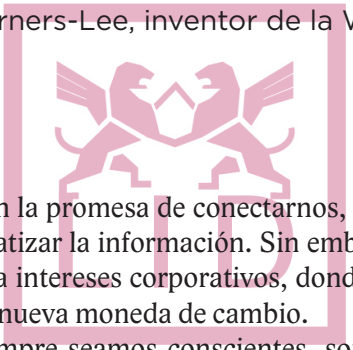
Índice

Introducción

«La web ha evolucionado hasta convertirse en un motor de inequidad y división; influida por fuerzas poderosas que la utilizan para sus propias agendas».

Tim Berners-Lee, inventor de la World Wide Web



Internet se creó con la promesa de conectarnos, de acercar el conocimiento y democratizar la información. Sin embargo, hoy tenemos una red vinculada a intereses corporativos, donde nuestra información personal es la nueva moneda de cambio.

Aunque no siempre seamos conscientes, somos objeto de una clara transacción; pagamos por servicios aparentemente gratuitos con nuestros datos y cedemos no solo nuestra identidad, sino también nuestra libertad.

Desde mi primer contacto con Bitcoin en 2012, cuando lideraba Tyba, mi primera *startup*, siempre he estado vinculado con la tecnología blockchain.

En 2012 empecé a invertir en criptoactivos, comencé por bitcoin, que era el único que existía en aquel entonces. Tres años después, en 2015, tras vender Tyba, ya daba mis primeros pasos sólidos en el campo de la inteligencia artificial con source{d}. En 2017 monté MAD Lions, ahora Movistar KOI, uno de los mayores clubes de esports del mundo, el cual fusionamos con Overactive Media y sacamos a bolsa en Toronto en el año 2021. Todo este contacto con la tecnología, las *startups* y la innovación digital me llevó, en 2021, a fundar Keyrock

Asset & Wealth Management, antes conocida como Turing Capital, una gestora de activos y patrimonios en criptoactivos, de la que actualmente soy CEO. Siempre he compaginado mi actividad profesional con la docencia, como profesor de innovación y emprendimiento en IE Business School, además de mi actividad en diversos consejos de administración de empresas del sector de los criptoactivos.

Este libro engloba en gran medida todo lo que he aprendido a lo largo de mi trayectoria profesional y parte de una profunda preocupación por la evolución que he visto en Internet, pero también de una firme convicción: podemos cambiar el rumbo y recuperar el poder sobre nuestros datos. Podemos dejar de ser un producto y recuperar nuestra identidad digital, apostando por un internet más justo y libre.

Hacia un internet más libre propone una mirada crítica al presente digital y una apertura hacia lo que está emergiendo: un nuevo internet basado en tecnología blockchain que nos dará herramientas para restaurar nuestro poder digital.

Nos encontramos en un auténtico punto de inflexión. Tenemos la oportunidad de transformar internet y ser partícipes de la creación de una red más justa y abierta, más democrática y menos totalitaria, más resiliente y segura, una red donde el poder no se concentre en las manos de unos pocos, sino que se distribuya de forma equitativa entre todos los usuarios.

Aún queda mucho por hacer y los avances son inabarcables. Sabemos que el progreso no está exento de desafíos y complicaciones, pero la tecnología siempre debe ser la solución y no el problema.

A lo largo de los próximos capítulos, me adentraré en el mundo de la web 3.0, desde sus inicios hasta lo que podría llegar a ser, y explicaré por qué gracias a la tecnología blockchain seremos capaces de recuperar nuestra soberanía individual sin quedar bajo el yugo de las grandes corporaciones que utilizan nuestra información para su propio beneficio.

A continuación, haré un sucinto resumen del recorrido que propongo en el libro a través de cada uno de los bloques que lo componen.

La historia que precede a la tecnología blockchain

En primer lugar, para entender cómo hemos llegado hasta el lugar en el que nos encontramos ahora —y que nos permitirá comprender lo que está por venir—, haré un breve repaso de la historia de internet

desde sus inicios hasta su transformación en la herramienta interactiva que conocemos.

Recorreré los años del auge de las redes sociales y mostraré cómo simples herramientas que buscaban conectar a las personas se convirtieron en poderosos intermediarios capaces de moldear opiniones, tendencias y, a escala global, comportamientos.

Abordaré la censura invisible, algoritmos opacos y directrices de moderación que permiten a las plataformas ejercer un control significativo sobre lo que vemos y lo que no vemos.

Finalmente, hablaré de cómo internet está gobernada por estados corporativos, detrás de los cuales se encuentran las grandes empresas tecnológicas del mundo, que influyen en aspectos esenciales de nuestras vidas, desde el acceso a la información hasta la libertad de expresión.

Las redes blockchain

En el segundo bloque, compartiré los secretos de la tecnología blockchain, qué es y cómo está cambiando no solo la economía o la forma en la que realizamos transacciones, sino también la manera en la que interactuamos y cómo podemos construir un internet más transparente y descentralizado.

Mostraré qué hay más allá de las criptodivisas, el funcionamiento de las redes blockchain y las nuevas tecnologías asociadas, los contratos inteligentes y las aplicaciones descentralizadas. Explicaré cómo trabajaban los nodos de las redes y la seguridad criptográfica que protege los datos y asegura la integridad de cada transacción de información.

Un cambio de paradigma

En el tercer bloque profundizaré en cómo la tecnología blockchain transformará radicalmente las redes sociales, la inteligencia artificial y la identidad digital tal y como las conocemos hoy, el proceso de transición entre la web 2.0 y la siguiente etapa, la web 3.0, un entorno mucho más transparente y justo sin intermediarios.

Desentrañaré mitos y realidades en torno a esta tecnología y abordaré los malentendidos que, a pesar de su potencial, existen. Son muchos los que asocian la tecnología blockchain con la volatilidad

de algunos criptoactivos sin conocer las diversas aplicaciones ni los potenciales beneficios. La blockchain sirve para mucho más que para la creación de monedas digitales.

Aplicaciones reales de la tecnología blockchain

Finalmente, en el último bloque explicaré cómo esta tecnología está destinada a revolucionar el entorno digital a lo largo de las próximas décadas. Analizaré su potencial transformador sobre múltiples industrias y su capacidad de establecer nuevas dinámicas de transparencia y confianza.

Por último, ahondaré en los conceptos de identidad y privacidad en el entorno blockchain, y analizaré cómo la identidad digital europea es un claro ejemplo de las posibilidades de la web 3.0. Poco a poco, los ciudadanos utilizaremos más y más aplicaciones y plataformas basadas en blockchain para acceder a servicios, realizar transacciones y autentificar nuestra identidad.

Durante todos estos años, he podido relacionarme con ingenieros visionarios y emprendedores con una valentía sin igual, con programadores y desarrolladores que vuelcan su conocimiento para desarrollar una internet más libre y transparente. Al igual que yo, ellos buscan crear un ecosistema digital mejor para nuestros hijos y nietos. Esa es, en esencia, mi principal motivación, como también lo es para sentarme ante las páginas en blanco y compartir hacia dónde vamos y cómo las personas pueden formar parte de la revolución que supone la siguiente etapa de internet.

La web 3.0 es el futuro y nos traerá la verdadera libertad, pues permitirá entender, no solo que nuestros datos y la información relevante sobre nosotros nos pertenece, sino que hay un camino para tener el control sobre ellos.

«El espíritu original era muy descentralizado.
El individuo estaba increíblemente empoderado.
Todo se basaba en que no había una autoridad central
a la que tuvieras que pedir permiso. Esa sensación
de control individual, ese empoderamiento,
es algo que hemos perdido».

Tim Berners-Lee, inventor de la World Wide Web

JORGE SCHNURA

HACIA UN INTERNET MÁS LIBRE

CÓMO EL BLOCKCHAIN PUEDE DEVOLVERNOS EL CONTROL SOBRE NUESTRAS VIDAS

1
El nacimiento de la red y la promesa incumplida

«Internet es para todos, pero no lo será a menos que hagamos que lo sea».

Vint Cerf, creador del protocolo TCP/IP, el Padre de Internet

A mediados de marzo de 2018, a través de varios reportajes en dos prominentes medios de comunicación, los periódicos *The Guardian* y *The New York Times*, se dio a conocer, gracias a las revelaciones de un exempleado, que Cambridge Analytica había utilizado datos recopilados en la red social Facebook para crear perfiles psicológicos y dirigir campañas políticas altamente segmentadas. Fue un escándalo mayúsculo, un incidente que evidenció las carencias en la privacidad de los datos y la utilización de información privada para manipulación política.

Se llegaron a compartir de manera ilegal y sin consentimiento los datos de más de 87 millones de usuarios. 87 millones. Casi el doble del número de habitantes de España entera.

Ocurrió en 2014, un año después de la fundación de Cambridge Analytica, una empresa británica que tenía como propósitos el análisis de datos y la comunicación estratégica en campañas electorales, la consultoría política.

Ese año, un profesor de la Universidad de Cambridge desarrolló una aplicación que se presentó como una herramienta de investigación psicológica. La aplicación, integrada en Facebook, se anunciaba como una prueba de personalidad, un test, y fue instalada por unas trescientas mil personas. Sin embargo, debido a las políticas de Facebook, la aplicación no solo recolectaba datos de los usuarios que la habían instalado, sino también de sus amigos y contactos en Facebook. Así, aproximadamente, la aplicación terminó acumulando información de casi noventa millones de usuarios sin su consentimiento explícito.

Los datos recolectados por esa aplicación se vendieron a Cambridge Analytica, que se sirvió de ellos para crear perfiles psicológicos detallados de los votantes. Dichos perfiles luego fueron utilizados para dirigir propaganda política personalizada y muy segmentada durante distintas campañas electorales, como es el caso de la campaña presidencial de Donald Trump en 2016 o la campaña a favor del Brexit en Reino Unido. Sin ninguna contemplación, la empresa empleó todos los datos obtenidos para influir en los votantes mediante anuncios personalizados y estrategias de comunicación diseñadas que manipulaban sus opiniones y su comportamiento.

Todo esto se hizo público gracias a la intervención de Christopher Wylie, exdirector de investigación de la empresa británica. En sendas entrevistas y declaraciones, detalló cómo la empresa había recolectado datos de manera inapropiada y los había utilizado con la intención de manipular a los votantes.

La revelación pública en los citados periódicos provocó una reacción a escala global. De inmediato, políticos, reguladores y el público en general comenzaron a exigir respuestas y responsabilidades. El CEO de Facebook, Mark Zuckerberg, fue citado a testificar ante el Congreso de los Estados Unidos y el Parlamento Europeo en relación con el uso de datos y las prácticas de privacidad de su red social. Y Cambridge Analytica perdió todos sus clientes hasta declararse en bancarrota y dar cierre a sus operaciones en 2018. Por su parte, a Facebook se le impuso una multa de récord. La Comisión Federal de Comercio de Estados Unidos impuso a Facebook una multa de cinco mil millones de dólares en 2019.

Este escándalo marcó un punto de inflexión en los debates sobre la privacidad de los datos personales y la ética en el uso de la información asociada a las personas en esta era. A partir de su revelación, hubo un cambio significativo en la conciencia pública sobre la privacidad, quedó subrayada la vulnerabilidad de la información personal en las redes sociales y cómo esta puede ser explotada para manipularnos.

Cada vez, con mayor intensidad, se demanda más protección y nuevas normativas. En estos últimos años, la sociedad está cobrando conciencia de la importancia de la privacidad digital, de la privacidad de nuestros yoes digitales.

Y no es la primera vez que en la red se desata el caos ligado a uno de los gigantes tecnológicos.

A finales de 2014, el medio *BuzzFeed News* publicó un artículo en el que revelaba cómo un ejecutivo de la empresa Uber había accedido a los datos de viaje de una periodista sin su consentimiento a través de una herramienta interna conocida como God View —de manera paradójica, el nombre de esta herramienta se traduce como 'vista de Dios', en relación con la perspectiva adoptada al usarla y ejemplarizando cómo se perciben las grandes empresas de este tipo—. Esta herramienta permitía a los empleados de Uber rastrear la ubicación de cualquier usuario en tiempo real, detallando puntos de recogida y de destino de los viajes.

Se expuso que el acceso a esta herramienta no estaba ni por asomo suficientemente controlado ni supervisado, y que se estaba utilizando para espiar a celebridades, políticos y otras figuras prominentes, no solo a periodistas.

En un primer momento, Uber negó las acusaciones, pero cuando todo se hizo público y mediaron organismos reguladores para examinar las prácticas de privacidad y seguridad, la empresa se vio obligada a someterse a auditorías y a implementar un programa de privacidad integral. Además, el entonces CEO y cofundador, Travis Kalanick, abandonó la empresa.

Este fue uno de los primeros escándalos en relación con la privacidad de los datos en la era digital. No el único, por desgracia.

En julio de 2019, el periódico *The Guardian* publicó un artículo sobre cómo trabajadores externos de Apple escuchaban de manera regular grabaciones de audio capturadas por el asistente virtual Siri. Estas incluían conversaciones privadas y detalles confidenciales de

los usuarios, como información médica, especificaciones financieras e incluso situaciones íntimas.

Según Apple, solo se escuchaba una pequeña fracción de las grabaciones de su asistente, y se hacía a modo de análisis para mejorar la precisión del asistente virtual. No obstante, se reveló que muchas de las grabaciones escuchadas y analizadas eran fruto de una activación accidental, sin que el usuario realmente lo supiera.

A raíz de este escándalo y de los graves problemas asociados a la privacidad, Apple suspendió temporalmente el programa de análisis de Siri y anunció que haría cambios y que los usuarios tendrían la opción de no participar en las grabaciones de audio si no lo deseaban.

Este incidente acrecentó la preocupación sobre la privacidad de los datos de los usuarios. Y no hablamos de cualquier empresa, sino de una que utiliza la seguridad y la privacidad por bandera. ¿Hasta qué punto debemos confiar en la publicidad que las empresas hacen de sí mismas o en la manera en la que intentan hacernos ver que operan? No queda otra, en cualquier caso. Las tecnologías de estas grandes tecnológicas exigen confianza por parte del usuario, al contrario de lo que sucede en la web 3.0, pues la propia tecnología blockchain suprime esa necesidad al ser *trustless,* es decir, no requiere esa confianza del usuario para operar de manera segura. Con la web 3.0 no es preciso depositar la confianza en ningún intermediario ni autoridad central para que todo funcione de manera correcta y segura.

De nuevo, salió a la luz la falta de transparencia por parte de las grandes tecnológicas en cuanto a la gestión de datos. En enero de 2020, poco antes de que se desatara la pandemia del covid-19, el periódico *The New York Times* publicó un artículo en el que quedaba expuesto cómo Clearview AI había creado una herramienta de reconocimiento facial sirviéndose de miles de millones de fotos obtenidas en páginas web y redes sociales sin el consentimiento explícito de los usuarios.

Partiendo de plataformas como Facebook e Instagram, Clearview AI recolectó más de tres mil millones de imágenes de personas para dar forma a una herramienta que luego utilizarían cientos de agencias policiales de diversos países para identificar sospechosos de delitos y resolver casos.

Obviamente, la capacidad para identificar personas a partir de fotos en la red generó grandes preocupaciones en torno a la

privacidad, el consentimiento y el potencial abuso de la tecnología. Hubo una ola de críticas y se presentaron múltiples demandas, que derivaron en discusiones sobre la necesidad de regulaciones más estrictas en cuanto al uso de tecnologías de reconocimiento facial e inteligencia artificial.

Este caso en particular suscita preguntas cruciales sobre consentimiento de uso, privacidad y control sobre la información personal.

En 2021 los servicios de Facebook, Instagram y WhatsApp —todos ellos englobados bajo el paraguas de Meta— sufrieron una interrupción de bastantes horas a causa de cambios en la configuración de los servidores que coordinaban el tráfico de la red entre los centros de datos de la gran tecnológica. Este incidente afectó a miles de millones de usuarios en todo el mundo y tuvo un impacto más que significativo en multitud de empresas que hoy en día dependen de estas plataformas para operar sus negocios y comunicarse con sus clientes. Aunque breve, resaltó la dependencia global para los negocios y la comunicación de unas pocas plataformas centralizadas.

A finales de 2022, se divulgó una serie de documentos que revelaban directrices internas de Twitter —ahora X—. En ellos se exponían pautas de moderación de contenido y la influencia gubernamental que se había ejercido sobre ellas. Quedó expuesto cómo en red social gestionaba el contenido mediante la censura de muchos temas y la influencia de terceros en cuanto a la restricción de información.

Fueron los periodistas Matt Taibbi y Bari Weiss quienes sacaron a la luz los pormenores después de tener acceso a documentos internos de la empresa, gracias a los cuales también detallaron casos específicos. Se hizo público que agencias gubernamentales, como el FBI y otras organizaciones de seguridad, estaban en contacto con, por aquel entonces, Twitter para sugerir y solicitar la moderación de determinados contenidos, fundamentalmente ligados con campañas electorales. Se reveló que, en algunos casos, estas agencias sugirieron que ciertos usuarios o publicaciones se eliminasen o censuraran, en especial en asuntos relacionados con seguridad nacional o con figuras relevantes. Uno de los aspectos más polémicos fue la censura de un artículo del *New York Post* en octubre de 2020 sobre el portátil de Hunter Biden, el hijo del entonces presidente, Joe Biden. Twitter llegó a bloquear temporalmente los enlaces al artículo, alegando preocupaciones sobre la posible desinformación. En los documentos publicados se demostraba que esta decisión se había tomado

de manera interna con cierta controversia, y quedó patente que la plataforma había actuado bajo presión política.

También se expuso cómo Twitter gestionaba las cuentas de políticos y figuras públicas, muchas veces suspendía su uso y suprimía contenido, y cómo censuraban y acotaban la difusión de ciertas publicaciones de medios de mucho renombre, como el caso del *New York Post*. Fueron muchas las figuras públicas de relevancia, incluidos científicos y periodistas, que sufrieron *shadow banning*, la limitación del alcance de sus publicaciones sin ser notificados.

Este caso recibió el nombre de Twitter Files, y ha sido el detonante de un extenso debate sobre la libertad de expresión, la censura en redes sociales y el papel de los gigantes tecnológicos en el discurso público.

A partir del escándalo de Twitter, todos hemos sido testigos de la relación que existe a puerta cerrada y en las sombras entre los gobiernos y las grandes empresas tecnológicas.

En relación con esta cuestión, otro caso que ha estado en el ojo público es la censura de contenidos sobre el covid-19 en Facebook. Mark Zuckerberg, CEO y fundador de Meta, denunció haber recibido presiones por parte de la Administración del Gobierno de Joe Biden para que se censurasen contenidos relacionados con el covid-19 en el año 2021. Lo hizo a través de una carta dirigida al Comité Judicial de la Cámara de los Representantes de Estados Unidos en la que hablaba de tales prácticas y de cómo en Facebook habían eliminado contenido. «En 2021, funcionarios de alto nivel de la Administración Biden, la Casa Blanca incluida, presionaron durante meses y repetidamente a nuestros equipos para censurar cierto contenido sobre el covid-19, incluyendo piezas sátiras y humorísticas, y también expresaron una gran frustración cuando alegábamos que no estábamos de acuerdo». Este es un extracto de la carta mencionada, en la que Zuckerberg admitió que sucumbieron a la presión y que ejercieron una censura activa. Y no solo con el covid-19, también con otros asuntos, como toda la información pública sobre los delitos del hijo del expresidente Joe Biden.

En mayo de 2023, la FTC —la Comisión Federal de Comercio— de Estados Unidos hizo públicas las prácticas indebidas por parte Amazon Ring, una empresa de cámaras de seguridad inteligentes, propiedad de Amazon. Según se relataba en el informe, trabajadores de esta empresa espiaban ilegalmente a los clientes y hubo una gran brecha de seguridad que permitió a piratas informáticos hacerse con el control de las cámaras y espiar también a los usuarios.

Tal como detallaba la FTC, diversos empleados accedían de forma inapropiada a las cámaras que activaban —sin el consentimiento de los clientes— para visualizar y compartir imágenes. Al mismo tiempo, dadas las escasas medidas de seguridad implementadas, piratas informáticos de distintas partes del mundo pudieron acceder a las cámaras y hacerse con información personal.

Fue un escándalo de proporciones bastante serias que evidenció la falta de regulación sobre dispositivos conectados al internet de las cosas, sobre la monitorización y las grabaciones en los hogares de los consumidores.

Nuevamente asistimos a la exposición de los riesgos y las responsabilidades de las grandes empresas y su gestión y control de los datos.

Cada día, avanzamos hacia una sociedad más interconectada y en la que internet se ha convertido en una necesidad esencial para la economía global, para la comunicación y, en general, para la vida cotidiana. Sin embargo, eventos como el de CrowdStrike revelan la vulnerabilidad sobre la que está construida la estructura.

En la madrugada del 19 de julio de 2024, una malograda actualización de un antivirus tumbó Windows, el sistema operativo de Microsoft. Windows es uno de los sistemas operativos más utilizados en el mundo, y durante esa madrugada ordenadores de todo el globo quedaron fuera de juego. La vorágine comenzó con una actualización de Falcon, un programa de ciberseguridad de la empresa estadounidense CrowdStrike —que luego daría nombre al evento global— que utilizaban muchas empresas, sistemas estatales y grandes corporaciones. Una incompatibilidad del *software* provocó que Windows se bloqueara en miles y miles de ordenadores. Los terminales entraban en un bucle de reinicio que impedía acceder, bloqueando de esta manera la herramienta con las que muchos trabajan y prestan servicios.

Este suceso puso de manifiesto la dependencia que tenemos de las grandes empresas tecnológicas, lo que implica la centralización del poder que ejercen. Pero insisto, ha habido muchos otros casos que han expuesto problemas muy serios.

Hoy, pese a que percibimos internet como una red infinita y abierta, son unas pocas empresas las que dominan la casi totalidad del tráfico y de los servicios.

Los gigantes tecnológicos se han hecho con el control progresivamente, y ahora, mediante complejos algoritmos, son capaces

hasta de determinar lo que vemos y consumimos, incluso de condicionar lo que pensamos, nuestra perspectiva. Y aunque indudablemente aportan un gran valor, los servicios de estas empresas traen consigo muchos aspectos negativos.

A través de sus diferentes plataformas, y gracias a la enorme cantidad de datos de uso que recopilan con las interacciones, Alphabet —la empresa matriz de Google— y Meta —la empresa matriz de Facebook— son capaces de ofrecer publicidad altamente dirigida y contenido personalizado que, sin que el usuario lo advierta, insta a mantener la atención. Mediante el uso de sistemas de seguimiento de uso muy avanzados, estas empresas monitorizan cada búsqueda, cada clic, cada interacción social. Todo bajo el amparo de complicadas y enrevesadas políticas de privacidad, acuerdos que los usuarios aceptan, pero que nadie realmente lee.

En la sombra. El 8 de agosto de 2024, el periódico *The Financial Times* publicó un artículo explicando cómo Alphabet y Meta habían firmado un acuerdo secreto para dirigir publicidad a jóvenes adolescentes de entre 13 y 17 años en YouTube, que sorteaba las propias normas de la empresa en cuanto a la relación con menores de 18 años.

No es la primera vez que Meta se ve involucrada en controversias por su política sobre menores. Solo en Estados Unidos, el gigante tecnológico dueño de Meta ha sido demandado por más de treinta estados por «prácticas manipuladoras» hacia los usuarios más jóvenes.

La manera en la que interactuamos con el contenido de estas plataformas es el alimento de los algoritmos que después nos muestran aquello que nos mantendrá conectados e interactuando —lo que, en resumidas cuentas, permite ganar más dinero a la empresa que gestiona la plataforma—. Los «me gusta», las reacciones, los comentarios y las publicaciones, el tiempo de visualización, lo que compartimos, las búsquedas... Todos esos parámetros son registrados y analizados para luego ponernos delante no solo lo que nos enganchará sino, también, lo que va a hacer que votemos en un sentido u otro, lo que va a hacer que compremos tal o cual producto. Y es un círculo que no tiene fin, pues como el contenido se adapta a los intereses del usuario, la satisfacción de este —y la adicción— aumenta.

Controlan lo que vemos, y se basan en el rendimiento económico que pueden obtener de nuestra atención. Se nos vende como

una forma de personalización, pero no deja de ser una maniobra de control. De hecho, sus algoritmos son capaces de alterar la vida o la marcha de un negocio, hasta de influir en elecciones. El gravísimo escándalo de Cambridge Analytica, la evidencia del uso indebido de información de 87 millones de usuarios, es solo una muestra.

La sociedad ha de cuestionarse el uso de datos sin consentimiento y los graves ataques a la privacidad de forma seria. Y no solo eso, también la manera en la que se nos dirige. Ha de cuestionarse si este es el internet que queremos. Debemos reflexionar qué queremos de la red en el futuro.

En las redes sociales existe un tipo de censura de la que apenas se habla, una suerte de censura invisible mediante la que se condiciona el contenido y la información que llega o no llega a los *feeds* de los usuarios. Sin que nos demos cuenta, se manipula y controla el contenido que publicamos y sobre el que discutimos, se acallan voces y se invisibilizan opiniones. Esta práctica comenzó con la intención de filtrar el contenido dañino o malicioso, pero hoy los algoritmos van mucho más allá.

En líneas generales, no somos conscientes de la cantidad de datos que se recopilan sobre nosotros. Miles y miles de datos de cada usuario. Y todos estos datos no son simples datos, sino que son lo que conforma nuestro yo digital, las versiones de nosotros mismos que existen en la red.

Estamos en manos de gigantes.

Amazon, la plataforma de comercio electrónico más grande del mundo, acapara gran parte de las ventas en la red, y sus servicios se extienden mucho más allá de la compraventa de productos propios, pues, además, permite a compradores externos vender sus productos. Y su servicio en la nube —Amazon Web Services, AWS— es el proveedor de infraestructura de nube más grande del planeta, que da cabida a muchas aplicaciones y páginas web. Amazon también hace uso de una enorme cantidad de datos recopilada a partir de las interacciones de los usuarios. Páginas y productos visitados, tiempo de permanencia en las páginas de los diferentes artículos, interacciones, historial de compra, frecuencia de compra, productos guardados en listas de deseos, productos añadidos al correo, pero no comprados, patrones de búsqueda...

Microsoft, conocido fundamentalmente por su sistema operativo, también compite por el espacio de infraestructura en la nube con

Microsoft Azure, pero, además, tiene un control considerable sobre el *software*, que incluye en la manera en la que los usuarios acceden y utilizan internet. Hoy, Microsoft 365 —que incluye Word, Excel, PowerPoint y otros programas— es la herramienta de trabajo estándar para una amplia mayoría de empresas y de usuarios. La gran empresa tecnológica lleva varias décadas enfrentándose a demandas de monopolio y luchando contra acusaciones de prácticas desleales y anticompetitivas.

Apple domina el mercado de la venta de dispositivos móviles. Más de doscientos millones de personas compran sus dispositivos cada año y están pendientes de cualquier novedad anunciada por la compañía. Durante muchos años, multitud de empresas han seguido la estela de Apple en cuanto a diseño e innovación. Además, la gran tecnológica también es conocida por sus servicios en la nube y por su sistema operativo: iOS.

Por otro lado, Alphabet, con su sistema operativo para móviles, Android, acapara casi la totalidad del mercado. Más del 70 % de los dispositivos móviles en el mundo utilizan Android.

El uso de Android e iOS sumado da como resultado casi el cómputo global de uso en el mercado digital.

Fuera de China, el 95 % del mercado de las aplicaciones digitales está controlado por Apple y Alphabet. Y no es un dato que deba despreciarse. De media, pasamos unas siete horas al día utilizando dispositivos conectados a internet, principalmente teléfonos móviles. Y la mitad de ese tiempo se emplea en aplicaciones. Hablamos de que pasamos casi la mitad de nuestro día despierto dentro de un entorno controlado por dos grandes empresas. Si dormimos 8 horas y estamos despiertos 16 horas, la mitad de ese tiempo transcurre en los estados digitales creados por Alphabet, Microsoft, Apple, Meta... Y esto no solo nos afecta a nosotros como usuarios, sino también a los desarrolladores a nivel creativo, pues deben seguir las directrices de estas dos empresas si quieren optar al mercado y a que su producto llegue al usuario.

El control sobre la distribución de aplicaciones en sus tiendas digitales es férreo, está muy marcado por políticas muy estrictas. Además de cobrar comisiones del 30 % sobre las compras dentro de las aplicaciones —lo cual se conoce vulgarmente entre los desarrolladores como «tarifa de monopolio»—, plantean políticas de revisión para operar que han sido vistas como anticompetitivas

por muchos desarrolladores y reguladores. Apple, por ejemplo, se ha visto varias veces frente a los tribunales. Quizás el caso más sonado sea el de Epic Games, una desarrolladora de videojuegos que demandó a Apple por las prácticas de la compañía después de negarles el acceso a la App Store, la tienda digital de aplicaciones de Apple.

Son Alphabet y Apple quienes determinan las aplicaciones que están disponibles en sus tiendas y, por ende, los servicios y los contenidos accesibles para los usuarios. Y ellos deciden cuáles son las aplicaciones recomendadas en las páginas de inicio y en los resultados de las búsquedas. En cierto sentido, hablamos de otro tipo de censura y de un ejercicio práctico de poder.

Una prueba evidente de que las grandes compañías tecnológicas gobiernan la red es la manera en la que asfixian a la posible competencia. Algunos ejemplos. A comienzos de la segunda década de este siglo, Facebook y Twitter realizaron cambios drásticos en sus políticas internas que afectaron con severidad a los desarrolladores que habían construido sus negocios sobre estas redes sociales, sobre la API que permitía acceder a las redes y ejecutar acciones en ellas. Una API, por explicarlo de manera sencilla, es un conjunto de herramientas y protocolos que permite a distintas aplicaciones comunicarse entre sí y acceder a ciertas funcionalidades. Las restricciones se extendieron durante varios años, desde 2012 en el caso de X y desde 2014 en el caso de Facebook, hasta entrado el año 2018, cuando cerraron el acceso a la API. Poco a poco, redujeron el espacio de aquello que no les pertenecía como tal, pero operaba dentro de su red. El caso más notable es el de los juegos en línea integrados en Facebook. Estos crecieron sirviéndose de las herramientas de la red de Meta para llegar a más usuarios, de las conexiones entre amigos y de las notificaciones. Sin embargo, a partir de los cambios introducidos con las nuevas políticas, Facebook suprimió sus posibilidades de crecimiento, eliminando las notificaciones de juegos ajenos o las notificaciones a amigos. No mucho más tarde, desarrollaron su propia plataforma de juegos en línea dentro de la red social. Esas políticas acabaron con muchas empresas, aunque no fue en vano. Hoy, cualquier desarrollador es consciente de lo poco fiable que es construir sobre los cimientos de cualquier red social.

Los gigantes tecnológicos son claramente anticompetitivos y trascienden más allá de las redes sociales.

Amazon, a partir de los datos recopilados de las interacciones de sus usuarios, toma como referencia los productos de terceros más vendidos para luego reproducirlos con una versión más barata. Y sus productos siempre aparecen frente a los usuarios antes que otros. Hay quien podría pensar que esta es una estrategia legítima, pero la cuestión es que Amazon no es solo una tienda compitiendo, además es la infraestructura en la que las otras tiendan proveen de productos y servicios.

Alphabet y Apple también posicionan sus productos por encima de los de los competidores en sus propias redes y buscadores. Legítimo, quizás, pero al igual que ocurre con Amazon, no solo son empresas compitiendo con otras, sino que son la propia infraestructura de las redes. Y ya he mencionado las prácticas sobre el control de acceso y distribución de aplicaciones en las tiendas digitales.

Privacidad, seguridad, libertad, censura... El monopolio de estas grandes empresas tecnológicas sobre internet tiene profundas implicaciones. Sus servicios y plataformas han evolucionado hasta convertirse en auténticos estados corporativos, *corporate states*. Es en estos nuevos estados en los que pasamos buena parte del día. Y lo hacemos bajo directrices y pautas de gobierno que se asemejan más a regímenes totalitarios que a sistemas democráticos, donde la libertad no es sino una mera ilusión.

Pero esto no siempre fue así. Internet se concibió como un proyecto de red descentralizada y colaborativa a través de la que podía accederse de manera ilimitada al conocimiento. En sus comienzos, en la mente de todos los grandes genios involucrados, se vislumbraba como un espacio abierto y libre, donde cualquier individuo —usuarios, artistas, desarrolladores, investigadores...— podía conectarse y consultar información.

La cultura de la colaboración y la idea de comunidad, el intercambio libre, eran pilares fundamentales de su fundación que fueron desarrollándose. Internet se diseñó para ser un lugar plural y abierto, donde nadie tendría privilegios sobre otros y no se tuviera control sobre la creatividad ajena.

Nadie imaginó que, apenas unas décadas después, la red estaría bajo el control de unas pocas empresas, que pasaría de ser una red en la que no se precisaba permiso para acceder y de la que nadie podía echarte a ser una red donde los intermediarios determinarían quién podía y quién no podía estar o a qué podía o no accederse.

Hoy, la capitalización del Nasdaq, uno de los principales mercados de valores en el mundo, está copada por los grandes gigantes tecnológicos. En torno al 50 % del valor total se encuentra en un puñado de empresas: Microsoft, Apple, Nvidia, Alphabet —Google y también YouTube—, Meta —Facebook, Instagram y WhatsApp— y Amazon.

Nadie lo preveía, sin embargo, debo decir que esto no ha sucedido de la noche a la mañana. Más bien ha ocurrido de manera orgánica. A medida que avanzaba la tecnología, esta iba adaptándose a las necesidades y pretensiones de la propia sociedad, que pronto descubrió lo mucho que gustaba de las facilidades y de lo positivo de las redes. A cambio de «nada» —lo pongo entre comillas, pues a lo largo del libro explicaré que lo que en apariencia es gratis no lo es en realidad—, se nos ofreció la posibilidad de conectar aún más con nuestros seres queridos, de compartir momentos sin estar presentes o de conocer el trabajo de personas que de otro modo jamás hubiésemos conocido. Pero había un coste. Y aunque en sus comienzos no había ninguna malicia detrás del desarrollo de las redes sociales, algo que creo sinceramente; en un punto indeterminado, las grandes empresas se vieron en la necesidad de competir y preservar los intereses de sus accionistas. A partir de entonces, pasamos de ser usuarios a ser el producto, el sustrato de las compañías tecnológicas para obtener más rentabilidad, más ganancias.

Es difícil establecer cuándo con precisión, aunque podemos enmarcar la curva de crecimiento de las grandes empresas tecnológicas a mediados de la primera década del siglo XXI, el período de transición de las primeras redes abiertas, el internet primitivo y los correos electrónicos, a las redes sociales. La transición de la web 1.0 a la web 2.0.

Las redes sociales han dado forma al mundo en el que vivimos. Antes de su existencia, lo que reinaba en internet eran los correos electrónicos y las páginas estáticas. A partir de la llegada de la WWW (World Wide Web) y de su posterior desarrollo, plasmado en las bases de datos centralizadas y la computación en la nube, comenzaron a surgir los foros de discusión y distintas tecnologías que promovían la interacción instantánea y las publicaciones en tiempo real. Y todo cambió. De pronto, las personas pudieron conectar con amigos y familiares en cualquier parte del mundo de manera inmediata, y se hizo mucho más fácil conectar con individuos ajenos

al círculo próximo, lo que derivó en la creación de comunidades y grupos sociales. También se nos ofreció la posibilidad de compartir nuestras opiniones e ideas ante una audiencia global, lo que, de otro modo, nunca podría llegar a ser posible.

Lo positivo que trajeron consigo las nuevas capacidades de las tecnologías, lo que originó el paso a la web 2.0, es incuestionable. Nadie lo pone en duda. Pero qué precio hemos tenido que pagar —y aún hoy en día pagamos—. Lo que en principio pretendía ser una red abierta y libre, paulatinamente pasó a ser una red gobernada por las empresas que controlan los pocos ecosistemas digitales centralizados en los que todos nos movemos, esos *corporate states* a los que me he referido.

A cambio de hacer uso de los servicios que nos ofrecían, nos han transformado en un producto del que obtener ganancias.

Hoy en día, el beneficio combinado de las cinco redes sociales más grandes es exorbitante. La cifra quita el aliento: docientos veintidós mil millones de euros, según datos de 2023. Y, en gran medida, a costa de los usuarios y de lo que los usuarios llevan a cabo dentro de cada plataforma.

Las redes sociales se han convertido en la herramienta más importante para el marketing y la publicidad. Gracias a los datos recogidos, a las empresas que invierten parte de su capital dentro de estos ecosistemas digitales se les permite llegar a audiencias específicas con sus campañas. Y ahí es, en esencia, donde está el dinero. Pero el uso de estos datos y su posesión es objeto de múltiples cuestiones en cuanto a la privacidad y la seguridad de la información —cabe mencionar otra vez el caso de Cambridge Analytica como referencia de este problema, con el que se puso de relieve el grave riesgo de la explotación de los datos de los usuarios—.

Nuestra atención como usuarios a la venta.

Los algoritmos de personalización de contenido, basados en nuestro uso de las redes, nuestros intereses y nuestro comportamiento, han transformado de forma radical la manera en la que descubrimos y consumimos el contenido, sean noticias o entretenimiento. Pero esto ha derivado en el surgimiento de burbujas en las que nosotros, los usuarios, solo vemos el contenido que refuerza nuestros intereses y conductas, o más bien los intereses y conductas que interesan a esas redes, porque ese contenido personalizado es lo que hace que estemos más tiempo delante de la

pantalla, viviendo dentro de la red social en cuestión, y eso significa más dinero.

Hoy, la rápida difusión de desinformación, noticias falsas y *deepfakes* generados por inteligencia artificial es un tema muy preocupante. La capacidad de manipulación sobre la opinión pública es un problema muy grave, y las medidas que se toman al respecto son cuando menos tibias. ¿Por qué? Pues porque ese tipo de noticias resultan cautivadoras y captan la atención, además de promover la interacción mediante la discusión. Si estamos replicando argumentos o dejando comentarios en publicaciones, permanecemos en la red, conectados y activos, que es lo que buscan. De nuevo, el origen de más beneficios.

Y no podemos dejar de lado el muy preocupante incremento de los problemas asociados a la salud mental, como la ansiedad, la depresión o la baja autoestima, desde el surgimiento de las redes sociales. No dejan de aumentar los casos. En los últimos quince años, los suicidios entre adolescentes se han multiplicado, al igual que el número de ingresos en salas de urgencia por trastornos alimenticios, autolesiones o intentos de suicidio. En lo que llevamos de década, son varios los estudios que han resuelto que los adolescentes que pasan más tiempo en redes sociales son más propensos a sufrir problemas de salud mental. Dos son los más destacados. El primero de ellos, publicado en la revista científica *Clinical Psychological Science* y firmado por la psicóloga estadounidense Jean Twenge, lleva por título *Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U. S. Adolescents After 2010*. En este estudio se detalla que los adolescentes que pasan más tiempo en las redes sociales y utilizando sus dispositivos electrónicos reportan mayores niveles de síntomas depresivos y comportamientos relacionados con el suicidio. El segundo estudio proviene de los datos publicados por el CDC, el Centro para el Control y la Prevención de Enfermedades de Estados Unidos. En un muy detallado informe queda patente que las tasas de visitas a urgencias por pensamientos suicidas y autolesiones entre los más jóvenes aumentaron muchísimo entre 2007 y 2015. En el caso de adolescentes de 15 a 19 años llegaron a duplicarse, y en el caso de adolescentes de 10 a 14 años, se triplicaron.

La relación entre estos fenómenos y el auge de las redes sociales es compleja y multifacética, pero innegable. Se origina en la manera en la que están diseñados los algoritmos y las interfaces para generar adicción y acrecentar la polarización.

La percepción de la belleza en nuestro tiempo se ha visto muy influenciada por el uso de las redes sociales, especialmente entre adolescentes. La edición de contenido, fotos y vídeos, y los filtros exponen, a ojos de todos, estándares de belleza inalcanzables, en muchos casos del todo irreales. La explotación de la imagen personal a través de herramientas para modificar la apariencia y crear versiones idealizadas se ha vuelto norma. Y esta exposición de cuerpos perfectos deriva en una disminución de la autoestima y de una percepción negativa sobre el cuerpo, lo que es muy perjudicial para adolescentes, todavía en una etapa crucial del desarrollo de sus cuerpos y sus identidades. Trastornos alimenticios asociados a la presión para alcanzar los estándares reflejados en redes, ansiedad y depresión al compararse con imágenes que no son reales... Son muchos los estudios asociados a esta cuestión. Por tomar simplemente uno de ejemplo, el publicado en 2017 en *New Media & Society* por las investigadoras Rachel Cohen, Philippa C.D.M. Griffiths e Ivanka Prichard. Con el título *Instagram use and young women's body image concerns and self-objectification: Testing mediational pathways*, en el estudio se examina cómo el uso de Instagram se asocia con la autoobjetivación en mujeres jóvenes y el aumento de la preocupación sobre la imagen corporal y las cuestiones de salud mental derivadas.

Pero esto no se queda aquí, pues las redes sociales continúan evolucionando con la integración de nuevas tecnologías, como es el caso de la inteligencia artificial o de la realidad aumentada, que moldean la manera en la que los usuarios interactúan con las diferentes plataformas y el contenido, agravando todavía más los problemas.

Las inteligencias artificiales precisan de grandes volúmenes de datos para entrenar y mejorar sus algoritmos, y esto ha impulsado una demanda sin precedentes de información personal. Las cuestiones asociadas a la preocupación en torno a la privacidad y la seguridad son aún mayores en este escenario. Cada vez resulta más difícil para los usuarios controlar cómo y dónde se utilizan sus datos.

Las grandes empresas tecnológicas, que ya poseían vastas cantidades de información gracias a sus plataformas y los servicios prestados, han visto en la IA una oportunidad para expandir su dominio. Con el pretexto de mejorar la personalización de servicios y la eficiencia de las tecnologías, estas compañías recopilan datos que luego utilizan para entrenar sus propios sistemas de IA y perfeccionar modelos predictivos, lo que se traduce en una

capacidad sin precedentes para influir en comportamientos, decisiones y el pensamiento crítico.

Este ciclo refuerza su posición dominante en el mercado y limita la capacidad de los usuarios para proteger su privacidad.

La falta de transparencia sobre cómo se utilizan los datos y la dificultad de los usuarios para optar por alternativas de verdad privadas acentúan la sensación de vulnerabilidad. Además, el uso de IA en la creación de perfiles detallados y la predicción de comportamientos puede llevar a una explotación aún mayor de las brechas de privacidad.

Ante esto, la respuesta se encuentra en la web 3.0, un internet descentralizado que nos devuelva el control sobre nuestros datos y experiencias, hasta ahora en manos de grandes corporaciones tecnológicas. A través de identidades soberanas en la blockchain podremos recuperar el control sobre el contenido que generamos. En la web 3.0 también disponemos de herramientas para luchar de forma activa contra la inteligencia artificial centralizada y los algoritmos, lo que es posible gracias a la gobernanza mediante tokens, la verificación de humanidad de un usuario y la comprobación de autenticidad de contenidos.

En los últimos años, estamos asistiendo a una explosión de los *deepfakes*, vídeos, audios o imágenes manipulados mediante inteligencia artificial para mostrar a alguien haciendo o diciendo algo que en realidad no ha hecho o dicho. Esta tecnología se sirve de los avances en redes neuronales y aprendizaje profundo para crear complejas manipulaciones que cada día que pasan son más convincentes. Permite, por ejemplo, crear vídeos falsos de figuras públicas en situaciones comprometedoras o suplantar la identidad de individuos con fines perversos, lo que provoca consecuencias personales y profesionales muy graves. Uno de los casos que mayor repercusión ha tenido es el de Patrick Hillmann, gerente de comunicaciones de la empresa Binance, a quien suplantaron la identidad recreando su imagen y su voz en videollamadas de Zoom para estafar a clientes y asociados. Y otro que puede mencionarse y tuvo mucha repercusión fue el del presidente de Ucrania, Volodymyr Zelenskiy, capitulando ante las demandas de Rusia. En este último caso, se podía ver al presidente de Ucrania pidiendo a los ucranianos que depusieran las armas ante los invasores rusos.

Tanto la cantidad como la calidad de los *deepfakes* están aumentando de forma exponencial, y esto plantea grandes desafíos

para su detección. Como cabría esperar, su exponencial crecimiento y su uso socavan la confianza en la información misma o en lo que se nos pone delante en redes sociales, que, y perdón por insistir, está controlado por los algoritmos de las grandes tecnológicas, cuyo objetivo es que pasemos más tiempo delante de las pantallas, dentro de sus *corporate states*, independientemente de la ética o de nuestro bienestar.

Las grandes empresas tecnológicas han reescrito las reglas del juego para su propio beneficio.

Internet, concebida como una red descentralizada, ha ido convirtiéndose, cada vez más, en un espacio en el que el poder se aglutina en unas pocas redes centralizadas, donde la capacidad de innovación es limitada y se da poco margen a la creatividad.

Y muchos de nosotros, sea por costumbre o simple comodidad, nos conformamos. Buena parte de la sociedad no percibe ningún problema en la estructura establecida. Están satisfechos con todo lo que ofrecen las grandes empresas tecnológicas. Podemos estar en contacto con quien nos parezca y cuándo queramos —siempre y cuando esté dentro de las pautas regladas establecidas por los directivos de la plataforma utilizada, claro— y tenemos a nuestra disposición multitud de servicios a coste cero, «gratis». A cambio, nada más que nuestros yoes digitales, no solo los datos de nuestra información personal, sino los datos que conforman las versiones de nosotros mismos en la red, lo que conforma quiénes somos. Lo que buscamos, dónde estamos en cada momento, aquello con lo que interactuamos, el momento en el que lo hacemos, lo que compartimos, con quién lo compartimos...

Hay quienes pueden pensar que merece la pena, que ganamos más de lo que perdemos, o quizás que no, pero que es un sacrificio aceptable, pues es la única manera viable de poder disfrutar de lo que las grandes empresas tecnológicas nos ofrecen. Y así fue durante un tiempo, pero ya no. Una nueva tecnología emerge en lo que será el próximo salto en la era digital, donde lo que ahora percibimos como natural quedará relegado por algo completamente diferente. Con el tiempo, lo más probable es que en futuras generaciones se perciba la aceptación de la «esclavitud de nuestras versiones digitales» como algo completamente incivilizado. Al igual que antaño la esclavitud estaba presente y aceptada en nuestra sociedad y luego fue abolida, la idea de la posesión de nuestros

yoes digitales por parte de terceros, por grandes empresas, será vista como algo barbárico. Seguro que dentro de doscientos años la sociedad se pregunta cómo es posible que en nuestro tiempo permitiésemos que las grandes tecnológicas nos sometieran a trabajos forzados mediante violencia psicológica.

El salto a la web 3.0 viene marcado por el surgimiento de la tecnología blockchain, que se presenta como una respuesta a la centralización del control de internet. Esta tecnología tiene la capacidad de devolver el control a los usuarios y de hacer desaparecer a los intermediarios. De fomentar una red mucho más libre y descentralizada, una red en la que los creadores son propietarios de sus creaciones y donde somos dueños de nuestros yoes digitales. En pocas palabras, de recuperar el espíritu fundacional de internet y aplicarlo sobre todo lo construido en los últimos veinte años con el desarrollo de las redes sociales.

La tecnología blockchain permite que internet evolucione a lo que visualizaban aquellos que la crearon, pero que en ese entonces no contaban con la capacidad para llevarlo a cabo por las propias limitaciones de la tecnología. El sueño de una red abierta basada en el consenso y en la colaboración, mantenida de forma colectiva por nodos interconectados pero independientes, con una perspectiva radicalmente distinta en cuanto a la gobernanza y la generación de valor.

A diferencia de los sistemas centralizados en los que hoy en día vivimos, la tecnología blockchain pavimenta el camino hacia un sistema completamente descentralizado en el uso de datos y en las transacciones en línea. Plantea un entorno sin intermediarios, regido por protocolos y contratos inteligentes que se ejecutan de forma automática cuando se cumple lo establecido, y en el que las decisiones se toman de manera colectiva.

Al contrario de la forma en la que internet funciona hoy en día, donde las decisiones y las pautas las establecen —y también las cambian a placer, sin previo aviso— autoridades centrales, en las redes blockchain la gobernanza es colectiva. Esto significa que todos y cada uno de los integrantes de una red tienen voz en las decisiones importantes, sean cuales sean los asuntos que tratar. Se migra así de un modelo de gobernanza de accionistas, *shareholders*, a un modelo donde son los usuarios, los operadores y los inversores, los *stakeholders*, quienes gobiernan. Actualizaciones de *software*, cambios en las tarifas por uso de la tecnología, gestión de la tesorería... Los

usuarios tienen la capacidad de influir en cualquier decisión importante. Esto es posible gracias a algoritmos y protocolos de consenso, que determinan que cualquier decisión ha de ser aprobada por una mayoría de nodos o de tokens (sobre ambas cuestiones hablaremos más adelante). El poder está perfectamente distribuido dentro de la misma red. Una verdadera democratización del poder, de la toma de decisiones. Y el acceso es completamente abierto. Cualquier persona con una conexión a internet puede unirse, no hay barreras y existe realmente la igualdad de oportunidades. Por ejemplarizarlo de una manera que permite entenderlo con mucha facilidad, es como si una hipotética aplicación descentralizada que conecta conductores y pasajeros —la idea detrás de Uber— estuviera gestionada no por la empresa que la ha creado, sino por los propios conductores, por los pasajeros, por los inversores y por todos los integrantes del equipo que trabajaban en mejorar la aplicación. Todos al mismo tiempo. Más adelante veremos cómo este ejemplo es ya una realidad.

Con blockchain, los datos son inmutables y transparentes, lo que significa que, una vez ha quedado registrada una transacción, esta no puede ser alterada y en todo momento puede ser verificable. Además, en el entorno blockchain las transacciones son mucho más seguras y protegen la identidad y la privacidad de los usuarios. Un claro contraste con los modelos centralizados de los *corporate states*, donde los datos pueden ser almacenados, recopilados y utilizados sin el consentimiento explícito de los usuarios.

Asimismo, debido a su naturaleza descentralizada, las redes de blockchain se sustentan en multitud de puntos de control, lo que imposibilita que cualquier entidad, sea un Gobierno, una empresa o un particular, pueda censurar o manipular la información. El contenido en una red blockchain está siempre disponible para su verificación por cualquiera de los nodos que integran la red.

La transparencia es una de las características inherentes de la tecnología blockchain. Cualquier usuario tiene acceso a la información presente en la red, y esto reduce las oportunidades de fraude y corrupción. Además, el almacenamiento de la información no depende de servicios centralizados —como pueden ser Google Drive o Microsoft OneDrive—, sino que se conforma sobre la red de nodos. La seguridad y la privacidad de los datos es muchísimo mayor.

La tecnología blockchain también tiene el potencial de transformar la economía tal y como la conocemos. Las criptodivisas —una

forma de dinero digital diseñada para operar de manera descentralizada— son solo uno de los muchos tipos de criptoactivos y permiten transacciones sin intermediarios tradicionales, como los bancos, por ejemplo, lo que conlleva amplias reducciones de costos y abre múltiples oportunidades para una mayor inclusión financiera a nivel de todo el globo. Los ejemplos más significativos y conocidos de criptoactivos son bitcoin y ether, de la red Ethereum.

«Estamos inmersos en el proceso de transformación tecnológica más significativo desde el dominio del fuego».

John Perry Barlow, autor de la *Declaración de Independencia del Ciberespacio*