-hand how US tech giants seduced the EU—and undermined democracy. *The*

Guardian. https://www.theguardian.com/commentisfree/2022/jun/28/i-saw-first-hand-tech-giants-seduced- eu-google-meta

Ro, Christine (11 de febrero de 2021). Reducing the environmental toll of paper in the publishing industry. *Book Riot*. https://bookriot.com/environmental-toll-of-paper-in-publishing/

Schiffner, Christine (31 de mayo de 2022). As tech giants push for IP reform, plaintiffs firms see new momentum for litigation. *The National Law Journal*. https://www.law.com/nationallawjournal/2022/05/31/as-tech-giants-push-for-ip-reform- plaintiffs-firms-see-new-momentum-for-litigation/

Tang, Daren (5 de enero de 2022). WIPO: the IP Office of the future. *World Trademark Review*. https://www.worldtrademarkreview.com/report/special-reports/q4-2021/article/wipo-the-ip-office-of-the-future

Vats, Anjali y Keller, Deidre A. (2018). Critical Race IP. *Cardozo Arts & Entertainment Law Journal*, 36(3). https://scholarship.law.pitt.edu/fac_articles/512

Vermeer, Karen (21 de septiembre de 2020). Two sides of the same coin: How the pulp and paper industry is profiting from deforestation in the Amazon rainforest. *Environmental Paper Network.* https://environmentalpaper.org/2020/09/ two-sides-of-the-same-coin-how-the-pulp-and-paper-industry-is-profiting-from-deforestation-in-the-amazon- rainforest/

WIPO (2017). *World Intellectual Property Report 2017: Intangible capital in global value chains*. Geneva: World Intellectual Property Organization. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_944_2017.pdf

WIPO (2021). *IP for the Good of Everyone: Report of the Director General to the 2021 WIPO Assemblies*. Ginebra: World Intellectual Property Organization. https://www.wipo.int/dg-report/2021/en/

Atar a Goliat

Estrategias activistas para afrontar y aprovechar el poder digital

Anastasia Kavada, Tina Askanius,
Anne Kaun, Alice Mattoni y Julie Uldam

Traducción al español por Nuria del Viso Pabón
Ilustración de Zoran Svilar

En la última década, se ha producido un cambio radical en nuestra percepción de las plataformas de redes sociales y su papel en los movimientos sociales. En la oleada de protestas de 2011, desde la llamada Primavera Árabe hasta las movilizaciones Occupy, estas plataformas se presentaron a menudo como tecnologías de liberación. Diez años después, sin embargo, las redes sociales han pasado a ser vistas como espacios de vigilancia y represión capturados por el capitalismo y los gobiernos autoritarios. Las revelaciones de Edward Snowden en 2013 supusieron un punto de inflexión en este sentido, cuando quedó meridianamente claro el papel de las plataformas comerciales de redes sociales en la vigilancia de activistas. Desde entonces, muchas de las principales plataformas de medios sociales se han visto saturadas por la desinformación y el discurso ofensivo. A menudo se han apoderado de ellas fuerzas de extrema derecha que, bajo la bandera de la *libertad de expresión*, las han utilizado para atacar sin piedad a sus oponentes. En 2022, puede que hayamos asistido a otro punto de inflexión en esta historia, ya que fue un año en el que el poder de las redes sociales se enfrentó a intensos desafíos. La caótica adquisición de Twitter por Elon Musk, las recientes pérdidas de valor de Meta (antes Facebook) y los crecientes llamamientos a regular los contenidos en estas plataformas han ido acompañados de un modesto éxodo de las redes sociales, y de Twitter en particular, y la migración a plataformas alternativas como Mastodon, aunque este movimiento podría ser efímero.

Por supuesto, las principales plataformas de medios sociales siguen teniendo un poder significativo. Se han convertido en importantes canales de noticias e información, y los estudios realizados tanto en Estados Unidos (Shearer, 2021) como en el Reino Unido demuestran que plataformas como Facebook y YouTube son cada vez más espacios en los que los usuarios obtienen sus noticias. El modelo empresarial

de estas plataformas promueve el *capitalismo de la vigilancia*, la incesante recopilación y venta de datos sobre el comportamiento de los usuarios. Además, las empresas que están detrás de ellas se han hecho demasiado grandes para regularlas y controlarlas, ya que no han dejado de adquirir pequeñas empresas de nueva creación y de añadir diversas plataformas y aplicaciones a su lista de productos. Así pues, aunque las plataformas de medios sociales pueden haber ofrecido más oportunidades a los usuarios para expresar su voz, siguen reforzando la capacidad de los poderosos para moldear la opinión pública, ya que disponen de los recursos necesarios para pagar las tarifas que cobran algunas de estas plataformas, para llevar a cabo propaganda negra mediante bots y cuentas falsas, y para invertir en campañas publicitarias digitales. Estas plataformas también mantienen una relación ambivalente con los regímenes represivos de todo el mundo, a veces en connivencia con ellos –como demostraron ampliamente las revelaciones de Snowden– y a veces proporcionando un canal para la disidencia que no está controlado por el gobierno, aunque siga estando moldeado por complejos intereses geopolíticos.

En este contexto, los activistas progresistas deben desafiar y aprovechar el poder de las redes sociales en un esfuerzo por construir el mundo que les gustaría ver. Pero, ¿cómo pueden hacerlo los movimientos sociales? ¿Cuáles son los obstáculos a los que se enfrentan? En este ensayo, exploramos algunas estrategias que los activistas pueden utilizar centrándonos en el ejemplo del movimiento ecologista, y en particular en los grupos y organizaciones que se movilizan contra el colapso climático. Estos son diversos y heterogéneos, y van desde las organizaciones no gubernamentales (ONG) tradicionales y las organizaciones benéficas, hasta grupos más recientes como Extinction Rebellion (XR), que se centran en la acción directa, pasando por las movilizaciones asociadas a Greta Thunberg y el movimiento Fridays for Future.

Nuestro análisis se basa en el trabajo del estudioso de los movimientos sociales Dieter Rucht sobre las estrategias que adoptan los activistas frente a la tendencia de los principales medios de comunicación

(MSM) a tergiversar, trivializar y marginar las causas activistas. A principios de la primera década del siglo XXI, Rucht observó que, en respuesta, algunos activistas deciden dejar de lado la visibilidad y se abstienen de la prensa dominante. Otros optan por culpar abiertamente a la prensa generalista en un intento de hacerla responsable de su información sesgada sobre las protestas. Y otros optan por eludir a la prensa generalista creando alternativas para atender a sus electores. Por último, algunos grupos intentan obtener una buena cobertura de los principales medios de comunicación tratando de entender cómo funcionan y adaptando su comunicación a ellos. El marco de Rucht recibió el nombre de *cuádruple A*, ya que cada una de las cuatro estrategias empieza por la letra "A": Abstención, Ataque, Alternativas, Adaptación. Aunque las estrategias de Rucht se referían originalmente a una época de dominio de la prensa dominante, siguen resonando hoy en día, cuando las plataformas de medios sociales, así como la prensa, ocupan un lugar central en las estrategias de comunicación de los grupos activistas.

Dado que los principales medios de comunicación siguen un modelo capitalista, no es de extrañar que estas cuatro estrategias se hagan eco de la discusión de Erik Olin Wright (2019) sobre las cuatro lógicas que caracterizan las luchas anticapitalistas: aplastar, escapar, erosionar y domesticar el capitalismo.[1] Cuando los activistas se comprometen en la acción colectiva con la lógica de aplastar el capitalismo, están en sintonía con las estrategias de comunicación que giran en torno al ataque a las plataformas de medios sociales. Del mismo modo, cuando los activistas promueven una acción colectiva que permitiría a la gente escapar del capitalismo, son coherentes con la estrategia de abstención de las plataformas de medios sociales. Cuando los activistas desarrollan una acción colectiva que no rechaza totalmente el capitalismo, sino que busca domesticarlo, podemos ver un parecido con la estrategia de adaptación. Por último, las luchas anticapitalistas que

[1] Ver Data Detox Kit (26 de enero de 2021). How many trees does it take to power the internet? https://www.datadetoxkit.org/en/wellbeing/environment/

pretenden erosionar el capitalismo se vinculan a activistas que están creando alternativas a las plataformas de medios sociales, construyendo y comisariando espacios de contención que pueden gestionar directamente.

Teniendo en cuenta estas diferentes lógicas anticapitalistas y las cuatro estrategias que los grupos activistas pueden emplear para abordar la cuestión de la visibilidad, exploramos cómo el movimiento ecologista se ha comprometido con las plataformas de redes sociales.

Abstención (escapar del capitalismo)

Las estrategias de abstención consisten en rehuir por completo las redes sociales dominantes como forma de protesta y protección frente a sus modelos de negocio y mecanismos de vigilancia. Decidir no delegar la visibilidad de tu grupo a la lógica del beneficio de las plataformas de redes sociales es liberador. Quita a los activistas la presión constante de ser visibles y producir contenidos en estas plataformas. También emancipa a los grupos activistas de la opacidad que caracteriza a los algoritmos de las redes sociales, cajas negras cuyo funcionamiento es difícil, si no imposible, de entender. La estrategia de la abstención puede promover formas más sostenibles de mantener la membresía más allá de los grupos de Facebook o los hilos de Twitter, desarrollando los propios medios de comunicación del grupo. También puede proteger a los activistas de los ataques y la vigilancia en línea. Como ha demostrado el caso de Greta Thunberg, los activistas destacados pueden ser objeto de ataques mordaces en las redes sociales que van desde el *trolling* hasta las amenazas de muerte. Estar presente en las redes sociales también hace que los grupos de activistas sean vulnerables a la vigilancia de las autoridades. Esto es especialmente peligroso para los activistas que utilizan tácticas de desobediencia civil o que sobrepasan los límites de la legalidad (Bacchi, 2022). Por lo tanto, abstenerse de utilizar plataformas de medios sociales es crucial para mejorar la privacidad y la integridad de los datos de la organización interna.

Además de la abstención, algunos grupos activistas también han lanzado campañas en las que instan a la gente a desconectarse de dichas plataformas o a participar en prácticas de *desintoxicación* digital o de datos. Por ejemplo, Tactical Tech ofrece un kit de herramientas para concienciar sobre los rastros de datos que dejamos en internet y para desarrollar prácticas alternativas para lo que ellos llaman "una relación más segura con la tecnología" (Global Witness, 2022).

Desconectarse de las redes sociales también puede hacerse por razones medioambientales. Como señala Tactical Tech, las estrategias de desintoxicación digital pueden ayudar en la lucha contra el cambio climático, ya que las tecnologías digitales son actualmente responsables del 3,7 % de las emisiones mundiales de carbono, una cifra que puede aumentar hasta el 8 % en 2025. Por tanto, los grupos ecologistas pueden optar por abstenerse de las redes sociales para reducir sus residuos electrónicos y su huella de carbono.

Sin embargo, las prácticas de *desintoxicación digital* suelen estar relacionadas con políticas de estilo de vida individual más que con esfuerzos colectivos para lograr un cambio sistémico. Asistir a campamentos de desintoxicación digital o restringir nuestra huella de datos digitales mediante el uso de navegadores y configuraciones específicas implican prácticas y formas individuales de relacionarse con los medios sociales. Por lo tanto, pueden tener un impacto menor en la lucha contra el capitalismo y las grandes empresas tecnológicas que, por ejemplo, la promoción de un cambio estructural a través de la regulación.

Además, una abstención total de las plataformas digitales parece prácticamente imposible, especialmente para las causas políticas de carácter transnacional o las que pretenden movilizar a un gran número de simpatizantes. En un mundo en el que la visibilidad en las redes sociales se ha vuelto crucial para ampliar la comunidad de un movimiento, abstenerse de estas plataformas significa aislarse de una densa red de relaciones que ha sostenido numerosas protestas en todo el mundo durante la última década. El movimiento ecologista no es una excepción, como demuestra el amplio uso de las redes sociales por

parte de organizaciones como Greenpeace y Extinction Rebellion o movimientos como Fridays for Future. En cambio, y como señalamos en las secciones dedicadas a las estrategias de Adaptación y Alternativas, los grupos activistas optan a menudo por utilizar las principales plataformas para promover su causa ante un público más amplio, aunque se abstengan de utilizarlas para la organización interna.

Atacar (*Smashing capitalism*)

Los activistas y los movimientos sociales también pueden atacar a las plataformas de medios sociales y hacer campaña para que reformen sus prácticas empresariales o la normativa que regula su funcionamiento. Las *estrategias de ataque* incluyen acciones antimonopolio que cuestionan el tamaño y la concentración de las empresas de medios sociales, así como campañas de derechos digitales que atacan el uso indebido o la apropiación indebida de datos por parte de empresas y gobiernos nacionales.

También hay muchas campañas contra la desinformación en los medios sociales, un problema que también está afectando enormemente a las campañas sobre el cambio climático. Las grandes empresas contaminantes, como las petroleras, realizan elaboradas campañas de lavado verde en las redes sociales. Han proliferado las declaraciones falsas sobre el cambio climático, a menudo difundidas por cuentas falsas y campañas *astroturf.*

El negacionismo del cambio climático está aumentando en las plataformas de medios sociales, también como resultado del fortalecimiento de las cuentas de extrema derecha y la falta de una moderación eficaz. En febrero de 2022, Reuters informó de que Facebook "no marcó la mitad de las publicaciones que promueven la negación del cambio climático" (Milman, 2022). La investigación llevada a cabo por Global Witness ha descubierto que el algoritmo de Facebook no solo encierra a los usuarios escépticos del clima en cámaras de eco del negacionismo climático, sino que también los dirige "a información peor,

de modo que lo que comenzó en una página llena de narrativas de distracción y retraso, terminó en páginas que propugnan la negación absoluta del clima y la conspiración".[2] En Twitter, la situación parece haber empeorado tras la adquisición de Elon Musk, que provocó el despido de equipos de gestión de contenidos, el desmantelamiento de la rama de sostenibilidad de la plataforma y el regreso de usuarios vetados a la plataforma, algunos de los cuales tienen un historial significativo de negacionismo climático (Avaaz, 2020a). En consecuencia, el hashtag #ClimateScam ha escalado posiciones y "ahora es regularmente el primer resultado que aparece cuando se busca 'clima' en el sitio" (Avaaz, 2020b).

Las campañas contra la desinformación en las redes sociales han incluido la campaña #StopHateForProfit en 2020, en la que varios grupos y organizaciones de la sociedad civil pidieron a los anunciantes que boicotearan Facebook por este motivo. La campaña fue iniciada por una coalición de grupos activistas, entre ellos la Liga Antidifamación, Free Press y GLAAD. En febrero de 2020, Avaaz llevó a cabo una campaña específica sobre el negacionismo del cambio climático en YouTube y otras plataformas, que se basaba en un informe detallado elaborado por la organización (Kavenna, 2019; Live5, 2009). Avaaz pidió "a todas las plataformas de medios sociales que desintoxiquen sus algoritmos poniendo fin a la amplificación y monetización de la desinformación y el discurso del odio". También instaba "a los reguladores a convertir esto en un requisito legal" y exigía que "las plataformas trabajen con expertos independientes para rastrear y degradar a los creadores de desinformación repetida y deliberada" (Noone, 2021). Cabe señalar que el grupo modificó el texto inicial de la petición para eliminar la "exigencia de 'desinformar' a los creadores de desinformación repetida y deliberada" (Noone, 2021). Aunque no se dio ninguna razón para esta enmienda, sospechamos que está relacionada con la

[2] Ver https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2021/how-and-why-do-consumers-access-news- social-media ; https://www.freepress.net/sites/default/files/2022-11/stop_toxic_twitter_coalition_open_letter_to_ twitter_final.pdf

pendiente resbaladiza en la que las peticiones de desinformar a individuos o grupos que venden desinformación pueden volverse en contra de los actores progresistas y utilizarse para restringir sus voces en las redes sociales. Los llamamientos al boicot y a la desinformación deben tener en cuenta las implicaciones para la libertad de expresión en todo el espectro político. Además, para que tales acciones sean eficaces, necesitan el respaldo de destacados grupos activistas y anunciantes, de modo que se consideren lo suficientemente eficaces como para que otros se unan a ellas y puedan atraer suficiente cobertura informativa.

Los ataques también pueden producirse de forma más directa, como la piratería informática. Por ejemplo, Twitter y Facebook han sido blanco de ataques de denegación de servicio en los que los ordenadores impiden a los usuarios acceder a la plataforma o ralentizan su uso. Estos ataques no siempre han estado claramente relacionados con críticas a las plataformas en sí, sino con protestas contra el papel de dichas plataformas a la hora de dar voz a determinados puntos de vista políticos, por ejemplo en relación con los conflictos de Rusia con los países vecinos (Hong, Meier y Bergman, 2020). Sin embargo, el *hacktivismo* requiere sofisticados conocimientos técnicos y conlleva el riesgo de detención y otras repercusiones. Esta es probablemente la razón por la que no hay constancia de casos de hacktivismo medioambiental, ni siquiera por parte de grupos como Extinction Rebellion, que se centran en la acción disruptiva (al menos hasta su reciente cambio de estrategia), aunque el grupo mantuvo debates internos sobre hacktivismo durante la pandemia.[3] Para la académica Gabriella Coleman, que ha llevado a cabo una amplia investigación sobre Anonymous, esto puede deberse a que hay pocas coincidencias entre los *hackers* empedernidos y los ecologistas empedernidos (Rucht, 2004), lo que significa que el movimiento ecologista carece de las habilidades y la experiencia necesarias para participar en este tipo de activismo. Por el contrario, son los activistas medioambientales quienes han sido víctimas de ataques de piratas informáticos. Por ejemplo, en 2017, grupos

[3] Ver https://riseup.net/

ecologistas que llevaban a cabo una campaña contra Exxon Mobil por el cambio climático recibieron correos electrónicos de suplantación de identidad por parte de cuentas que se hacían pasar por sus colegas y abogados, como parte de "una extensa operación de pirateo por encargo que durante años ha tenido como objetivo las cuentas de correo electrónico de funcionarios gubernamentales, periodistas, bancos, activistas ecologistas y otras personas" (Kolodni, 2016).

Las acciones colectivas que siguen una estrategia de ataque suelen considerarse intervenciones espectaculares, por lo que es probable que atraigan la atención de los medios de comunicación. Sin embargo, la información de los medios de comunicación tiende a centrarse en el ataque en sí, más que en el mensaje que intenta transmitir, lo que dificulta su resonancia entre el público en general y los responsables políticos. Al mismo tiempo, los ataques que perturban el uso cotidiano de las redes sociales por parte de los usuarios corren el riesgo de generar molestias, lo que de nuevo puede restringir el impacto del mensaje.

Alternativas (erosión del capitalismo)

La estrategia de las alternativas (o erosión del capitalismo) implica que los activistas construyan sus propias plataformas de medios sociales o propiedades digitales donde puedan trabajar en red sobre cuestiones sociales y difundir información alternativa al público. Estas plataformas funcionan con reglas diferentes: a menudo están diseñadas por defensores del software libre y de código abierto (FOSS), lo que significa que el código está abierto para que todos puedan utilizarlo, adaptarlo y cambiarlo, siempre que no lo hagan por motivos comerciales. Estas plataformas también operan con diferentes políticas de anonimato y privacidad, en un esfuerzo por garantizar la seguridad de sus usuarios. Algunos ejemplos son la plataforma N-1 desarrollada por activistas en España justo antes de la primera etapa del movimiento de los Indignados en 2011, así como RiseUp!, Crabgrass, y

Occupii, la alternativa activista a Facebook creada por Occupy Wall Street en 2011.[4] Otros ejemplos incluyen plataformas de *streaming* de vídeo como BitChute (antes también Vine o Periscope) o canales de podcast alojados fuera de las plataformas comerciales dominantes para eludir la moderación. Los activistas pueden utilizar además plataformas como Mastodon, que está surgiendo ahora como alternativa a Twitter, que, aunque no han sido desarrolladas explícitamente por movimientos sociales, siguen funcionando de forma acorde con los valores progresistas.

También existen alternativas a la mensajería instantánea o al correo electrónico que facilitan procesos de organización interna más seguros para los movimientos sociales. Por ejemplo, Riseup.net, una red social independiente con sede en Seattle, ha proporcionado servicios cifrados de correo electrónico seguro y gestión de listas de correo para los movimientos sociales desde su creación en 1999-2000. Más recientemente, plataformas como Signal, Telegram o GroupMe también se han utilizado para la coordinación, con Telegram en particular facilitando tanto la comunicación interpersonal como la difusión. Estos canales también son utilizados por activistas medioambientales que emplean tácticas más disruptivas.

Los movimientos sociales han creado sus propias plataformas para difundir información sobre sus causas e informar sobre sus movilizaciones, en un esfuerzo por hacer frente a la marginación y la desinformación que difunden la mayoría de los principales medios de comunicación y plataformas de redes sociales. Un ejemplo es Unicorn Riot, un colectivo de noticias en línea sin ánimo de lucro fundado en 2015 por activistas que participaron en medios de comunicación alternativos en torno al movimiento Occupy, las movilizaciones contra

[4] Ver Standing Rock: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022/how-people-access-and-think-about-climate- change-news; Robertson, Craig (15 de junio de 2022). How people access and think about climate change news. *Reuters institute*. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022/how-people-access-and-think-about-climate-change-news/

las arenas bituminosas y las protestas de Ferguson.[5] [y 6] Unicorn Riot informó desde el terreno en Dakota del Norte durante las protestas #NODAPL o Dakota Access Pipeline Protests en 2016, cuando diferentes tribus de nativos americanos se opusieron a la construcción de un oleoducto que transportaba crudo desde Dakota hasta Illinois. Los manifestantes consideraban que el oleoducto, que iba a atravesar la reserva india de Standing Rock, suponía un grave peligro de contaminación del agua. Autodenominados *protectores del agua*, los activistas establecieron un campamento de protesta en la zona e intentaron detener la construcción del oleoducto. Los principales medios de comunicación ofrecieron escasa cobertura informativa, mientras que destacados periodistas de investigación, como Amy Goodman, cofundadora y presentadora de Democracy Now!, fueron detenidos acusados de disturbios. En cambio, Unicorn Riot pudo ofrecer una cobertura independiente de las protestas, con periodistas que permanecieron en el campamento y entrevistaron a los manifestantes (Robertson, 2022). La plataforma en línea descentralizada es, por tanto, un buen ejemplo del tipo de medios de comunicación comunitarios creados al servicio de los movimientos sociales y de la importancia que sigue teniendo el periodismo producido desde *dentro de las comunidades activistas*.

Con algunas excepciones notables, sin embargo, los esfuerzos por construir alternativas anticapitalistas tienden a ser efímeros, carecen de financiación y son incapaces de sustituir por completo los servicios que ofrecen los medios sociales corporativos. De lo que también

[5] Las movilizaciones contra las arenas bituminosas fueron protestas contra la construcción de oleoductos que transportan arenas bituminosas en Canadá en 2014. Las arenas bituminosas son un tipo de petróleo de baja calidad cuya extracción y procesamiento suele ser más peligroso para el medio ambiente. En las movilizaciones contra las arenas bituminosas a los grupos ecologistas se unieron manifestantes de los Pueblos Originarios. Idle No More fue uno de los grupos clave en la organización de las protestas.

[6] The Ferguson protests [las protestas Ferguson] constituyó un evento clave en el movimiento Black Lives Matter. Surgieron en Ferguson, Misouri tras el asesinato de Michael Brown a manos de la policía en agosto de 2014.

carecen estas plataformas es de *efectos de red*, un término que apunta a una dinámica crucial de las redes sociales: cuantos más miembros adquieren, más útiles resultan, ya que pueden utilizarse para comunicarse con un mayor número de participantes. En realidad, muchas plataformas alternativas solo las utilizan los conversos, activistas experimentados que ya están familiarizados con las movilizaciones en cuestión. Por lo tanto, al comunicarse únicamente en estos espacios, los activistas pueden permanecer invisibles dentro de un nicho comunicativo.

Adaptación (domar el capitalismo)

Las limitaciones de las plataformas alternativas a pequeña escala llevan a menudo a los activistas a utilizar aplicaciones corporativas como Facebook, Twitter e Instagram para atraer a un público más amplio. Los activistas adoptan así una estrategia de adaptación, es decir, se adaptan a las reglas de las plataformas corporativas, tratando de aprovechar su poder para aumentar la visibilidad de su movimiento.

Las plataformas corporativas de medios sociales se han convertido en canales clave para publicar información sobre el cambio climático. La mayoría de los principales grupos y movimientos activistas utilizan sus cuentas en las redes sociales para difundir información sobre su causa. Las redes sociales también han facilitado el auge de los *influencers verdes*, activistas medioambientales que cuentan con un gran número de seguidores en las redes sociales (Martini, 2018). Junto a ellos, encontramos colectivos como EcoTok, que informan sobre cuestiones medioambientales en TikTok (Kavada y Specht, 2022). Según el Reuters Institute for the Study of Journalism (Instituto Reuters para el Estudio del Periodismo), estos canales son especialmente importantes para los usuarios menores de treinta y cinco años, que "suelen ser dos o tres veces más propensos a decir que prestan atención a famosos, personalidades de las redes sociales o activistas para obtener noticias

sobre el cambio climático que las personas mayores de treinta y cinco años" (Telford, 2021).

También hay casos en los que los canales de las redes sociales han permitido que voces marginadas salgan a la palestra. Un ejemplo es la página de Facebook Digital Smoke Signals, fundada por el fallecido periodista nativo americano Myron Dewey, que proporcionó una importante cobertura de las protestas #NODAPL. La página fue uno de los medios de noticias más seguidos sobre las protestas y algunos de sus videos acumularon más de 2,5 millones de visitas. Facebook live también se utilizó para informar en directo de las protestas, lo que permitió a los activistas informar desde el terreno sin filtros ni censura. En los años transcurridos desde la Primavera Árabe, la retransmisión en directo se ha convertido en una importante aplicación en manos de los reporteros ciudadanos. Mientras que en la oleada de movilizaciones de 2011 la retransmisión en directo corría a cargo de pequeñas empresas de nueva creación, a mediados de la década de 2010 la mayoría de las principales plataformas de medios sociales, incluidas Instagram y Facebook, empezaron a ofrecer esta funcionalidad, eclipsando así a los actores más pequeños del sector.

Las estrategias de adaptación también incluyen el desarrollo de nuevos enfoques para comprometerse con los objetivos de la campaña o para demostrar el propio apoyo a una causa, que se adaptan al entorno de las redes sociales. Puede tratarse de actos relativamente *sencillos*, como añadir un banner a la foto de perfil en las redes sociales para mostrar el apoyo a una causa medioambiental. Aunque estas tácticas son útiles para ganar visibilidad en un panorama mediático saturado, a menudo se las califica de *clicktivismo*, un término que combina *click* y *activismo*. Los críticos señalan el escaso compromiso necesario para participar en este tipo de activismo y su potencial para crear una sensación engañosa de eficacia y conexión. Sin embargo, esto depende del contexto político, ya que en los países más restrictivos y autoritarios un tuit o una publicación en Facebook puede llevarte fácilmente a la cárcel, o incluso enfrentarte a una pena de muerte. En otras palabras, el *clictivismo* depende del ojo del espectador.

Las estrategias de adaptación también están asociadas a la aparición de nuevas tácticas activistas como las tormentas de Twitter, por las que los usuarios bombardean un *hashtag* con tuits para convertirlo en *trending topic*. El secuestro de *hashtags* es una variante de esta táctica, en la que los activistas se hacen con el control del *hashtag* de un objetivo. Los activistas medioambientales también han sido pioneros en la táctica del *greentrolling* de las cuentas de redes sociales que difunden desinformación sobre el clima o se dedican al *lavado verde*. El "greentrolling" es una estrategia de adaptación, ya que se basa en la adopción de "una forma de refutación que se asocia mejor con el "trolling" de los "ne'er-do-wells" de internet, impregnada de voz, brío y humor mordaz" (Just Stop Oil). Al dirigirse a las redes sociales de grandes empresas, los activistas climáticos consiguen un mayor alcance para sus mensajes y atraen el interés de los principales medios de comunicación. Un ejemplo famoso se produjo en noviembre de 2020, cuando Shell publicó una encuesta en las redes sociales en la que preguntaba a los usuarios "¿qué estás dispuesto a hacer para reducir las emisiones?". La encuesta recibió muchas respuestas irónicas de activistas medioambientales, políticos y usuarios de a pie, incluidas personas de alto perfil como Greta Thunberg y Alexandria Ocasio-Cortez, que utilizaron la encuesta para denunciar el papel de Shell en el aumento de las emisiones (Askanius, 2012).

Sin embargo, para llevar a cabo estrategias de adaptación, los activistas tienen que obtener un conocimiento íntimo de cómo funcionan las plataformas de medios sociales comerciales. Esto puede exigir una mayor profesionalización de las comunicaciones de los activistas, lo que llevaría a los movimientos a contratar a profesionales de los medios sociales o a proporcionar formación a los administradores de estos medios, así como a desarrollar directrices y protocolos específicos.

La estrategia de adaptación tiene varios riesgos para los activistas progresistas. Les obliga a renunciar a la gestión directa de sus espacios de visibilidad, ya que pueden ejercer un control muy limitado sobre los materiales que publican en plataformas comerciales o sobre la infraestructura que permite su publicación. Esto hace que su visibilidad

sea especialmente frágil: si un medio de comunicación social decide eliminar el perfil de un grupo, es probable que desaparezca todo el archivo de contenidos publicados hasta ese momento, junto con la red de contactos creada gracias al uso continuado de la plataforma.

Las plataformas comerciales de medios sociales ajustan constantemente sus algoritmos para impedir que los creadores de contenidos atraigan a audiencias más amplias sobre la base del alcance orgánico. Esto les permite cobrar a los creadores por llegar a sus propios seguidores con precios que a veces resultan desorbitados para la mayoría de los grupos activistas. También crea asimetrías de poder en los esfuerzos de los activistas por contrarrestar la desinformación. Los grupos que difunden información falsa sobre, por ejemplo, el papel de los contaminadores en la ralentización de la adopción de políticas sobre el cambio climático suelen estar financiados por esos mismos contaminadores, capital que les permite pagar por un mayor alcance. Las redes sociales también explotan los datos de los usuarios creados por la actividad de los movimientos sociales en la plataforma. Cuanto más polarizante es la causa, más beneficios genera para la empresa, ya que alimenta el tráfico y la actividad de los usuarios. Por tanto, no es de extrañar que la estrategia de adaptación tienda a estar reñida con valores fundamentales de las comunidades activistas de izquierdas, como su aversión al capitalismo. De hecho, el uso de plataformas propietarias suele estar en el centro de los conflictos internos de los grupos activistas, entre quienes apoyan su uso por razones pragmáticas y quienes se niegan a utilizarlas.

La vigilancia corporativa de las principales redes sociales también alimenta los sistemas de vigilancia estatal. Se trata de la doble espada de la visibilidad, en la que hacerse más visible en las redes sociales también hace a los grupos activistas más vulnerables ante las autoridades. Una estrategia clave a este respecto es utilizar plataformas comerciales para promocionar actos públicos, pero mantener toda la organización interna en plataformas alternativas con comunicación encriptada o fuera de los medios digitales, empleando los viejos métodos de las reuniones secretas cara a cara. En otras palabras, los grupos activistas

deben combinar diferentes estrategias y plataformas, en función de las tareas que deban realizar y de su privacidad o necesidad de mayor visibilidad.

Avanzar: colaboración, interconectividad y curaduría

Los movimientos sociales progresistas, y los activistas medioambientales en particular, pueden utilizar diferentes estrategias tanto para desafiar como para aprovechar el poder de las redes sociales comerciales. Pueden abstenerse, construir alternativas, pasar al ataque y adaptarse. Cada una de ellas tiene ventajas e inconvenientes en términos de eficacia e impacto, y depende del contexto. En la práctica, los activistas suelen desplegar algunas o todas las formas.

En otras palabras, los cuatro tipos de estrategias descritas en la *cuádruple A* de Rucht funcionan mejor combinadas que por separado. Sin embargo, es precisamente este arte de perseguir diferentes estrategias simultáneamente lo que resulta más formidable. ¿Cuál debe ser el equilibrio entre desafiar a las plataformas corporativas y, al mismo tiempo, aprovechar su poder? ¿Y puede un grupo hacer todo esto solo o debe trabajar en coalición, de modo que pueda especializarse en estrategias específicas?

En este sentido, trabajar en colaboración parece ser el camino a seguir. Esto puede adoptar la forma de coaliciones más formales y plataformas paraguas o producirse de manera más informal mediante el desarrollo de temas comunes en las campañas, el intercambio de recursos, así como compartiendo los contenidos de los demás y creando cabeceras de comunicación más densamente hipervinculadas. Los grupos ecologistas, por ejemplo, también han empezado a trabajar de un modo más interseccional, considerando las cuestiones sobre las que hacen campaña desde las perspectivas de las distintas partes interesadas y trazando un mapa de los sistemas de poder entrelazados que hay que superar (Wright, 2019). Este tipo de colaboración y formación de coaliciones debe reflejarse con más fuerza en el ámbito digital, con

una mayor hipervinculación e interconectividad entre los grupos ecologistas, ya sea a través de cuentas de redes sociales en plataformas comerciales o de medios de comunicación alternativos. En este sentido, los estudios sobre el activismo en video en torno a la justicia climática y los movimientos de justicia social en la segunda década del siglo XXI mostraron conexiones muy débiles entre los actores en YouTube (Uldam, 2018). Las acciones y los actores dentro de los movimientos de justicia social estaban en gran medida desconectados, o al menos no se unían de manera significativa en esa plataforma en particular. Por lo tanto, como posible lugar de resistencia, YouTube no proporcionó un espacio para prácticas mediáticas sostenibles, horizontales y radicales (Tactical Tech).

Esto parece aún más cierto hoy en día, una década después y en un contexto en el que YouTube se discute principalmente en términos de madrigueras de conejo, radicalización y desinformación en lugar de difusión democrática, pruebas visuales y testigos oculares radicales. Cuando hay pruebas que sugieren que se está materializando de hecho una red de acciones conectivas, el proceso está dirigido por fuerzas reaccionarias antidemocráticas y de extrema derecha. En gran medida, han logrado conectarse por encima de las líneas partidistas y las diferencias internas del movimiento, crear una audiencia considerable y formar una red coherente de canales y contenidos relacionados que se extienden a una ecología mediática más amplia de medios de extrema derecha alternativos. Lo hacen a través de una serie interconectada de prácticas conectivas que incluyen apariciones como invitados en los canales de YouTube de los demás, retransmisiones en directo conjuntas, así como diversas prácticas de referencias e hipervínculos.

Incluso cuando la derecha ha sido desplazada, por ejemplo tras la manifestación Unite the Right en Charlottesville en 2017, los grupos de extrema derecha han migrado a plataformas Alt-Tech que son más difíciles de controlar, como Gab, Parler, Gettr, BitChute, Rumble, PewTube, Odysee, Hatreon y muchas otras. Estas plataformas han sido diseñadas siguiendo los modelos de las grandes plataformas tecnológicas e imitan sus características, al tiempo que ofrecen anonimato

y muchas menos restricciones sobre el nivel de material ofensivo y dañino que puede publicarse.

La extrema derecha ha sido muy capaz de participar en una amplia gama de plataformas al mismo tiempo y con diferentes propósitos –combinando lo alternativo y lo dominante–, adoptando deliberadamente un tono diferente para las distintas plataformas con cierto grado de éxito. A ello contribuye, por supuesto, que, en comparación con los movimientos progresistas, los activistas de extrema derecha tienen menos escrúpulos a la hora de utilizar un tono más ofensivo, irreverente y populista que funciona bien en las redes sociales en términos de viralidad y optimización algorítmica. La extrema derecha también es menos reacia a utilizar plataformas comerciales y lucrativas, y ha encontrado formas de monetizar sus contenidos intercalando estrategias comerciales con técnicas de propaganda política.

Los activistas de extrema derecha han construido así un ecosistema de plataformas Alt-Tech que ha superado a los medios alternativos progresistas en términos de *crowdsourcing* y éxito en la recaudación de fondos para *start-ups* tecnológicas. Por supuesto, el reciente éxito de la extrema derecha ha sido el resultado no solo de hábiles estrategias en las redes sociales, sino también de un contexto político más amplio que favorece sus objetivos. Tras la represión –y, en algunos sectores, el fracaso percibido– de los movimientos progresistas de 2011, parte de la misma ira contra el *establishment* ha sido aprovechada por actores reaccionarios y conservadores. Los activistas de extrema derecha han aprovechado así al máximo las oportunidades que les brinda estar en línea con corrientes políticas más amplias y, en particular, con el auge de la política del miedo que acompaña a la incertidumbre y al aumento de la desigualdad. Sin embargo, la tormenta perfecta de crisis económica, social y climática a la que nos enfrentamos actualmente también está abriendo la puerta a un cambio radical en el lado progresista del espectro político. En este contexto, es fundamental desarrollar una mayor conectividad entre grupos, temas y medios digitales.

Aparte de los hipervínculos y la interconectividad, la coherencia y la continuidad también ayudarán a los grupos progresistas, y al

movimiento ecologista en particular, a aprovechar el poder digital. Los vínculos duraderos de colaboración pueden aliviar los inmensos esfuerzos del trabajo voluntario para establecer y gestionar plataformas alternativas mediante el desarrollo de rutinas y un depósito de conocimientos y experiencia. Ese trabajo también es necesario para atacar a las redes sociales comerciales, que a menudo se basan en la meticulosa recopilación de información sobre la lógica lucrativa de las grandes tecnológicas. La colaboración sostenida a lo largo del tiempo hace posible este trabajo voluntario, ya que permite la transferencia de conocimientos entre diferentes grupos y generaciones de activistas, recopilando información de experiencias pasadas, de lo que funciona y lo que no, y garantizando que estas lecciones se transmitan y se combinen con nuevas ideas para las nuevas generaciones de activismo.

Como demuestra el ejemplo de la extrema derecha, la selección de contenidos digitales es otro aspecto crucial de la interconectividad y la colaboración. La curación se refiere al proceso de encontrar, seleccionar, organizar e interrelacionar mensajes adecuados. De este modo, ayuda a crear una red colaborativa de actores y comunicaciones interconectados que proporciona un mensaje rico y coherente y ofrece a los usuarios diferentes puntos de entrada al *espacio de mensajes* de los movimientos progresistas. En el fondo, la curación tiene que ver con el cultivo de la comunidad, la conectividad y la participación, una lógica que va en contra de los modelos de negocio de las redes sociales, que fomentan el individualismo y la personalización de la acción política.

Obviamente, estas estrategias de colaboración suelen tropezar con numerosos obstáculos. Las diferencias doctrinales e ideológicas, por ínfimas que parezcan a los de fuera, pueden dividir a los movimientos progresistas y aumentar el faccionalismo. Una mayor colaboración puede plantear riesgos para la legitimidad, ya que los grupos pueden temer alinearse más estrechamente con, por ejemplo, un actor más radical, ya que pueden verse manchados por asociación. O la razón puede ser más interesada, ya que los grupos pueden querer conservar audiencias en sus propias propiedades de medios sociales en lugar de compartirlas con actores afines. La falta de financiación y recursos

para la política progresista puede llevar a competir por las audiencias y a una falta de conectividad entre los grupos activistas en línea.

Así pues, para que la colaboración funcione, los activistas deben comprometerse a trabajar juntos para ofrecer alternativas. De cara al futuro, esta creencia en el valor de construir redes de redes más amplias es lo que puede ayudar a los activistas a aprovechar el poder de los medios digitales, resistir a las grandes tecnológicas y cambiar el mundo.

Bibliografía

Askanius, Tina (2012). *Radical online video: YouTube, video activism and social movement media practices* [Tesis doctoral]. Lund Studies in Media and Communication 17, Lund University.

Avaaz (16 de enero de 2020a). Why is YouTube Broadcasting Climate Misinformation to Millions? https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/

Avaaz (5 de febrero de 2020b). Social media: Detox the Algorithm. https://secure.avaaz.org/campaign/en/detox_the_algorithm_loc/

Bacchi, Umberto (23 de febrero de 2022). Explainer: Facebook and climate change: can falsehoods be reined in? Reuters. https://www.reuters.com/business/cop/facebook-climate-change-can-falsehoods-be-reined-2022-02-23/

Data Detox Kit (26 de enero de 2021). How many trees does it take to power the internet? https://www.datadetoxkit.org/en/wellbeing/environment/

Global Witness (28 de marzo de 2022). The climate divide: How Facebook's algorithm amplifies climate disinformation. https://www.globalwitness.org/en/campaigns/digital-threats/climate-divide-how-facebooks-algorithm-amplifies-climate-disinformation/

Hong, Nicole, Meier, Barry y Bergman, Ronen (9 de junio de 2020). Environmentalists Targeted Exxon Mobil. Then Hackers Targeted Them. *The New York Times*. https://www.nytimes.com/2020/06/09/nyregion/exxon-mobil-hackers-greenpeace.html

Just Stop Oil. https://juststopoil.org/background/

Kavada, Anastasia y Specht, Doug (2022). Environmental movements and digital media. En María Grasso y Marco Guigni (eds.), *Routledge Handbook of Environmental Movements*. Nueva York: Routledge.

Kavenna, Joanna (4 de octubre de 2019). Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy'. *The Guardian*. https://www.theguardian.com/books/2019/oct/04/shoshana-zuboff-surveillance-capitalism-assault-human-automomy-digital-privacy

Kolodny, Lora (15 de octubre de 2016). Multi-media journalists face jail time after reporting on North Dakota pipeline protest. *Join Tech Crunch*. https://techcrunch.com/2016/10/15/multi-media-journalists-face-jail-time-for-reporting-on-north-dakota-pipeline-protest/

Live 5 news (6 de agosto de 2009). Hackers attack Twitter, Facebook also slows down. https://www.live5news.com/story/10860187/hackers-attack-twitter-facebook-also-slows-down/

Martini, Michele (2018). Online distant witnessing and live-streaming activism: emerging differences in the activation of networked publics. *New Media & Society*, 20(11), 4035–4055.

Milman, Oliver (2 de diciembre de 2022). #ClimateScam: denialism claims flooding Twitter have scientists worried. *The Guardian*. https://www.theguardian.com/technology/2022/dec/02/climate-change-denialism-flooding-twitter-scientists

Noone, Greg (30 de septiembre de 2021). The return of the hacktivists. *Techmonitor 30*. https://techmonitor.ai/technology/cybersecurity/the-return-of-hacktivists

Robertson, Craig (15 de junio de 2022). How people access and think about climate change news. *Reuters institute*. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022/how-people-access-and-think-about-climate-change-news/

Rucht, Dieter (2004). The quadruple 'A': Media strategies of protest movements since the 1960s'. En WimVan De Donk, Brian D. Loader, Paul G. Nixon y Dieter Rucht (eds.), Cyberprotest: New media, citizens and social movements (pp. 25-48). Londres: Routledge.

Shearer, Elisa (12 de enero de 2021). More than eight-in-ten Americans get news from digital devices. Pew Research Center. https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital- devices/

Standing Rock. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2022/how-people-access-and-think-about-climate-change-news

Tactical Tech. Data Detox Kit. https://tacticaltech.org/projects/data-detox-kit/

Telford, Taylor (30 de julio de 2021). These self-described trolls tackle climate disinformation on social media with wit and memes. *The Whashington Post*. https://www.washingtonpost.com/business/2021/07/30/greentrolling-big-oil-greenwashing/

Uldam, Julie (2018). Social media visibility: challenges to activism. *Media, Culture & Society*, 40(1), 41–58. https://doi.org/10.1177/0163443717704997

Wright, Erik Olin (2019). *How to be an anti-capitalist in the 21st century.* Londres: Verso. Books

Sobre autoras y autores

Apoorva PG es coordinadora de campañas para Asia y el Pacífico del comité nacional de Palestinian Boycott, Divestment and Sanctions (BDS). Es una de las organizadoras de las campañas de BDS contra HP y el Proyecto Nimbus, el contrato de Google y Amazon para proporcionar servicios en la nube al gobierno y al ejército israelíes. Estudió Sociología y anteriormente participó en campañas de acceso a la educación, copyleft y software libre en la India.

Mizue Aizeki es directora ejecutiva del Laboratorio de Resistencia a la Vigilancia. Durante casi veinte años, Mizue se ha centrado en poner fin a las injusticias –incluida la criminalización, el encarcelamiento y el exilio– en las intersecciones de los sistemas de control penal y migratorio. Antes de trabajar en el Laboratorio, Mizue fue asesora principal del Proyecto de Defensa de los Inmigrantes (IDP) y directora del Proyecto de Vigilancia, Tecnología e Inmigración. Mizue es coeditora de *Resisting Borders and Technologies of Violence* (de próxima publicación en Haymarket Books, otoño de 2023).

Tina Askanius es profesora asociada de Medios y Comunicación en la Escuela de Artes y Comunicación de la Universidad de Malmö e investigadora afiliada al Institute for Future Studies de Estocolmo. Su investigación se centra en la interacción entre movimientos sociales, tecnologías mediáticas y procesos de mediación.

Tomás Balmaceda es doctor en Filosofía por la Universidad de Buenos Aires. Actualmente es Investigador del IIF (SADAF/CONICET) y parte del grupo GIFT, que analiza la tecnología y la inteligencia artificial a través de la lente de la filosofía. Autor de varios libros, sus intereses incluyen la ética de la influencia en redes, la nueva longevidad y la educación financiera para la población LGBTIQ+.

Laura Bingham dirige el Instituto de Derecho, Innovación y Tecnología de la Universidad de Temple. Anteriormente, Laura fue directora jurídica de la Open Society Justice Initiative. Estableció y dirigió un programa global sobre datos, tecnología y derechos humanos. Desde 2017, Laura ha impartido cursos sobre derechos humanos y migración forzada como miembro adjunto de la facultad en el Centro de Asuntos Globales de la Universidad de Nueva York.

Kean Birch es director del Instituto de Tecnociencia y Sociedad y profesor asociado en el Programa de Posgrado en Estudios de Ciencia y Tecnología de la Universidad de York, Canadá, donde investiga el surgimiento y las implicaciones del capitalismo tecnocientífico: http://www.keanbirch.net/

Chris Byrnes es abogado especializado en propiedad intelectual (PI), académico independiente y cofundador del colectivo artístico AbolishIP. Su trabajo se centra en la concesión ética de licencias de PI, la puesta en común de la PI basada en la web3 y el pirateo de la PI para proteger la biodiversidad y potenciar imaginarios radicales. Es doctor en Derecho por la Universidad de Georgetown, máster en Religión, Ética y Política por la Universidad de Harvard y licenciado en Física por la Universidad de Denison.

Julia Choucair Vizoso es productora independiente de conocimiento y cofundadora del colectivo artístico AbolishIP. Trabaja en el ámbito de la justicia medioambiental y climática en el mundo árabe, imparte cursos de economía política y, ocasionalmente, traduce literatura

árabe al inglés. Es doctora en Ciencias Políticas por la Universidad de Yale y licenciada en Estudios Árabes y Servicio Exterior por la Universidad de Georgetown.

Cory Doctorow es un prolífico escritor y novelista de ciencia ficción, periodista y activista tecnológico. Es consultor especial de la *Electronic Frontier Foundation* (eff.org), una ONG que trabaja sobre libertades civiles y defiende la libertad en las leyes, políticas, estándares y tratados tecnológicos. Su libro más reciente es *Chokepoint Capitalism* (en coautoría con Rebecca Giblin), una exposición de cómo los monopolios tecnológicos han sofocado los mercados laborales creativos y cómo los movimientos podrían contraatacar.

Roberto J. González es presidente del Departamento de Antropología de la Universidad Estatal de San José. Es autor de varios libros, entre ellos *Guerra virtual: la búsqueda para automatizar conflictos, militarizar datos y predecir el futuro*, *Conectado: cómo un pueblo mexicano construyó su propia red de telefonía celular* y la colección coeditada Militarización: un lector. Es miembro fundador de la Red de Antropólogos Preocupados.

Maximilian Jung se graduó recientemente en el Programa de Estudios Globales de la Universidad de Leipzing y Gante. Su investigación se centra en el ámbito ambiental, decolonial y el de la historial global de la economía digital. Es también activista por la justicia climática en la plataforma Degrowth Bélgica.

Anne Kaun es catedrática de Medios y Comunicación en la Universidad de Södertörn. En 2021 fue Wallengerg Academy fellow y dirige varios proyectos que exploran el estado de bienestar digital y la toma de decisiones automatizada. En 2023 saldrá a la luz su libro *Prison Media*, que publicará MIT Press.

Anastasia Kavada es profesora de Medios y Política en la Escuela de Medios y Comunicación de la Universidad de Westminster, donde

dirige el Máster en Medios, Campañas y Cambio Social. Su investigación se centra en los vínculos entre medios digitales, movimientos sociales, democracia participativa y campañas para el cambio social.

Alice Mattoni es profesora asociada en el Departamento de Ciencias Políticas y Sociales de la Universidad de Bolonia. Investiga la relación entre los movimientos sociales y los medios de comunicación, digitales y de otro tipo. Es una de las tres cofundadoras y actual editora de la Routledge Series Media and Communication Activism.

Santiago Narváez es investigador desde 2016 en la ONG de derechos digitales R3D: Red en Defensa de los Derechos Digitales, con sede en Ciudad de México, donde investiga cómo se ejerce la vigilancia gubernamental y su impacto en los derechos humanos. Es licenciado en Relaciones Internacionales y tiene formación en análisis de datos.

Karina Pedace es profesora de grado y posgrado en la Universidad de Buenos Aires y la Universidad Nacional de Matanza, y es investigadora del Instituto de Investigaciones Filosóficas de la Sociedad Argentina (IIF-SADAF-CONICET). Sus áreas de investigación actuales incluyen la filosofía de la tecnología, la metafísica de la mente y las metodologías de investigación. Es secretaria ejecutiva de la Red Latinoamericana de Mujeres Filósofas de la UNESCO y cofundadora del Grupo de Investigación en Inteligencia Artificial, Filosofía y Tecnología (GIFT). En 2022, fue reconocida internacionalmente como una de las 100 mujeres brillantes en ética de la IA https://womeninaiethics.org/the-list/of-2022/

Nils Peters es miembro de Sociología Económica de la LSE.

Tobías J. Schleider es abogado y especialista en derecho penal de la Universidad Nacional de Mar de Plata y doctor de la Universidad de Buenos Aires en Filosofía del Derecho. Es profesor de la Universidad Nacional del Sur, donde dirige la Licenciatura en Seguridad Pública.

Sus líneas de investigación actuales incluyen la prevención de la violencia apoyada en tecnología, la teoría de la acción humana, la causalidad y la influencia de la suerte en la atribución de responsabilidad.

Julie Uldam es profesora asociada en la Copenhagen Business School, donde dirige el proyecto Imagining Digital Power and the Power of Digital Imagination in Business and Society Encounters. Su investigación explora el papel de los medios digitales de activismo en los retos sociales, incluida la crisis climática y el debate democrático.

La tecnología digital ha concentrado un vastísimo poder económico, lo cual, sumado a la colusión de los Estados, ha traído como resultado una extendida vigilancia, una creciente desinformación y un debilitamiento de los derechos de trabajadores y trabajadoras. Este libro, la traducción al español del reporte número 11 de Estado de Poder, expone a los actores, las implicancias y las estrategias de este poder digital, y comparte ideas sobre cómo los movimientos podrían llevar esta tecnología para que esté bajo el control popular.

FUHEM educación + ecosocial
tni transnationalinstitute
CLACSO
ISBN 978-987-813-629-5