LIBERTAD DE EXPRESIÓN Y FAKE NEWS

Un futuro sin secretos

Tecnología, vigilancia, derechos y libertades

Stephen Armstrong



Una ciberactivista con su ordenador. Fotografía: Jordi Borràs

«En el futuro, no habrá secretos», afirma el corresponsal de seguridad de la BBC, Gordon Corera. «En el futuro, todos seremos espías y nos espiaran a todos.»

¿La visión de Corera es utópica o distópica? Cuando consideramos el lento recorrido por parte de demócratas y filósofos hacia un gobierno transparente desde la Ilustración hasta la actualidad, no podemos ignorar el panóptico: la 'cárcel perfecta' imaginada por el filósofo inglés Jeremy Bentham, que creía que el poder debía ser visible y no verificable. Bentham pensaba que con una vigilancia constante se reformaría la moral, se preservaría la salud y se revitalizaría la industria.

La visión de Bentham era limitada por la tecnología de su época: describió celdas apiladas alrededor de una torre central, siempre abierta, con todas las salas inundadas de luz. El filósofo francés Michel Foucault odiaba esta idea: la calificaba de «jaula cruel e ingeniosa», una mazmorra donde la desviación significaba la muerte.

Si Corera tiene razón, ya vivimos en un panóptico tecnológico, aunque en la visión de Bentham, la vigilancia sólo iba en una dirección. Si todos nosotros también somos espías, entonces hay un cierto poder en nuestra mirada. ¿En qué pensamos cuando pensamos en tecnología, vigilancia, derechos y libertades? ¿En la búsqueda masiva de correos

electrónicos para rastrear y controlar a los disidentes? ¿En las agencias gubernamentales que toman el control de nuestros teléfonos inteligentes para grabar nuestros momentos más íntimos? ¿O en los fans del K-pop en TikTok que capturan las etiquetas de la derecha para apoyar al movimiento *Black Lives Matter* y en los activistas independentistas catalanes que utilizan el modo avión para crear centros de comunicaciones secretos?

De alguna manera estamos luchando por el alma del ordenador. Para situarnos en la creación de esta alma, tenemos que remontar la historia de la libertad y la tecnología hasta el día en que pusieron en marcha Colossus, el primer ordenador programable del mundo, en la casa rural de Bletchley Park, donde se encontraba la escuela británica de código y cifrado durante la Segunda Guerra Mundial. Colossus se construyó con un propósito: la vigilancia. Fue diseñado exclusivamente para descifrar los mensajes encriptados con el código Lorenz que se intercambiaban Hitler y sus generales durante la Segunda Guerra Mundial. Parece que el ordenador fue construido para espiarnos.

> Muchos de los fundadores de Internet eran idealistas de la contracultura y veían el ordenador como un elemento libertador. ¿Se equivocaron?

Sin embargo, muchos de los fundadores de Internet eran idealistas de la contracultura, como el equipo de la revista estadounidense de cibercultura de los años ochenta y noventa *Mondo 2000*, los fundadores de la *Electronic Frontier Foundation* o incluso Tim Berners-Lee, el creador de la World Wide Web, y en la actualidad las campañas para la neutralidad de la red, la libertad en Internet y la democracia. Todos ellos veían, y aún ven, el ordenador como un elemento libertador. ¿Se equivocaron?

¿Internet nos hace libres?

«La premisa era que la red nos haría libres a todos, pero pronto se convirtió en un terreno de caza para las fuerzas policiales y en un espacio donde el negocio es el rey», argumenta Alan Pearce, un defensor y asesor en materia de privacidad personal. La filósofa y psicóloga Shoshanna Zuboff lo llama «capitalismo de vigilancia», donde nuestras vidas son espiadas tanto para obtener beneficios como para controlarlas. «Alguien secuestró nuestro sueño», dice Pearce. «Pero la gente es irreprimible y nos estamos poniendo al día. Así pues, nos hallamos en un juego interminable del gato y el ratón: encontramos la manera de escondernos, nos descubren, seguimos adelante, siempre cambiando, siempre protestando».

El gobierno catalán y los activistas independentistas ya han sobrevivido a un juego en línea del gato y el ratón con el Estado español. El 13 de septiembre de 2017, el gobierno español usó una orden judicial para cerrar las webs que difundían información sobre el referéndum sobre la independencia de Catalunya. Los activistas clonaban las webs tan rápidamente

como los bloqueaba el gobierno, hasta que agentes de la Guardia Civil entraron en la sede del registro .cat el 20 de septiembre, confiscaron ordenadores y detuvieron al director de tecnología de la empresa, Pep Masoliver.

«El gobierno español utilizó una infraestructura técnica *antifishing* para evitar que la gente fuera a determinados sitios web», explica John Graham-Cumming, director general de la empresa de seguridad web Cloudflare. Troy Hunt, consultor australiano de seguridad web que fundó el *breach site* 'Have I Been Pwned', comparte su conmoción. «Esto no es algo que normalmente se vea en una democracia moderna», argumentó. «Es el tipo de cosas que se ven en Turquía, Egipto, China e Irán».

Como respuesta, los activistas configuraron canales a través de aplicaciones de mensajería cifrada como Telegram, para guiar los usuarios de Internet hacia las webs afectadas mediante redes privadas virtuales y servicios de proxy. Durante el referéndum del 1 de octubre, los voluntarios de las mesas electorales se comunicaron a través de redes de datos clandestinas creadas al encaminar los teléfonos inteligentes a través de VPN para poder funcionar sin acceso a Internet. En la calle, los activistas y los organizadores del referéndum coreaban «modo avión» para instar a los votantes a reservar el ancho de banda de la red para las personas que trabajaban en los colegios electorales.

> La escala exponencial de la penetración de las tecnologías digitales en nuestras vidas significa que Google, como dijo Eric Schmidt en 2010, puede mirar nuestros mensajes y nuestra ubicación, utilizar la Inteligencia Artificial y, a continuación, predecir dónde iremos

Por un lado, esta es sólo la última de una larga serie de batallas entre las élites y los demócratas para el control y el uso de la tecnología de la información. En 1501, el papa Alejandro VI decretó la excomunión de cualquier persona que usara la imprenta sin la aprobación de la Iglesia. Durante los siguientes 40 años, Martín Lutero imprimir sus *Noventa y cinco tesis*, John Calvin produjo en masa las teorías del protestantismo y Copérnico publicó *Sobre las revoluciones de las esferas celestiales*, y todo ello desencadenó la revolución científica. Controlar la imprenta significaba controlar la información, el arma más poderosa en las guerras religiosas que sacudieron el continente. Desde entonces poco ha cambiado.

Por otra parte, la escala exponencial de la penetración de las tecnologías digitales en nuestras vidas significa que Google, como dijo Eric Schmidt en 2010, puede «mirar nuestros mensajes y nuestra ubicación, utilizar la Inteligencia Artificial y, a continuación, predecir dónde iremos. Muéstrenos 14 fotos suyas y podremos identificar quien es. Es posible que toda esta información esté a disposición de las autoridades. Si tiene algo que no quiere que nadie sepa, quizás mejor sería no hacerlo, así de claro».

Un control inédito

Esta nueva y profana alianza entre el capitalismo corporativo y el poder imperial del estado significa que el potencial de control y libertad va mucho más allá de los precedentes históricos. Vivimos en un mundo donde la Directiva Europea sobre la Conservación de Datos exige a los estados miembros de la UE que almacenen datos de telecomunicaciones de los ciudadanos entre seis meses y dos años, mientras que el sistema de crédito social de China registra comportamientos «buenos» y «malos», deniega billetes de avión a las personas «poco fiables» y permite que el Partido Comunista mida y reprima la disidencia. Asimismo, el gobierno de los Estados Unidos despliega tantos sistemas diferentes para controlar los mensajes, el tráfico en webs, datos de motores de búsqueda y «actividades sospechosas» que ha perdido el control sobre algunos proyectos, con lo cual también ha perdido software malicioso como Stuxnet a manos de piratas informáticos, que lo han usado para hacer caer el sistema sanitario del Reino Unido mediante un ataque de secuestro de datos.

«Los tanques, los rifles y la munición que han utilizado contra nosotros durante generaciones ahora se disfrazan de nueva tecnología para alcanzar los mismos propósitos coloniales», afirma Yeshimabeit Milner, fundadora y directora ejecutiva del movimiento *Data for Black Lives*. Sin embargo, cree que en estos momentos la lucha está lejos de haber terminado y que aún no se sabe quién será el vencedor. «Necesitamos que los datos y la tecnología se utilicen para cumplir su verdadera promesa de cambio social: ser liberadores y formar parte de una nueva forma de activismo que realmente pueda cambiar las condiciones y empoderarnos».

Desde hace años, los demócratas y los liberales han estado presionando para la transparencia: la luz del descubrimiento para desinfectar el secretismo y las mentiras de las élites. El resultado ha sido la desaparición de una larga tradición de secretismo radical, barrida por el impulso y la práctica de la transparencia. Históricamente, la democracia ha necesitado el secretismo en épocas turbulentas: para organizarse y esconderse de aquellos que la querían destruir. Siempre ha habido conversaciones a escondidas, desde la jerga callejera hasta publicaciones radicales como el *Berthold's Political Handkerchief*, un diario radical de 1831 impreso en Londres sobre un pañuelo de algodón para evitar los impuestos de timbre sobre el papel y permitir a aquellos que compraban la publicación sumergirla simplemente en agua si la policía llamaba.

Ante el aumento del control social, muchos activistas sostienen que estas técnicas son la mejor defensa de los opositores. «Tal y como va el mundo, los gobiernos, incluso las democracias liberales, están aumentando la vigilancia y el control sobre la población porque ya que la tecnología existe sería estúpido no hacerlo», dice Pearce. «Es posible para los activistas desaparecer en el *dark web*, pero tan pronto como se haga, pensarán que ocultan algo. Por lo tanto, siempre hay que darles algo para controlar».

Pearce sugiere el equivalente a cebos y bengalas: hacer mucho ruido y esconderse en medio de este ruido. Existe *TrackMeNot*, una extensión del navegador que hace infinidad

de consultas de búsqueda aleatorias para ocultar la actividad real del usuario en una nube de preguntas sin sentido, o *OpenStego*, un software gratuito de código abierto que puede ocultar archivos de texto, películas o sonidos codificándolos en *selfies* o pistas de música. De este modo, según Pearce, los periodistas podrían ocultar un video de fosas comunes dentro de Beethoven.

Pero la doctora Clare Birchall, autora de *Radical Secrecy*, argumenta que la naturaleza tradicional de estas técnicas, en el mejor de los casos, nos deja atrapados en un bucle continuo y, en el peor, puede resultar insuficiente en estos tiempos tumultuosos. Birchall cree que la transparencia por la que los activistas, los demócratas y los radicales lucharon en el siglo XX ha perdido su poder en el siglo XXI. «No confiamos en la revelación cuando tenemos líderes que son inmunes a la vergüenza», argumenta.

> Históricamente, la democracia ha necesitado el secretismo para organizarse y esconderse de aquellos que la querían destruir. Ante el aumento del control social, muchos activistas sostienen que estas técnicas son la mejor defensa

Que la transparencia parezca agotada como táctica política, no debe significar un retorno a las sociedades secretas de la vieja escuela creadas para debatir sobre la democracia. Sugiere que, en vez de eso, debemos experimentar con formas de opacidad y disimulo para crear espacios que nos permitan pensar en un futuro radical.

«Podrían ser espacios digitales, o podría significar un cambio en nuestra manera de pensar sobre el secretismo, pero tenemos que ir más allá del control que tanto el secretismo como la transparencia ejercen sobre la política», argumenta. «La privacidad es una idea liberal / conservadora de propiedad y derechos: retroceder de la luz del *demos* a las sombras. No fomenta la colectividad. El derecho a la opacidad es el derecho a ser ilegible. En esta ilegibilidad, nos podemos agrupar para combatir el ojo que nos vigila».

Espacios de opacidad radical

Mientras los manifestantes de todas las edades luchan contra los gobiernos, los jóvenes en particular están creando formas improvisadas de opacidad radical. En Estados Unidos, los manifestantes del movimiento *Black Lives Matter* se enfrentaron a policías equipados con falsas torres de telefonía móvil que capturaban información de los teléfonos de los manifestantes, controlaban sus correos electrónicos, páginas de Facebook y Twitter y, incluso, un software que se apodera de los teléfonos y los utiliza para espiar a sus propietarios. Para contraatacar, los jóvenes manifestantes utilizaron vídeos temporales en formato corto de aplicaciones como TikTok para organizar sus acciones. El etiquetado en vídeos que se suprimían rápidamente permitió a los activistas coordinarse para inundar las aplicaciones policiales que pedían a los ciudadanos que informaran de actividades ilegales.

En el momento más álgido de las protestas por la muerte de George Floyd, el Departamento de Policía de Dallas, por ejemplo, pidió que la gente enviara a su aplicación iWatch Dallas vídeos de Twitter con «actividades ilegales llevadas a cabo durante las protestas «. En cambio, la aplicación se inundó de videos de estrellas del pop de Corea del Sur, que bloqueaban cualquier notificación de los delitos. Finalmente, el Departamento de Policía twiteó: «Debido a dificultades técnicas, la aplicación iWatch Dallas estará inactiva temporalmente.» Mientras tanto, los rastros digitales de los vídeos habían desaparecido, por lo que ya no era posible rastrearlos. En junio, etiquetas anti *Black Lives Matter* como #WhiteLivesMatter, #WhiteoutWednesday y #BlueLivesMatter, se vincularon a muchas imágenes y actuaciones de grupos de K-pop, lo que inundó a los emisores originales de los mensajes. A finales de junio, los manifestantes utilizaron TikTok para organizar la petición masiva de cientos de miles de entradas falsas para un mitin electoral de Donald Trump en Tulsa, lo que provocó que se viera montón de asientos vacíos ante las cámaras de televisión.

Códigos, significados ocultos, correos electrónicos que desaparecen al cabo de diez minutos, etiquetas que inundan los mensajes de la derecha: es posible que las nuevas formas de organización vayan un paso por delante de los agentes estatales que son menos reactivos, pero tenemos que plantearnos lo que podrían producir los espacios radicales reseñados por Birchall de cara a futuros radicales. Yeshimabeit Milner, fundadora i directora executiva del moviment *Data for Black Lives*, argumenta que sólo tomando el control de los medios de reproducción de la tecnología (para ella, esto significa los datos y los sesgos en función de los cuales se procesan estos datos), la sociedad puede encontrar su verdadero yo en línea.

«Herramientas como la modelización estadística, la visualización de datos y el *crowd-sourcin*g, en buenas manos, son instrumentos poderosos para combatir los sesgos, construir movimientos progresistas y promover el compromiso cívico», argumenta. «Pero la historia nos revela una situación diferente en la que los datos se utilizan demasiado a menudo como instrumento de opresión, refuerzan la desigualdad y perpetúan la injusticia. El *redlining* fue una práctica basada en la selección sesgada de datos que conllevó la exclusión sistemática de las comunidades negras de los servicios financieros clave. Las tendencias más recientes, como la policía predictiva, las sentencias basadas en el riesgo y los préstamos abusivos, constituyen variaciones preocupantes del mismo tema. Hoy día, la discriminación es una empresa de alta tecnología».

Milner se radicalizó por primera vez en su instituto de Miami, que funcionaba como una prisión: los estudiantes eran enviados a casa si se olvidaban del DNI y se les podía suspender por llevar un «color de banda» si infringían las normas sobre el uniforme. Cuando los estudiantes organizaron una protesta después de que un miembro del personal casi asfixiara un estudiante, les enviaron furgonetas SWAT con agentes de policía totalmente armados. La CNN informó de un «motín en la Miami Senior High School».

Ante esta situación, Yeshimabeit Milner estaba furiosa. Se unió a un grupo local, *Power U Center for Social Change*, y empezó a elaborar su propia recogida de datos sobre el tratamiento infligido a los estudiantes negros. Hicieron una encuesta a 600 estudiantes cuyos resultados se publicaron en un cómic: *Telling It Like It Is: Miami Youth Speak Out on*

the School-to-Prison Pipeline (*Las cosas como son: la juventud de Miami habla sobre el proceso de transición de la escuela a la cárce*l).

> Jóvenes manifestantes del movimiento Black Lives Matter utilizaron vídeos cortos temporales de aplicaciones como TikTok para organizar sus acciones e inundar las aplicaciones policiales que pedían a los ciudadanos que informaran de actividades ilegales

Tras graduarse, trabajó en una campaña para recoger datos sobre la alta tasa de mortalidad infantil entre la población negra, que es el doble de la tasa para los bebés blancos, según el Departamento de Salud y Servicios Humanos. Descubrió que la lactancia materna estaba relacionada con la salud infantil y que los hospitales disuadían las madres negras de hacer lactancia materna en favor de las fórmulas infantiles que les proporcionaban los fabricantes. Gracias a sus investigaciones, el hospital despidió al jefe de su unidad de maternidad.

Pronto se dio cuenta de que este tipo de sesgo estaba en el núcleo mismo de algoritmos aparentemente neutros. En 2019, por ejemplo, se comprobó que un algoritmo ampliamente utilizado en los hospitales de Estados Unidos para asignar asistencia sanitaria a los pacientes había discriminado sistemáticamente la gente negra. Una investigación publicada en la revista *Science* demostró que el algoritmo, cuando detectaba pacientes con el mismo grado de gravedad, tenía menos probabilidades de derivar los pacientes negros hacia programas de mejora de la atención a pacientes con necesidades médicas complejas.

Cambiar los algoritmos

Pero, ¿qué podemos hacer para cambiar los algoritmos? Primero, tomando conciencia de que sólo es una receta: una lista de instrucciones para elaborar un plato que puede ser saludable o poco saludable, sabroso o insípido según los ingredientes, o los datos, que decidimos incluir. Del mismo modo que no dejaríamos que el estado eligiera nuestros ingredientes, también deberíamos controlar nuestros datos para poder cambiar poco a poco el resultado final.

«El uso de los datos como arma no se puede cambiar sólo con un cambio de política», argumenta. «No se trata de una llamada para acabar con todos los datos, al igual que la llamada a abolir las cárceles no es una llamada a no asumir la rendición de cuentas, sino a poner fin a un sistema punitivo violento que no funciona. Es una nueva manera de entender el mundo que comienza en nuestras mentes, organizaciones e instituciones académicas. Se trata de construir coaliciones, desarrollar más habilidades y más empatía. Tenemos la oportunidad de abolir, de volver a imaginar y recrear nuevas estructuras de producción de conocimiento, nuevas formas de toma de decisiones y nuevas maneras de relacionarnos. Las posibilidades para el futuro son infinitas».



Stephen Armstrong

Stephen Armstrong es periodista freelance y escritor. Habitualmente, escribe para el Sunday Times, Wired, Daily Telegraph y The Guardian, entre otros medios. Es autor de cinco libros de no ficción: *The White Island* (2004), *War plc*: *The Rise of the New Corporate Mercenary* (2008), *The Super Rich Shall Inherit the Earth* (2010), *The Road to Wigan Pier Revisited* (2012) y *The New Poverty* (2017). Fundó los encuentros Wigan Pier Workshops en colaboración con el English PEN, la organización Interncional de escritores a favor de los derechos humanos, y es miembro del Orwell Youth Prize y de la RSA.