CIBERESPACIO

AMPLIACIÓN DEL CAMPO DE BATALLA

G. Carbonell
Movimientos sociales: cambio social y participación
UNED, 2021

“Just because you're paranoid doesn't mean they aren't after you.”

ÍNDICE

Hipótesis

La génesis de internet no es un proceso lineal, sino la interacción dialéctica de diversos actores en pugna por ocupar un nuevo espacio de información, que de manera genérica se ha definido como *ciberespacio*. En este contexto, “hay una coordinación creciente de la acción de organizaciones e individuos usando medios digitales para crear redes, estructurar actividades, y comunicar sus puntos de vista directamente al mundo”[1].

Y este proceso incluye dos tendencias, tan antagónicas como complementarias. La primera, a la que llamaré *convergencia*, representa la voluntad de centralizar los procesos de información y la persistencia de los datos en conglomerados corporativos con tendencia monopolística. La segunda, a la que llamaré *distribución*, se define por la intención de colectivizar el proceso de la información y la persistencia de los datos entre los miembros de una misma red. Tomadas en conjunto, sus acciones construyen una dialéctica por la hegemonía dentro de un mismo espacio tecnológico. Enfrentadas, se destila una lucha de posiciones ideológicas por el control de los recursos materiales de la red.

Como relato factual de ambas corrientes, encontramos dos grupos de actores principales. Por un lado, los «Gigantes Tecnológicos», empresas con una preponderancia sobre la red que hace que sus acciones definan la respuesta de los actores en minoría, y entre quienes encontramos grandes compañías como Amazon, Google y Facebook —de la liga norteamericana— y JD.com, Alibaba y Tencent —de la liga china—; por otro, encontramos el movimiento *cypherpunk*, heredero de la «filosofía hacker», emparentado con el movimiento de «software libre», y cuyo cometido pasa porque cada miembro de la red tenga autoridad suficiente para defender sus datos de la explotación ilegítima por parte de terceros.

Cuando planteamos la relación entre dichas tendencias, cabe tener en cuenta las conclusiones de McNeill y McNeill sobre la historia de las redes humanas, pues “las redes han combinado cooperación y competición” [...], la dirección general de la historia ha sido hacia una mayor cooperación [...], la escala de las redes humanas ha tendido a crecer [y] el poder de la comunicación humana, en sus vertientes cooperativa y competitiva, también ha afectado a la Tierra en un grado mayor”[2]. Por ende, es insensato plantear dicha relación como una mera dicotomía.

El presente estudio pretende clarificar la relación entre ambas vertientes. Esto es, aclarar *en qué medida se diferencian o retroalimentan los paradigmas comparados*. ¿Estamos

[1] Bennett y Segerberg, 2012, p. 749.
[2] Van Dijk, Jan, 2012, p. 23.

hablando de tendencias enfrentadas o cooperativas? Si bien pudiera parecer que los *cypherpunk* exhiben una posición antagónica frente a la lógica de las corporaciones mercantiles, no es menos cierto que estas mismas corporaciones parecen capaces de fagocitar las aportaciones de los *cypherpunk* para su propio beneficio.

Y de manera subsiguiente, tal planteamiento invita a cuestionar el potencial del movimiento *cypherpunk* inmerso en la lógica del desarrollo de internet como un proyecto cívico, más allá del criterio mercadotécnico de su crecimiento en las últimas tres décadas. En otras palabras, aclarar *en qué medida se consolidan los cypherpunks como una acción colectiva capaz de influir en las decisiones políticas sobre la configuración de internet*: si sus propuestas son capaces de medrar en las políticas hegemónicas de la red, o si por contra su discurso no llega a calar lo suficiente como para provocar cambios.

Metodología

Ambas cuestiones planteadas exigen juzgar la relación de los *cypherpunks* con la totalidad de los agentes en red desde finales de los años 80 hasta la actualidad, periodo que comprende desde su nacimiento hasta su *status quo* presente. Y siendo la pretensión de este estudio entender el resultado *material* de sus planteamientos *teóricos* a lo largo del tiempo, se hace necesario adoptar un enfoque que permita ponderar la acción política desde su génesis individual y prospectiva hasta la acción colectiva factual a lo largo del tiempo; cómo se construye la intención de cambio desde el individuo particular hacia una masa potencial de individuos con capacidad de reconfigurar y/o reconectar (*network-making power*)[3] la arquitectura de la red. En este sentido, merece tener en cuenta que los datos recabados respondan a quiénes participan y por qué lo hacen en primera instancia[4], y a de qué forma actúan en sociedad en segunda.

En un ecosistema digital emergente donde los recursos pueden ser creados —y lo serán— por los actores en pugna, no tiene sentido plantear la movilización de recursos colectivos como se podría, por ejemplo, plantear una redistribución del gasto público, tanto como plantear en qué medida la acción individual puede sumar a la acción del conjunto. En otras palabras, deberíamos centrarnos en cómo la "dimensión individual de la participación"[5] construye un "un proceso social de doble vía, un movimiento convergente que se produce

[3] Catells, 2011, p. 776-777.
[4] Funes Rivas, 2019, p. 228-229.
[5] Funes Rivas, 2019, p. 226.

desde el individuo a la sociedad y desde la sociedad al individuo"[6]. Tal y como argumentaron algunos padres de la cibernética, entre los que se incluye el matemático Norbert Wiener, estudiar este tipo de procesos implica considerar la retroalimentación (*feedback*)[7] de los actores; cómo estos alcanzan sus propósitos mediante la sinergia, no mediante la toma y división. En un paradigma sociológico mediado como el actual,

> El contexto general presenta una serie de propuestas analíticas o conceptuales que proponen que la Internet y los medios digitales cambian profundamente la sociedad, a través de las posibilidades de interconexión y asociación que ofrecen. [...] Partamos por establecer que la Internet permite una transformación fundamental de la acción de los ciudadanos [...], gracias a la existencia de mecanismos de asociación distintos, más diversos y menos concentrados en manos de los actores políticos tradicionales [...].[8]

En otras palabras, para entender cómo se retroalimentan convergencia y distribución y hasta qué punto el movimiento *cypherpunk* se postula como un movimiento contestatario frente al *Establishment* tecnológico, tendremos en cuenta en qué medida la *conexión* (humana) se ve condicionada por la *conectividad* (tecnológica), y si dicho proceso es capaz de transformar la *acción conectiva* (la mera presencia de los medios tecnológicos para el intercambio de significado) en una *acción colectiva*[9] (la consolidación de un movimiento con capacidad de cambio social). Tal y como apuntan Bennett y Segerberg[10], cabe distinguir entre una acción conectiva autoorganizada (en la que el individuo mediático tiene acceso a la esfera pública pero está solo en la acción), una acción conectiva con potencial organizativo (en el que existe convergencia de intereses individuales pese a que las instituciones planteadas son incapaces de cuestionar el *status quo*, por lo que el discurso se orienta hacia la acción individual), y una acción colectiva propiamente dicha (una situación donde la connivencia de razones e instituciones comunes promueven la acción coordinada).

Aunque "las compañías tienden a enfatizar [la *conexión*] y minimizar [la *conectividad*]"[11], confundiendo los conceptos, no podemos obviar que la estructura social y las posibilidades tecnológicas son dos abstracciones categóricas distintas, que pese a estar relacionadas no tienen por qué determinarse de manera necesaria; ya que "no hay nada preestablecido acerca

[6] Funes Rivas, 2019, p. 226.
[7] Rosenblueth, Wiener, Bigelow, 1943, p. 2.
[8] Villanueva 2015, p. 59-60.
[9] Bennett y Segerberg, 2012.
[10] 2012.
[11] Van Dijck, José, 2013, p. 12.

de los resultados de los procesos mediados digitalmente"[12]. Esta consideración nos será útil para trazar causalidades entre progreso técnico y cambio social, en lugar de tomar ambos fenómenos como un todo ontológico a modo de caja negra. Además, ignorando tal distinción favoreceríamos a la parte convergente, dando por hecho que su modelo de negocio tecnológico es tan lícito como la adopción social que tenga:

> Mercantilizar las relaciones —transformar *conexión* en *conectividad* mediante tecnologías de programación— es exactamente lo que las plataformas corporativas, particularmente Google y Facebook, descubrieron como el huevo de oro que su oca les daba. Además de generar contenido, [la] producción [colectiva por parte de los usuarios] genera un subproducto valioso que los usuarios no suelen dar intencionadamente: datos sobre conducta y perfil.[13]

Como contrarespuesta a esta tendencia, también se observa, en los disidentes en red,

> un patrón de búsqueda de recursos organizativos informales, en el que los recursos organizativos informales y los espacios de comunicación son vinculados y compartidos (ej: *retweet*), permitiendo que emerjan sensibilidades políticas y objetivos que pueden ser perseguidos sin ser compartidos por organizaciones preexistentes con agendas políticas fijas.[14]

Con lo dicho, podemos aventurar cuatro dimensiones sobre las que hay que tener constancia a la hora de abordar el problema: las tecnologías implicadas, qué discursos suscita el progreso tecnológico, que instituciones generan dichas interacciones y en qué medida estos tres aspectos afecta al legislador cuando se trata de regular el ciberespacio emergente.

Por motivos prácticos, la investigación sobre estas dimensiones presentará el estado de la cuestión de internet en dos momentos capitulares de su definición, con tal de establecer una comparativa entre ambos. Dicha puesta en común del antes y el después debería permitirnos responder a las hipótesis propuestas en términos de evolución desde los presupuestos originales —eminentemente teóricos— y la actual situación —de naturaleza práctica—.

El primer hito será situado en torno a 1990, momento en el que los antecedentes de internet convergen para crear la «red de redes», con la esperable confrontación entre el *ethos*

[12] Bennett y Segerberg, 2012, p. 754.
[13] Van Dijck, José, 2013, p. 16.
[14] Bennett y Segerberg, 2012, p. 758-759.

altruista de quienes entienden el asunto desde un punto de vista socialista, libertario o romántico, y la intención de las empresas tecnológicas por invertir en la construcción de un nuevo espacio comercial desde la lógica mercantil. Y el segundo hito pivotará en torno al año 2018, momento en el que tanto las corporaciones como los *cyberpunk* han implementado las tecnologías que proponían hace tres décadas y empezamos a intuir las consecuencias de su puesta en práctica; del lado de Facebook, escándalos como el de Cambridge Analytica como pináculo de los escenarios distópicos a los que nos aboca la centralización nos ayudarán a entender los vicios de un discurso en pro del determinismo tecnológico y la lógica aplastante de su trasfondo neoliberal; del otro, tecnologías como Bitcoin o TOR inauguran un desafío a las democracias liberales, caracterizadas por la transparencia y el estado de derecho, ahora puestos en duda a través de tecnologías distribuidas y criptográficas que exceden la capacidad de las naciones-estado para fiscalizar las actividades públicas de la ciudadanía.

Con tal de establecer una comparativa en igualdad de condiciones, teniendo en cuenta las dimensiones objetivo, para ambos momentos se tratará de resolver dos preguntas: *cómo se estructura la «red»*, pues el concepto de «internet» no parte de la nada ni se mantiene estático en el tiempo; y *cuál es el estado del movimiento cypherpunk como contrarrespuesta a la lógica de políticos y corporaciones en el desarrollo de internet*. Para la primera cuestión, se hace necesario entender la evolución de la topología de la red, cuantificar la creación y adopción de las tecnologías que emergen conforme pasan los años en forma de respuesta a los distintos problemas que plantea la arquitectura de la red, y hacer un análisis cualitativo sobre la legislación vigente. Para la segunda, un análisis crítico de los discursos que esgrimen ambas partes dotará de justificación a sus posiciones, mientras que inventariar las instituciones nacientes que se van articulando nos dará una idea del calado sociocultural de las propuestas y su posición frente a los *policy makers* (los políticos), quienes a fin de cuentas facilitarán la acción de unos u otros amparándolas en su legitimidad jurídica.

Hecho este trabajo, debería ser posible volver a las cuestiones principales y responder a *en qué medida se diferencian o retroalimentan los paradigmas comparados*, y *en qué medida el movimiento cypherpunk se consolida como un contrapoder frente a las fuerzas centralizadoras de internet*.

A tal efecto, será menester definir en primer lugar qué entendemos por «ciberespacio»: sus naturalezas ontológica y epistemológica, desde un planteamiento hipotético hasta su instauración como un nuevo territorio en lid.

Luego, se utilizarán los hallazgos para construir sendos relatos en función del momento histórico, aunando los datos en dos narraciones historiográficas. Una vez tengamos ambas

narraciones, nos será posible comparar su evolución, para después destilar conclusiones en forma de pesquisas; con la intención de que estas últimas consideraciones nos permitan dilucidar la tendencia actual de internet en lo relativo a su convergencia y distribución.

Definición de «Ciberespacio»

La definición original que Norbert Wiener (1961) hace de *cibernética*, como "el control y la comunicación en el animal y en la máquina", rehuye la consideración moral sobre las consecuencias de dicho control y comunicación. Los sistemas actúan, se retroalimentan, aprenden de esa interacción y vuelven a actuar con el conocimiento adquirido. En resumidas cuentas, la cibernética se postuló como la ciencia sobre los sistemas y su autorregulación. No obstante, como matizó William R. Ashby en su *Introduction to Cybernetics*:

> La cibernética [...] es una "teoría de las máquinas", pero no trata de cosas sino de *maneras de comportarse*. No pregunta "¿qué *es* esta cosa?" sino "¿*qué hace* esta cosa?" Por lo tanto está muy interesada en un aserto como "esta variable está pasando por una oscilación simple y armónica", y se preocupa mucho menos con el hecho de si la variable es la posición de un punto o de una rueda, o el potencial eléctrico del circuito. Es pues esencialmente funcional y conductista.[15]

Dicho esto, cuando hablamos de *ciberespacio* nos podemos referir en primera instancia a un *locus* conceptual, al paradigma que filtra la realidad desde esta concepción fenomenológica, aunando los intereses de humanos y máquinas en una interacción constante mediada por la información. En este sentido amplio, que trata la cibernética como una ciencia equivalente a la física o las matemáticas, cualquier espacio en el que se produce un intercambio de información entre las partes es susceptible de ser considerado un *ciberespacio*; del mismo modo que la biología podría pretender entender el mismo espacio en términos de *ecosistema*, o la sociología en términos de *cultura*.

No obstante, resulta fácil intuir, juzgando desde el año 2020, qué puede entenderse por *ciberespacio* cuando el concepto se presenta en sociedad. Esta segunda instancia, que representa la consideración hegemónica del concepto, tiende a tratarlo como sinónimo de "internet" o "red global", circunscribiendo la frontera de los fenómenos que se autorregulan al espacio tecnológico de los medios. Y habida cuenta del desarrollo de internet en las últimas

[15] Ashby, 1956, p. 1.

décadas, y de la penetración de esta tecnología en la vida en común, bien podrían equipararse ambos conceptos y deducir que, en su sino, el ciberespacio se estructura desde la "red de redes", y que su extensión permea todo sistema que participe en éstas (desde servidores hasta *smartphones*). Por su parte, internet ya fue el resultado de la agregación de redes preexistentes, tales como ARPANET o USENET, en un espacio común de transmisión de información bajo el protocolo TCP/IP. Y en suma, en el presente escrito trataremos el ciberespacio desde esta perspectiva.

Tal como inauguró el concepto el autor de ciencia ficción William Gibson, desde esta segunda instancia, el ciberespacio se podría definir como:

> Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos… Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano.[16]

En otras palabras: el ciberespacio es un territorio alegórico. Y Gibson, uno de los mayores exponentes de la literatura *cyberpunk* (no confundir con *cypherpunk*), articulaba esta definición de ensueño digital dentro de un marco distópico, donde el futuro había traído "high tech, low life"[17].

En este contexto, similar al que evoca el literato Neil Stephenson en *Snow Crash* (1992), el avance tecnológico supone al mismo tiempo una Ítaca cibernética y un Leviatán digital impredecibles. El momento intelectual de los Estados Unidos en los años 80 sitúa el ciberespacio como algo más que un receptáculo de información: es un espacio epistemológico, una "alucinación consensuada" que emerge de la puesta en común del legado informático humano. Lo que queda por discutir en este momento es qué nacerá de la incipiente propuesta tecnológica, consistente en comunicar los ordenadores.

Herederos de los movimientos previos al nacimiento de la "World Wide Web" de Tim Berners-Lee unos años más tarde, los discursos tecnófilos del momento no parecen alejarse de la idea de que una red de información global supondrá un nuevo continente por conquistar y civilizar. Como afirmó el matemático Charles M. Hammill en su conferencia *From Crossbows to Cryptography: Techno-Thwarting The State*[18]: "la tecnología representa una de las vías más prometedoras para recapturar nuestras libertades de aquellos que nos las han robado".

[16] Gibson, W. *Neuromante*, 1984.
[17] Trad.: alta tecnología, vida precaria.
[18] Hammill, 1987.

Estado de la cuestión en 1990

El estado embrionario de internet es el resultado de la suma de intereses académicos, políticos, empresariales y militares. Por lo tanto, internet nace como un intento por conectar todas las redes aliadas preexistentes en una más grande; en un contexto de colaboración científica sin precedentes. La 1ª Conferencia Internacional de Comunicación por Ordenador (Washington, 1972) da cuenta de los perfiles profesionales implicados en su desarrollo, sobre todo del desarrollo de ARPANET, una red encargada por el Departamento de Defensa de los Estados Unidos:

> ARPANET es la estrella del histórico encuentro. Bob Kahn, de la oficina de Mando [y] Control del Departamento de Defensa estadounidense, consigue conectar veinte ordenadores en vivo y en directo, "el punto de inflexión que hizo que la gente se diera cuenta de que la conmutación de paquetes era una tecnología real". Allí nace el International Networking Group (INWG), el primer grupo de trabajo de la red. Su núcleo son Alex McKenzie, los británicos Davies y Roger Scantlebury y los franceses Louis Puozin y Hubert Zimmermann. No hay ninguna mujer y todos son del frente aliado. Su primer presidente es un joven matemático llamado Vint Cerf.[19]

Tan pronto como se pusieron a trabajar, se hizo evidente el conflicto de intereses entre los propietarios de la red y quienes enviaban información a través de la red. En este momento todavía no consideramos la implementación de aplicaciones sobre los protocolos, sino que lo que se debate es la fórmula técnica que haga posible la conectividad misma. Esta rivalidad se mantendrá en el tiempo, y hará entrar en conflicto a empresarios, *telecos*, políticos y usuarios.

> El grupo debatió entre las dos versiones enfrentadas de la conmutación de paquetes. La solución Cerf-Kahn era dejar que el itinerario y ancho de banda de la transmisión fuera preasignado por la operadora, como una llamada telefónica. Este modelo se llamaba de "circuito virtual". La solución Pouzin-Davies era repartir esa responsabilidad entre los nodos, que podían recalcular la trayectoria óptima de cada paquete en función del tráfico existente, el ancho de banda disponible y el número de nodos disponibles en ese preciso momento. [...] Cerf lo recordaría como una guerra religiosa. [...] Se enfrentaba el universo constante de los objetos de los ingenieros de telecomunicaciones con el

[19] Peirano, 2018, p. 64.

> mundo cambiante de los departamentos de comunicación. Era *hardware* [contra] *software*, un cambio total de paradigma. El grupo de trabajo no sabía qué tecnologías surgirían, qué clase de ordenadores habría o para qué la iban a necesitar en el futuro. Tenía que poder evolucionar sin estar optimizada para ningún tipo de material, técnica, conductor o metodología específica, de manera que una o muchas de sus partes pudieran ser reemplazadas sin alterar su estructura fundamental.[20]

Por estas razones la red se diseñó como un esquema genérico; como una implementación TCP/IP multiprotocolo que garantizase versatilidad y crecimiento.

Si bien es cierto que hasta principios de los 80 los sistemas de información representaban una idea Orwelliana del mundo[21], denostada por los libertarios, la adopción de la informática personal y la progresiva incorporación de los hogares a las redes pareció propiciar un sentido de comunidad, cuyo epítome son los *Bulletin Board Systems* (o BBSs) y cuyo espíritu pasa por compartir el código. En este contexto, USENET[22] nace como una red alternativa entre civiles:

> Fuera del entorno militar, el ambiente era completamente distinto. "USENET estaba organizado en torno a los grupos de noticias, donde el receptor controla lo que recibe —explica [Stephen] Daniel [padre de USENET]—. ARPANET estaba organizado en torno a listas de correo, donde hay un control central para cada lista que potencialmente controla quién recibe el material y qué material se transmite."[23]
>
> [...]
>
> En [los] grupos de noticias [de USENET] se anunció y compartió por primera vez el código fuente de algunos de los pilares de la red, desde la World Wide Web al kernel de [GNU]/Linux. Fue la inspiración de los canales IRC y de los primeros movimientos sociales online.
>
> [...]
>
> Comparada con el modelo OSI y con TCP/IP, USENET era la verdadera red abierta, democrática y neutral. Al menos, si olvidamos por un momento que eran todos

[20] Peirano, 2018, 66-67.
[21] Hammill, 1987.
[22] Acrónimo de *USErs NETwork* ("la RED de los USUarios"), creada por Tom Truscott y Jim Ellis en 1979.
[23] Peirano, 2018, p. 70.

> hombres de entre veinte y treinta años, programadores y blancos de clase media/alta con acceso a un ordenador y una línea telefónica.[24]

Y en este contexto, antes incluso del nacimiento de internet, nace en 1983 el Proyecto GNU[25], que inicia Richard Stallman, como un intento por democratizar el sistema operativo UNIX con una solución de código libre (*free software*). Como forma legal, las licencias GPL[26] son la fórmula propuesta para gestionar estos frutos, y aspiran a garantizar cuatro libertades básicas: poder usar el *software* para cualquier propósito, poder estudiar cómo funciona y hacer modificaciones, poder distribuir copias y poder modificar el programa y distribuir estas modificaciones[27]. La intención de dichas licencias es que quien adquiera un programa no lo haga en forma de archivo compilado, sino con el permiso legal para examinar todos los detalles de su implementación incluyendo el código fuente y hacer modificaciones. La propuesta tendrá un calado de tal relevancia que ya no se podrá concebir la adopción de una tecnología criptográfica sin la posibilidad de examinar su código con el fin de asegurar que está libre de funciones de espionaje.

La propuesta de Stallman evolucionará, y en 1985 se creará la *Free Software Foundation*, cuya misión es facilitar la adopción del paradigma del software *libre* en el ecosistema tecnológico, frente al llamado *software privativo*; la antítesis cerrada donde el usuario suscribe unos términos *de uso* (no de tenencia), no tiene acceso al código, ni se le permite hacer modificaciones y/o distribuir copias.

Un año más tarde, en 1986, nacerá la *Internet Engineering Task Force*, "un encuentro de investigadores financiados por el gobierno de los EE.UU."[28], que invitará a otras partes a participar en sus proyectos, y cuya misión consiste en desarrollar "estándares abiertos a través de procesos abiertos"[29].

En este periodo, donde unos construyen un ARPANET a escala global mientras otros operan en redes específicas al tiempo que todos comparten propuestas teóricas de implementación, comienzan a plantearse los problemas futuros de la adopción masiva de las tecnologías conectivas: ¿qué sucederá cuando todo esté conectado? Con una red abierta y adaptable, el ciberespacio podría crecer, pero los datos quedarían a merced de las aplicaciones y sus protocolos. Y si los futuros operarios no fueran cuidadosos, su información

[24] Peirano, 2018, p. 70-72.
[25] Acrónimo recursivo de *GNU is Not Unix* ("GNU No es Unix").
[26] Acrónimo de *General Public License* ("Licencia General Pública").
[27] Free Software Foundation, 2016.
[28] Bradner, 1999.
[29] IETF, n.d.

personal podría estar al descubierto para los creadores de estas aplicaciones y protocolos. En última instancia, los usuarios serán tomados como los únicos garantes confiables de sus propios intereses.

Por aquel entonces, los ingenieros y académicos Chuck Hammill[30], Timothy C. May[31], Eric Hughes[32], Hal Finney[33], John Perry Barlow[34], Phil R. Zimmermann[35] *et al.* empezaron a advertir de una relación directa entre el desarrollo de los medios de información y los riesgos para la ciudadanía que ello conlleva. "A finales de 1985 había ya 2.000 ordenadores conectados por TCP/IP[;] en 1987 eran 30.000 y en 1989 159.000"[36], por lo que el acuciante cambio de paradigma les obligaba a actuar, so pena de tener que circunscribirse al ciberespacio tal como lo definiesen otros actores (políticos, corporaciones, militares) de quienes no se podía asumir, axiomáticamente en el contexto de la Guerra Fría, que eran confiables.

Su postura pasará por adoptar el cifrado como forma de defensa frente a los potenciales fallos del resto del sistema, asumiendo que dicha adopción cambiaría el paradigma social. Como vaticinó May,

> La tecnología informática está a punto de proporcionar la capacidad de que individuos y grupos se comuniquen e interactúen entre sí de una manera totalmente anónima. [...] Los métodos se basan en cifrado de clave pública, sistemas de prueba interactivos de conocimiento cero y varios protocolos de *software* para interacción, autenticación y verificación. [...] La reputación será de vital importancia, mucho más importante en las transacciones que incluso las calificaciones crediticias de hoy. [...] La criptoanarquía permitirá el comercio libre de secretos nacionales y permitirá el comercio de materiales ilícitos y robados [...] El Estado por supuesto que tratará de enlentecer o detener la difusión de esta tecnología, aduciendo a motivos de seguridad nacional, al uso de la tecnología por traficantes de droga y evasores de impuestos, y a los miedos sobre la desintegración de la sociedad [...]. Al igual que la tecnología de impresión alteró y redujo el poder de los gremios medievales y la estructura de poder social, también los métodos criptológicos alterarán fundamentalmente la naturaleza de las corporaciones y de la interferencia del gobierno en las transacciones económicas[37].

[30] 1987.
[31] 1988, 1994.
[32] 1993.
[33] 1994.
[34] 1996.
[35] 1999.
[36] Peirano, 2018, 74-75.
[37] 1988.

Con este planteamiento, Barlow y sus correligionarios fundaron en 1990 la *Electronic Frontier Foundation*, una organización cuyo cometido a partir de entonces será "liderar la organización sin ánimo de lucro para defender las libertades civiles en el mundo digital"[38].

Como corroboran Bennett y Segerberg, en oposición a la distribución vertical de contenidos a través de estructuras jerárquicas, "la conectividad social implica la coproducción y codistribución, revelando una lógica económica y comercial diferente: coproducción y compartición."[39] Esto significa que, en la medida en que la sociedad se conecta por medios tecnológicos, se expresa un fenómeno emergente de puesta en común de la información. Y hasta el momento, quedan patentes: la naturaleza interdisciplinar del desarrollo de internet, la multiplicidad de redes privadas y públicas, y la confianza en que las aportaciones individuales al común no suman, sino que multiplican el potencial de lo compartido.

Este era el clima preexistente a internet, el paroxismo de la ideación antes de que, una vez conectadas las redes a nivel mundial mediante el protocolo TCP/IP y una estructura de servidores capaz de hacerlo realidad, Tim Berners-Lee y sus colegas definiesen el Protocolo de Transferencia de HiperTexto (HTTP), un lenguaje para definir los hipertextos (HTML) y la World Wide Web como una suma de documentos interconectados. Pero, en un principio, internet no se inauguró como *La Web*, entendida en exclusiva como una colección de "páginas web", sino como un medio polivalente multiprotocolo. La propuesta de la "Gran Telaraña Mundial" dio a luz en el ciberespacio a un territorio de documentos enlazados; que convivirá con otros protocolos como el IRC[40], el FTP[41], las ya citadas BBSs o Telnet[42], igualmente capaces de conectar ordenadores a través del TCP/IP. La presentación oficial ocurrió el 6 de agosto de 1991 en *alt.hypertext*, un grupo de noticias de USENET, y sus creadores optaron por legar la tecnología al dominio público.[43] "Como repitió [Berners-Lee] en las siguientes dos décadas, la web era demasiado importante para dejarla en manos del mercado."[44]

> Si internet nació como una red abierta y fuertemente descentralizada, fue porque el Gobierno estadounidense no entendió su potencial y porque la única operadora que

[38] EFF, 2007.
[39] Bennett y Segerberg, 2012, p. 752.
[40] *Internet Relay Chat* (algo similar a un "Sistema de charla por relevos", que daba la posibilidad de converger en un mismo espacio de diálogo a tiempo real en forma de texto).
[41] *File Transfer Protocol* ("Protocolo de Transferencia de Ficheros").
[42] *TELetype NETwork* ("RED de TELetipos", una forma de enviar comandos remotos).
[43] Peirano, pp. 78, 81.
[44] Peirano, pp. 81-82.

> podía comprarla [AT&T] dijo que no la quería. Si el experimento llegaba a algún lugar, tendría que seguir haciéndolo con el dinero público y como bien público.[45]

En este mismo año se producen otros dos sucesos relevantes. Por una parte, el ingeniero Phil Zimmermann regalará al mundo *Pretty Good Privacy*, que dotará a dos dispositivos dentro de una red monitorizada con la capacidad de establecer comunicaciones encriptadas seguras. El Senado norteamericano había intentado pasar la Ley Anticrimen 266, que "habría forzado a los manufactureros de equipos de comunicación segura a insertar [puertas traseras] en sus productos, de forma que el gobierno pudiese leer los mensajes encriptados de cualquiera"[46], lo que motivó a Zimmerman a liberar su tecnología ese mismo año. Y por otra parte, se aprobó en el 102º Congreso de los Estados Unidos la *High Performance Computing Act*, que agilizó la inversión pública y la implementación de una infraestructura de comunicaciones en dicho país, colocándolo a la vanguardia del desarrollo de internet; hasta el punto de que el acta justificó la provisión de fondos para la creación de Mosaic, el navegador "Web" que propiciaría la adopción masiva del hipertexto a partir de 1993.

Y aquí nacen los *cypherpunk*. Las letanías cibernéticas de los *hackers* altruistas se encontraron de frente con la realidad: el hipertexto materializaba la "alucinación compartida" de Gibson en forma de vistosas impresiones en pantalla, empresas y legisladores estaban allanando el terreno comercial, y la comercialización del nuevo entorno audiovisual cibernético resultaba inminente frente al celo de los otros por construir un nuevo paradigma social en lugar de alimentar el anterior.

En 1992 se fundará la "lista de correo *cypherpunk*" que coordinará el movimiento, "energizada por la batalla con el establishment de la inteligencia de los Estados Unidos en lo relativo a la exportación de criptografía[, …] una batalla que el movimiento *cypherpunk* y la extensa comunidad civil en torno a la criptografía ganaron de pleno"[47]. Dos años más tarde, la lista de correo tendrá 200 miembros, para multiplicar esa cifra por diez alrededor de 1997[48]. Y en 1993, el criptógrafo Eric Hughes publicará a través de este canal *A Cypherpunks Manifesto*, un breve texto al que le podemos atribuir los dogmas básicos del movimiento:

> La privacidad es necesaria para una sociedad abierta en la era electrónica. [...] No podemos esperar que gobiernos, corporaciones y otras organizaciones mayores sin

[45] Peirano, 2018, p. 63.
[46] Zimmerman, 1991-1999.
[47] cryptoanarchy.wiki, n.d.
[48] cryptoanarchy.wiki, n.d.

> rostro nos garanticen privacidad más allá de su beneficencia. [...] Cuando mi identidad es revelada por los mecanismos subyacentes de una transacción, no tengo privacidad. [...] Privacidad no es secretismo. [...] Privacidad es el poder de revelarse a uno mismo selectivamente al mundo. [...] Un sistema anónimo empodera a los individuos para revelar su identidad cuando quieran y solo cuando lo quieran; esta es la esencia de la privacidad. [...] Nosotros los Cypherpunks queremos conocer tus preguntas y preocupaciones y esperamos poder involucrarte con tal de no engañarnos a nosotros mismos. [...] La criptografía se extenderá ineludiblemente por todo el globo, y con ella los sistemas de transacciones anónimas que posibilita. [...] Nosotros los Cypherpunks nos dedicamos a construir sistemas anónimos. [...] Los Cypherpunk escriben código. [...] Nuestro código es libre para que lo usen todos, mundialmente.[49]

Con esta declaración, popularmente resumida en el aserto "*cypherpunks write code*", Hughes dejó claro que el combate no pasaría únicamente por exigir a otros, como ya se ha comentado, una redistribución de recursos y derechos, sino también por construir las herramientas para conquistar la hegemonía en el ciberespacio. La revolución debía de nacer del individuo, de sus aportes al movimiento y de cómo este se relacionaría en red. Esto tiene sentido, si tenemos en cuenta que el ciberespacio recién constituido estaba vacío de contenido pero repleto de posibilidades, y que plantear una redistribución de los medios físicos (servidores, cables, satélites, etc.) significaría volver a un paradigma revolucionario decimonónico que desviaría la atención de la conquista del nuevo territorio.

Al tiempo, la batalla se recrudeció desde el legislativo, con una presión adicional para cierta parte de la industria de las telecomunicaciones. Como reflexionaría Zimmerman tres años después de regalar PGP:

> La Ley de Asistencia de Comunicaciones para la Aplicación de la Ley (CALEA) de 1994 ordenó que las compañías telefónicas instalen puertos de escuchas telefónicas remotas en los conmutadores digitales de su oficina central. Ahora la mayoría de nuestras conversaciones se llevan a cabo de forma electrónica. Esto permite que nuestras conversaciones más íntimas se expongan sin nuestro conocimiento.[50]

[49] Hughes, 1993.
[50] Zimmerman, 1991-1999.

Las amenazas legislativas y la pérdida del control de internet por la parte académica servían de justificación para el sostenimiento del movimiento *cypherpunk*. En contraposición a otros movimientos de corte liberador, no obstante, los *cypherpunk* admiten que no saben en qué consistirá la "criptoanarquía" a la que les lleve la encriptación; sus postulados inmediatos tienen cometidos inmediatos (salvaguardar las garantías civiles en el creciente ciberespacio), y les resulta imposible prometer con firmeza una distopía mejor que aquella que critican. Resulta reseñable que, mientras se sigue defendiendo la encriptación como un valor en alza para las nuevas democracias en red, pues las "implicaciones negativas [...] son sobrepasadas en la totalidad por los beneficios"[51], activistas como Timothy C. May llegan a plantearse que la criptografía podría traer consigo vicios de los que nos salva una sociedad sin encriptación. Por eso, en 1994, rodeado de motivos para desconfiar del resto, llega a resumir las desconfianzas hacia su propia propuesta: mercados de asesinos a sueldo, secuestro, extorsión; *crowdfunding* para hacerle a alguien la vida imposible; facilidades para el chantaje y el soborno; un espacio seguro para abusadores, pederastas y violadores; reventa de secretos corporativos y nacionales; *vigilantes* cibernéticos al margen de la ley; desconfianza en el entorno familiar, sobre todo si el Gobierno ofrece incentivos; evasión fiscal; conspiraciones; etcétera.[52] Claramente, unas consideraciones autocríticas que no encontraremos en políticos ni en corporaciones sobre sus sendos *modus operandi*.

En este momento, a tres años del nacimiento de *La Web*, Tim Berners-Lee y los suyos fundan el *World Wide Web Consortium* (o W3C); una asociación que, en la línea de la *Internet Engineering Task Force* nacida en los 80, tiene como cometido promover la utilización de estándares abiertos sobre la incipiente red de comunicación multifuncional.

Y otras costuras que se rompen: el *free software* no redefine sus principios fundamentales, aunque otros comienzan a reciclar sus propuestas. En 1996 surge la *Open Source Initiative*, que Stallman y los suyos entenderán como una respuesta de la industria privatizadora por apuntarse al éxito del software libre:

> El software libre se extendió como un incendio a lo largo y ancho del planeta. Sin más publicidad que el acceso al código, sin más satisfacción que la posibilidad de aprender, buscar soluciones, hacer juegos y programas y compartirlos con personas afines.
>
> [...]

[51] May, 1994, 16.10.2.
[52] May, 1994, 16.10.2.

> La industria no podía rociarse con el perfume revolucionario del software libre tal cual estaba. La GPL lo había blindado contra la explotación, la exclusividad y el monopolio. Así que introdujeron una pequeña reforma: ya no se llamaría software libre sino "open source" o código abierto. Y no usaría GPL sino otras licencias "parecidas" pero más modernas y molonas (sic). Y vendría vestido con la capa de colores brillantes de lo que Stallman había querido evitar: el capitalismo.[53]

La gota que colma el vaso para la tendencia distributiva es la *Telecommunications Reform Act* de 1996, que "libera radicalmente el mercado de las telecomunicaciones en los Estados Unidos, eliminando toda restricción sobre fusiones, adquisiciones, propiedades o negocios cruzados."[54] Con ella se abrirá la veda para que propietarios de distintos medios converjan en conglomerados corporativos. Esto se traduce en mayores concentraciones de capital, lo que revierte en un mayor poder de influencia frente al legislador (*lobbyism*) frente a la capacidad de los activistas individuales, que ven en esta acción de la administración Clinton una declaración de intenciones desde la corporatocracia, que traiciona el *ethos* fundacional de la red (cooperativo, descentralizado, libre) en pro de una red mercantil, corporativa y regulada. En este sentido, y en relación con el sentimiento de privación individual, el discurso de la tendencia distribuida se estructura desde "la dimensión afectiva y emotiva, que no irracional, [y] la participación [se produce] como consecuencia de experiencias intensas de agravio o privación"[55].

En una declaración desesperada, un enfurecido John P. Barlow publica su *Manifiesto de independencia del Ciberespacio*:

> Gobiernos del Mundo Industrial, cansados gigantes de carne y acero, vengo del Ciberespacio, el nuevo hogar de la Mente. En nombre del futuro, le pido al pasado que nos dejen en paz. No son bienvenidos entre nosotros. No tienen soberanía donde nos reunimos. [...] Estamos formando nuestro propio Contrato Social. Esta gobernanza surgirá de acuerdo con las condiciones de nuestro mundo, no el suyo. Nuestro mundo es diferente. [...] El nuestro es un mundo que está en todas partes y en ninguna parte, pero no es donde viven los cuerpos.
>
> [...]

[53] Peirano, 2018, 159-161.
[54] Peirano, 2018, p. 82.
[55] Funes, 2019.

En los Estados Unidos, ustedes han creado hoy una ley, la [Telecommunications Reform Act de 1996], que repudia nuestra propia Constitución e insulta los sueños de Jefferson, Washington, Mill, Madison, DeTocqueville y Brandeis.

[...]

El Ciberespacio no se encuentra dentro de sus fronteras. No crean que pueden construirlo, pues se pensó como un proyecto de construcción pública. [...] Ustedes no conocen nuestra cultura, nuestra ética, o los códigos no escritos que ya proveen a nuestra sociedad más orden del que podría obtenerse de cualquiera de sus imposiciones.

[...]

Los gobiernos obtienen sus poderes justos del consentimiento de los gobernados. Ustedes no han solicitado ni recibido el nuestro.

Estado de la cuestión en 2020

Nos centraremos ahora en la situación de internet tres décadas después de su génesis. Para ello, resulta necesario resumir el lapso entre principios de siglo y el surgimiento de las plataformas sociales que hoy son hegemónicas. Este periodo comprende desde el estallido de la "Burbuja Puntocom" a principios de siglo hasta la presentación del primer iPhone por Apple en 2007, y supone un periodo de efervescencia de las propuestas *cypherpunk* al tiempo que la industria reinventa el *software libre* en forma de *open source*.

El celo de las empresas por tomar el espacio emergente trajo consigo un aumento considerable de la inversión especulativa en nuevas tecnologías, lo que infló la valoración de las teleoperadoras y los incipientes "portales web" en bolsa. "La inmensa burbuja generada en torno a las empresas tecnológicas de Internet pinchó[, y] el mercado perdió en dos años cinco billones de dólares. [...] La burbuja fue creciendo hasta los 5.048 puntos que alcanzó el Nasdaq. [...] Año y medio después del crack, el Nasdaq seguía en caída libre y había perdido el 78% de su valor. El mínimo lo marcó el 9 de octubre de 2002, cuando el índice se situó en 1.114 puntos."[56] Y esta debacle financiera costeada por los grandes inversores, que bien podría haberse entendido como un acto de justicia poética por parte de los *cypherpunk*, aceleró la selección natural de los más fuertes. "La red quedó en manos de unos cuantos monopolios y la deuda redistribuida entre los contribuyentes y futuros usuarios."[57]

[56] El País, 2010.
[57] Peirano, 2018, p. 84.

No hay que olvidar, tampoco, que en este mismo periodo se produce el atentado del 11 de septiembre del 2001 contra las Twin Towers del Wall Trade Center. Entre todas sus consecuencias y el potencial cambio de paradigma geopolítico que suscita el crimen, la que concierne a los *cypherpunk* tiene que ver con la aprobación, el 26 de octubre de 2001, de la *USA PATRIOT Act*[58], que pretendía dotar de más poder de fiscalización del ciudadano al Gobierno de los Estados Unidos con el pretendido objetivo de combatir a los terroristas. No obstante, como denunciaron multitud de organismos, el texto infringía "el derecho a la privacidad y [eliminaba] muchos tipos de revisión judicial sobre actividades de inteligencia"[59]. Como explicó el Comité de Abogados por los Derechos Humanos en 2003,

> Los últimos dos años han visto una creciente preocupación bipartidista de que las salvaguardas de la Cuarta Enmienda contra la intrusión gubernamental arbitraria se estén erosionando en nombre de la seguridad nacional. La ley que regula la autoridad del poder ejecutivo para entrometerse en la vida privada de los estadounidenses ha cambiado drásticamente desde el 11 de septiembre. El fiscal general John Ashcroft levantó las restricciones que limitaban la supervisión del FBI de las organizaciones religiosas, cívicas o políticas nacionales. La Ley PATRIOTA redujo los estándares para búsquedas clandestinas, escuchas electrónicas y acceso secreto a registros de clientes e información personal. El ejecutivo ha iniciado una serie de proyectos de minería de datos diseñados para buscar en grandes cantidades de información personal, buscando patrones de comportamiento sospechoso. Estos cambios han suscitado temores de que los principios fundamentales de sospecha individualizada y presunta inocencia hayan sido reemplazados por una nueva normalidad de sospecha y vigilancia generalizadas.[60]

Retomamos entonces el "*cypherpunks write code*". Pese a que por aquel entonces ya existía *Freenet*, una tecnología de *software* libre presentada en el año 2000, que permite de forma anónima "compartir archivos, buscar y publicar *freesites* (sitios web accesibles sólo a través de Freenet) y hablar en foros, sin miedo a la censura"[61], la situación dio pie a la creación de al menos otras dos[62] tecnologías relevantes por parte de los *cypherpunk*, como contrarrespuesta

[58] Acrónimo de *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* Act ("Ley para unir y fortalecer América proveyendo las herramientas apropiadas, requeridas para impedir y obstaculizar el terrorismo").
[59] Amnesty International USA, 2010.
[60] Humans Rights First, 2003, p 15.
[61] The Freenet Project Inc., 2013.
[62] Cartografiar el total de las tecnologías implementadas resulta imposible por las limitaciones de espacio y tiempo, por lo que reseño los aportes con mayor adopción social.

a las medidas crecientes de monitorización de la ciudadanía en red. En 2003 nace I2P (acrónimo de "*Internet-to-Peer*"), "una capa de red privada completamente encriptada que ha sido desarrollada con privacidad y seguridad por diseño para brindar protección para su actividad, ubicación e identidad"[63], similar a la anterior pero con capacidad de integrar dentro de su potencial de anonimización cualquier servicio que pueda presentarse en la red abierta. Y, en 2006, Roger Dingledine y Nick Matheson inauguran *The Tor Project*, una asociación sin ánimo de lucro que se valerá del concepto de "enrutación cebolla" concebido en los 90 por David Goldschlag, Mike Reed y Paul Syverson, del *U.S. Naval Research Lab*[64], "que se preguntaron a ellos mismos si había una forma de crear conexiones de internet que no revelen quién habla con quién, incluso si hay alguien monitorizando la red"[65]:

> El objetivo del enrutamiento de cebolla era tener una forma de usar Internet con la mayor privacidad posible, y la idea era enrutar el tráfico a través de varios servidores y cifrarlo en cada paso del camino. Esta sigue siendo una explicación simple de cómo funciona Tor hoy.[66]

No obstante, el perfil técnico de los *cypherpunk* no parece facilitar la adopción de sus tecnologías por parte del público en general. Cuando hablamos de "encriptación", "PGP", "*onion routing*", etc., no podemos dar por sentado que el conocimiento del público general capacite a la sociedad para una aceptación masiva; la curva de aprendizaje es demasiado inclinada, el mensaje se envía desde un púlpito tecnófilo. Por eso, la adopción de las tecnologías criptográficas se ve condicionada por el activismo a su alrededor y por ell momento de oportunidad política en el que se invocan. Como reconocen los propios fundadores de *The Tor Project*:

> Tor comenzó a ganar popularidad entre los activistas y los usuarios expertos en tecnología interesados en la privacidad, pero todavía era difícil de usar para las personas con menos conocimientos técnicos, por lo que a partir de 2005 comenzó el

[63] I2P, 2019.
[64] Trad., "Laboratorio de Investigación Naval de los Estados Unidos".
[65] The Tor Project Inc., 2010.
[66] The Tor Project Inc., 2010.

desarrollo de herramientas más allá del proxy[67] Tor. El desarrollo de Tor Browser[68] comenzó en 2008.

Dado que Tor Browser hizo que Tor fuera más accesible para los activistas y usuarios de Internet, Tor fue una herramienta fundamental durante la Primavera Árabe que comenzó a finales de 2010. No solo protegió la identidad de las personas en línea, sino que también les permitió acceder a recursos críticos, redes sociales y sitios web. que estaban bloqueados.

La necesidad de herramientas de protección contra la vigilancia masiva se convirtió en una preocupación principal gracias a las revelaciones de [Edward] Snowden en 2013. Tor no solo fue fundamental para la denuncia de irregularidades de Snowden, sino que el contenido de los documentos también confirmó las garantías de que, en ese momento, Tor no podía ser descifrado.[69]

Imbricado en este contexto de celo por diferenciar a los emisarios de los receptores, nace WikiLeaks en ese mismo año; una organización que provee una ruta a través de la red TOR para que los soplones (*whistleblowers*) puedan filtrar información sensible sobre gobiernos y organizaciones. El cantidad de filtraciones de los años posteriores y la cuestionable acusación de abuso sexual contra su fundador, Julian Assange, hacen sospechar de las tensiones geopolíticas que la organización suscita; y que terminarán cobrándose con un Assange huido de la justicia y refugiado en la embajada de Ecuador en Reino Unido desde 2012, hasta que en 2019 las tensiones entre Estados Unidos, Ecuador y Reino Unido terminan por confinarlo en la prisión de Belmarsh (Londres).

Un destino similar le sucederá a Edward Snowden[70], quien pasó de trabajar como agente de inteligencia para la *Nacional Security Agency* estadounidense a revelar en 2013 que su país ocultaba los programas de vigilancia masiva PRISM y Keyscore, para terminar exiliado en Rusia bajo el amparo de Putin.

Como afirmón May, “el poder de la tecnología crea con frecuencia nuevas realidades políticas”[71]. Cuando hablamos de que los “*cypherpunks write code*”, no se refieren a la simple expresión de la implementación tecnológica, sino también a que “los *cypherpunk* le dan más

[67] Un *proxy* es un nodo intermediario entre dos nodos de una red cuya finalidad excede el mero enrutamiento de la información (por ejemplo, proveyendo credenciales, control de contenidos o anonimidad).
[68] Un “navegador web” que incluye la tecnología Tor, y que permite a los usuarios ignorar los pormenores de la configuración; basta con pulsar un botón para conectarse a internet a través de Tor.
[69] The Tor Project Inc., 2010.
[70] Serra, 2019.
[71] May, 1994, 3.4.1.

importancia al cambio factual de las cosas, a conseguir que el código funcional se distribuya, que a meramente hablar sobre cómo las cosas *deberían* ser"[72]. De vuelta a 2006, en relación con el desarrollo de internet y debido a la particular batalla jurídica que la industria discográfica practica contra los usuarios que comparten canciones en redes distribuidas como lo han sido Napster, Gnutella y BitTorrent, nace el Partido Pirata sueco, liderado por Rickard Falkvinge y fundado junto a los padres de *The Pirate Bay*, un *tracker* para archivos distribuidos en la red BitTorrent. Cuatro años más tarde, en 2010, los distintos Partidos Pirata nacionales se organizarán en una internacional en Bruselas. El Partido Pirata sueco llegará a colocar 2 diputados en el Parlamento Europeo, y el alemán contará con hasta 45 diputados nacionales y 199 concejales, entre otras victorias representativas[73]. Y su presencia será crucial para considerar en las agendas de Europa, el contexto internacional y los respectivos países con representación, el cuestionamiento de las propuestas legislativas que pretenden limitar la libertad en internet. Así, apoyada por una campaña masiva por parte de las plataformas de internet desde Wikipedia hasta Google, no fue posible aprobar la *Stop Online Piracy Act* ni la *PROTECT IP Act* en 2011, cuyo cometido era dar poder de acción a los poseedores de la propiedad intelectual para ejercer sus derechos de propiedad en internet, en detrimento de el libre albedrío de los internautas. Y confirmando lo dicho sobre la adopción de los postulados *cypherpunk* en función del momento de oportunidad política, cabe reseñar que el Partido Pirata sueco vio cómo su número de miembros aumentó de 15.000 a 37.000 entre el viernes 17 de abril, momento en el que se falló la una sentencia contra *The Pirate Bay* por motivos de *copyright*, y el miércoles siguiente[74].

Guiado por este mismo espíritu de anonimidad y distribución, en 2008, alguien con el pseudónimo de Satoshi Nakamoto envió a una lista de correo sobre criptografía en metzdowd.com un artículo titulado *Bitcoin: A Peer-to-Peer Electronic Cash System*[75]. Era la manifestación funcional del concepto de dinero electrónico y distribuido que ya se aventuraba en los 90.

Tal y como proponía Nakamoto en su artículo, la tecnología Bitcoin se definiría como "una versión puramente entre personas [*Peer-to-Peer*] de dinero electrónico [que] permitiría que los pagos se enviasen directamente de una parte a otra sin las cargas que implica hacerlo a través de una institución financiera"[76].

---

[72] May, 1994. 4.5.2.
[73] VV.AA., 2020
[74] Waters, 2009.
[75] Nakamoto, 2008, November 1.
[76] Nakamoto, S. (2008)

Sin desmerecer el haber sido la primera criptodivisa implementada, el aporte más relevante de Bitcoin fue dar con un sistema de certificación de transacciones entre iguales. Si el dinero avalado por los estados-nación lo está además por los bancos centrales en una relación de jerarquía, quienes permiten además a los bancos comerciales un entramado contable que consiste en traducir el dinero fiduciario en dinero anotado, y las relaciones de crédito o tenencia se ven afectadas por productos financieros, especulación y secretismo; la tecnología que propuso Bitcoin otorga la igualdad a cualquier tenedor: todos los actores tienen el mismo tipo de dinero, todos conocen las acciones de todos, ningún actor tiene más poder que otro para limitar el uso del dinero dentro de la red. En otras palabras, la implementación de Bitcoin no reinventa el dinero sino que inaugura el concepto de *blockchain*[77]: una cadena de bloques (u operaciones) con una naturaleza común, compartida por todos los miembros de una misma operativa.

Tras poco más de una década en funcionamiento, el surgimiento de criptodivisas no reguladas ha creado un ecosistema especulativo sobre el valor de estas, similar al mercado FOREX de monedas. A diferencia de la banca y la inversión tradicionales, estos sistemas son discretos (y con frecuencia anónimos), por lo que sirven a los especuladores como un contexto para sus prácticas alejadas del intervencionismo estatal. En este sentido, el mercado de criptodivisas representa una contraparte; donde antes teníamos estados de derecho gestionando sus monedas, ahora sumamos un entorno donde no hay más forma de gestionar el valor de las divisas que la propia homeostasis del sistema. Ambos escenarios parecen retroalimentarse, pues existen agentes de cambio que permiten comprar criptomonedas con dinero bancario y viceversa; y los indicios sugieren que los cambios sociales (en un contexto de crisis, por ejemplo) se reflejan en las valoraciones de cualquier divisa, independientemente de su naturaleza. Así, el mercado especulativo de las criptomonedas sirve de vía de escape al mercado regulado cuando sus condiciones estatales no son favorables, como el mercado regulado sirve de refugio de las inversiones cuando el entorno descentralizado se vuelve demasiado volátil. La Mano Invisible de Adam Smith estrecha la Mano del Estado a conveniencia, poniendo en jaque cualquier paradigma que abogue por decantarse por uno u otro modelo como solución última.

Sumando lo dicho, empiezan a materializarse desafíos frente a las agendas públicas de los gobiernos que exceden la capacidad de estos para perseguir el crimen. La presencia de una forma anónima de pago, sumada a la implementación de otras tecnologías como The

[77] Trad.: “cadena de bloques”.

Onion Router[78] y PGP, ha dado por finalizada la "Cruzada contra las drogas". Poco pueden hacer las fuerzas del orden si el tráfico se traslada de la calle a los domicilios, siendo el agente que traslada las sustancias un operario de correos y el volumen de correo tal que la inspección de todos los envíos se mantiene como un problema irresoluble. Los pedidos se tramitan dentro de mercados similares a Amazon, donde las plataformas retienen el dinero hasta que ambas partes (ofertante y demandante) quedan satisfechas, y donde los usuarios aún siendo anónimos ven sus avatares evaluados en términos de reputación. Tras un proceso que implica traducir dinero bancario a criptodivisas, conectarse a una red cifrada y comunicar la dirección de envío codificada con una llave criptográfica dispuesta por el vendedor, el consumidor recibe en su buzón un paquete sellado herméticamente, tratado contra perros antidroga, con unas condiciones sobre la pureza de la sustancia y unos precios que no encuentran equivalente en el mercadeo tradicional.

Más allá de la complicación técnica de las implementaciones, las distintas aplicaciones humanas del concepto de *blockchain* redefinen (y por tanto resignifican) las relaciones entre los actores de una red; mientras se mejoran los procesos y se hacen transparentes las funciones, los actores han de adaptar su efectividad a las exigencias colectivas, ahora compartidas como no lo eran antes. Y si hablamos de sistemas humanos, ello implica que los propios humanos se adapten al nuevo paradigma; en primera instancia, asumiendo que la imposición de una *blockchain* en sus mecanismos de acción obliga a asumir, axiomáticamente, esta tecnología como una nueva "institución cero" que replantea la forma de relacionarse con el medio.

> Así, en términos culturales, las "cadenas de bloques" han alterado la forma en la que entendemos y nos relacionamos con el dinero, han puesto en cuestión la idea de valor tras el dinero fiduciario (una de nuestras instituciones hegemónicas), ponen en jaque la relación de los estados para con sus ciudadanos y diluyen el poder de las instituciones económicas para gestionar las divisas, amplían las relaciones civiles amparadas por el secretismo, mejoran las garantías en entornos compartidos, y dan cabida a una gran cantidad de aplicaciones industriales que desafían los aspectos de la cultura empresarial que se apoyan en decisiones políticas (fenómeno que, seguramente, se cobre con una gestión más tecnocrática).[79]

[78] "El Enrutador Cebolla", que establece caminos de comunicación seguros entre pares, incluidos servidores cuya posición geográfica es desconocida.
[79] Para una explicación más detallada sobre el potencial del *blockchain*, remito al Anexo 1, del que se han extraído partes de esta disertación, incluida la resaltada.

En términos más llanos, la *Electronic Frontier Foundation*, en colaboración con *The Tor Project*, desarrollaron y distribuyen desde 2010 "HTTPS Everywhere"; un *plugin*[80] para navegador que insta a las páginas consultadas a establecer relaciones cifradas con el usuario bajo el protocolo seguro HTTPS que creó la *Netscape Communications Corporation*, padres del navegador web *Netscape*, en 1992.

Implementada sistemáticamente, frente a las tecnologías anteriormente mencionadas, el protocolo HTTPS sí que tiene una adopción mayoritaria por parte de internet. En 2017, el HTTPSWatch Project afirma que el 80% de los 40 sitios más visitados de internet disponen de HTTPS opcional (que "HTTPS Everywhere" exigirá) aunque solo el 35% lo tienen por defecto. Por otro lado, el ránking de Google sitúa el HTTPS como una tecnología por defecto en el 44% de los 100 sitios más populares.[81]

Llegados a este punto, nos queda por analizar el fenómeno que partirá de la aparición y connivencia de dos nuevos actores en red: los *smartphones* y la consolidación de las llamadas "redes sociales"; plataformas que, como ya aventuró van Dijk[82], tienden a confundir *conexión* (humana) y *conectividad* (técnica) para hacer negocio gracias a los metadatos.

La presentación del iPhone de Apple en 2007 populariza la idea de que una persona pueda estar permanentemente conectada a la red. Las aplicaciones se trasladan del escritorio al teléfono móvil, con ella las interacciones personales, y con la movilización social hacia este formato lo hacen también la industria cultural y la esfera política. Este proceso, de aparente trivial cambio de formato, acarreará cambios para la monitorización ciudadana sin precedentes, pues cualquier ciudadano empezará a llevar consigo un dispositivo capaz de geolocalizarlo, con un micrófono y cámaras equipadas; lo que creará un terreno fértil para aquellos que sepan correlacionar comercialmente estos metadatos.

Hasta el momento no hemos tratado la arquitectura de la red. En 1964, Paul Baran, quien trabajaba para el *RAND Institute*, definió un diagrama con tres modelos básicos de red: un paradigma *centralizado*, donde todos los clientes obedecen a un nodo coordinador que actúa como intermediario en todas las operaciones; un paradigma *distribuido*, donde no existe un centro definido y cada nodo se comunica con otros nodos de forma arbitraria; y un paradigma *descentralizado*, en el que ciertos nodos mejor conectados interactúan entre sí para trasladar la información entre otros nodos conectados a estos primeros pero no entre ellos.

Dicha consideración tiene consecuencias fundamentales para el epifenómeno social de la puesta en marcha de una red. Si bien los *cypherpunk* apuestan por modelos distribuidos, los

[80] Trad.: "módulo".
[81] Felt et al., 2017.
[82] Van Dijck, José, 2013.

medios convergentes pasan por un modelo descentralizado. Esta consideración tiene que ver con la *simetría de la red*; con el número promedio de conexiones por nodo. En una red simétrica, la distribución dibuja una campana de Gauss, donde todos los nodos tienen más o menos el mismo número de conexiones; mientras que, en una red asimétrica, un mínimo número de nodos concentran la mayoría de las conexiones.

Lo que pone en peligro el proyecto distribuido de los *cypherpunk* es precisamente que la red se estructure de forma asimétrica, dando poder a unos mínimos actores para delimitar el margen de acción de todos los demás. En estas *redes sin escala*[83] la diferencia de fuerzas entre actores resulta insoslayable, pues el poder de conectividad termina imposibilitando a los actores menores competir en igualdad de condiciones por la popularidad. No hay que olvidar que el poder de un actor en red viene determinado por su posición en la red (el número de conexiones) y la capacidad para satisfacer las necesidades de la red, no tanto por su ontología específica[84]. Dentro de una economía de mercado, donde el capitalismo tiende a la concentración de capital, esto tiene como consecuencia que gigantes como Google, Amazon o Facebook comiencen una escalada de adquisiciones que desdibuja el espíritu cooperativo y horizontal que encontramos en los años 80. En relación a *Amazon Web Services*, que ostenta "la mitad del negocio mundial de la nube"[85], y su indiscutible hegemonía, Peirano asegura que

> Ahora mismo, el 70 por ciento del tráfico de internet pasa por Tysons Corner, una nube tan opaca, infranqueable, indesglosable como una cámara acorazada que no solo se ocupa de conducir gran parte del tráfico sino que, para hacerlo, lo tiene que leer.[86]

En otras palabras, asistimos a un fenómeno en el que la configuración natural de internet da lugar a una industria que comienza a agregar metadatos en grandes conglomerados cibernéticos con muy pocos propietarios.

> Este sencillo mecanismo es el origen del ecosistema que los académicos, tecnólogos y analistas empiezan a llamar "Economía de la vigilancia", "capitalismo de plataformas", y "Feudalismo Digital".[87]

[83] Van Dijk, Jan, 2012, pp. 19-41.
[84] Jan Van Dijk, 2012, p. 36.
[85] Peirano, 2018, p. 116.
[86] Peirano, 2018, p. 80.
[87] Peirano, 2018, pp. 93-94.

En el caso de Jaron Lanier, él hablará de "servidores sirénicos"[88], por las sirenas de la mitología griega; nodos capaces de atraer la atención de todos los navegantes con la intención de, una vez atados por su propuesta, devorar sus metadatos para explotarlos comercialmente:

> El problema sobre el que estoy tratando es que una forma específica de digitalizar la economía y la actividad cultural reducirá en última instancia la economía mientras concentra la riqueza y el poder de nuevas maneras que no son sostenibles.
>
> [...]
>
> Un *Siren Server* ["Servidor Sirénico"], como me referiré a tal cosa, es un ordenador de la élite, o una colección de ordenadores coordinados, en una red. Se caracteriza por el narcisismo, la aversión hiperamplificada al riesgo, y la extrema asimetría de la información. Es el ganador en un concurso de todo-o-nada, e [involucra en] concursos menores de todo-o-nada a aquellos que interactúan con él.[89]

Teniendo en cuenta esta nueva configuración, no podemos obviar de qué forma los crecientes monopolios digitales le dieron un giro lingüístico al concepto de *libre* para dar paso a un modelo de negocio basado en el minado de datos que los usuarios ceden libremente:

> La palabra clave no era libre sino abierta: código abierto, cultura abierta, que es la cultura de internet. Esta filosofía fue la alfombra que se encontraron las empresas como Google y Apple y los nuevos "visionarios" del mundo de la cultura tecnológica, un grupo de evangelistas, consejeros y charlatanes capitaneados por el editor Tim O'Reilly y promocionados sin descanso por la revista *Wired*.[90]

Amparados por la participación desinteresada de los usuarios, que no vimos en la publicidad de los inicios de internet una barrera suficientemente significativa como para no adoptar tecnologías en red que se nos ofrecían gratis (GMail, Facebook, Twitter, etc.), estas empresas encontraron su modelo de negocio en la "modificación algorítmica de la conducta"[91]: a partir del minado de datos de los usuarios, que incluye seguirlos a lo largo de internet por medio de tecnologías como las *cookies*, que se crearon para mantener ciertos datos en el ordenador del

[88] Lanier, 2013.
[89] Lanier, 2013, pp. 53-55.
[90] Peirano, 2018, p. 162.
[91] Lanier, 2018, p. 2.

usuario en lugar de en el servidor, estas empresas construyen modelos conductuales de los usuarios y tratan de adelantarse a sus querencias, con tal de presentarles productos y servicios entre los contenidos que consumen gratis en los momentos en los que son más susceptibles de tomar la acción (comprar, suscribirse, etc.)

> Un experimento mental puede ayudar a exponer cómo de rara se ha vuelto nuestra situación. ¿Puedes imaginar que Wikipedia mostrase diferentes versiones de sus voces a cada persona en función de un perfil de datos secretos de cada persona? Los visitantes pro-Trump verían un artículo completamente diferente de aquél que se mostraría a la gente anti-Trump, pero no habría constancia de qué es diferente o por qué.[92]

Hasta el momento, queda claro que "el negocio no es venderles productos a los usuarios, sino vender los usuarios como productos a una industria hambrienta de atención"[93].

Al mismo tiempo, tanto Peirano como Lanier apuntan a la paradoja de que estas mismas tecnologías que privatizan su código mientras fagocitan los datos de los usuarios sin costear su uso fueron construidas con las tecnologías que el movimiento de *software* libre empezó a desarrollar en los 80[94] y aprovechando el código "abierto" que vino después. Y la propuesta corporativa tampoco fue más halagüeña: "este movimiento del *open software* ha fallado absolutamente en la misión de buscar apertura y transparencia en el código que ahora gobierna nuestras vidas"[95].

Y en su paroxismo, del mismo modo que los *cypherpunk* se cuestionaron los resultados de sus postulados e inscribieron bajo el concepto de "criptoanarquía" los resultados difíciles de prever, cabe preguntarse por los efectos epifenomenológicos de una red centralizada. En el espacio temporal que comprende la Administración Trump, a partir de 2016, empezamos a encontrar indicios de que *las redes multiplican la respuesta emocional frente a la información, previamente seleccionada por las plataformas hegemónicas, reforzando el miedo y polarizando a la sociedad*[96]. En el menor de los casos, hablamos del escándalo de Cambridge Analytica, una empresa que utilizó Facebook para construir arquetipos de personalidad y modelos predictivos capaces de alterar la intención de participación política de una masa de votantes

[92] Lanier, 2018, p. 75.
[93] Peirano, 20018, p. 212.
[94] Peirano, 2018, p. 166. Lanier, 2018, p. 95.
[95] Lanier, 2018, p. 95.
[96] Lanier, 2018, pp. 73-92.

mediante la promoción de tales o cuales contenidos, y que fue contratada por la administración Trump[97]; o la creación en esta y otras redes de grupos de activistas ficticios, enfrentados pero controlados por los mismos servicios de inteligencia rusos con el objetivo de incendiar a la sociedad estadounidense[98]. En el peor, sucesos que se cobran la vida de personas, cuando no la vinculación de la actividad en las redes a un proceso de limpieza étnica como el que sufrió recientemente Myanmar:

> Dos investigadores de la universidad de Warwick estudiaron 3.335 ataques contra refugiados en Alemania, analizando todas las variables acerca de las distintas comunidades donde ocurrieron: factores socioeconómicos, políticos, tamaño, demografía, distribución de periódicos, historial de manifestaciones, historial criminal. Encontraron que la única variable significativa era Facebook. Los inmigrantes sufren más ataques violentos en las ciudades donde hay más usuarios de Facebook.
> [...]
>
> Un oficial de la UNESCO confesó en el *MyanmarTimes* que los países que habían entrado en internet con una alfabetización mediática muy pobre y sin un programa previo de adaptación, eran particularmente susceptibles a las campañas de desinformación y odio. En el este de India, un falso rumor en WhatsApp sobre unos hombres extranjeros que secuestraban niños para vender sus órganos se saldó con al menos siete linchamientos. El mismo rumor llegó hasta México, donde un muchacho y su tío que habían ido a comprar material de construcción para terminar un pozo de cemento fueron golpeados y quemados vivos por una turba enfurecida en la localidad de Acatlán. Su agonía fue grabada en vídeo por la multitud. La escena se repitió la misma semana en otras localidades mexicanas; en Oaxaca lincharon a siete hombres, en Tula golpearon y quemaron a dos. El mismo fenómeno se repitió en Bogotá y en Ecuador.[99]

Hechas estas consideraciones, cerraremos este capítulo con las reflexiones de Lanier que cimentan los resultados de la relación entre *convergencia* y *distribución* a lo largo de tres décadas:

[97] Peirano, 2018, 223-290.
[98] Peirano, 2018, 223-290.
[99] Peirano, 2018, 262-263.

Irónicamente, la presión social y política de los *hippies* tecnológicos es lo que llevó a los emprendedores a enfocarse casi exclusivamente en modelos de negocio basados en anuncios cuando nació internet[100].

[...]

Lo que no consideramos fue que ciertas necesidades digitales fundamentales [que podrían haber sido implementadas en el corazón de cómo funciona internet,] como [un mecanismo de identidad personal, un lugar donde almacenar información persistente, una forma de enviar y recibir pagos, una forma de encontrar a la gente con la que tienes algo en común] nos llevaría a nuevas formas de monopolios debido a los efectos de la red y a los bloqueos [tecnológicos que suceden cuando una implementación pasada limita otra futura]. Les hicimos el trabajo más duro [a los monopolios. O mejor dicho,] nuestro idealismo libertario inicial resultó en gargantuescos monopsomios de datos [porque tú eres el producto, y ellos concentran la demanda].[101]

Análisis comparativo de momentos movimientos

Presentado el estado de la cuestión en sendos momentos históricos, es tiempo de compararlos para responder a nuestros dos interrogantes principales: *en qué medida se diferencian o retroalimentan los paradigmas convergente y distribuido*, y *en qué medida se consolidan los cypherpunks como una acción colectiva capaz de influir en las decisiones políticas sobre la configuración de internet*.

La primera cuestión, que dará pie a responder la segunda, arroja luz sobre una relación de interacción dialéctica constante, con frecuencia bidireccional.

Por el lado de los discursos, porque la génesis de los argumentos del movimiento *cypherpunk* no tienen sentido fuera de la lógica del miedo a un futuro definido por otros agentes; que como se ha explicitado implican instituciones económicas y políticas cuya estructura capital (y por ende su posibilidad de acción) es mucho mayor que la de unos cientos de activistas reunidos. Así, el discurso *cypherpunk* tiende a definir un futuro distópico, en función de cómo se perciben las instituciones presentes (“Gobiernos del Mundo Industrial, cansados gigantes de carne y acero”), donde una comunicación abierta da poder a los principales gestores de la información para fiscalizar y actuar contra los emisores. En este

[100] Lanier, 2018, p. 94.
[101] Lanier, 2018, p. 22.

caso, el *Manifiesto de Independencia del Ciberespacio* de Barlow es un ejemplo paradigmático de cómo un cambio legislativo suscita una reafirmación en los principios; del mismo modo que la lista de correo *cypherpunk*, el espacio gestacional del movimiento, se construye tras la disposición de la administración estadounidense para financiar a grandes empresas que desarrollen internet; y tras la presentación al público de una tecnología como la *Word Wide Web*, que pone a disposición de ambos frentes el potencial de crecer exponencialmente.

Por el lado de los medios, porque el desarrollo tecnológico de ambos frentes, *convergentes* y *distribuidos*, no se diferencia sino que se retroalimenta; la motivación de la acción personal de un *cypherpunk* pasa por construir herramientas en aras de defender su individualidad frente a un sistema cuya complejidad potencial puede ponerla en entredicho; mientras los resultados del trabajo agregado de los *cypherpunks* tienden a ser reciclados por instituciones convergentes con tal de construir nuevas tecnologías al servicio de estas mismas instituciones. De esta forma, el protocolo HTTPs es adoptado por todas las partes, dando por hecho que cierto grado de privacidad es un interés compartido, aunque la *convergencia* lo use para afianzar sus relaciones de poder (cómo acceden los usuarios a sus plataformas cerradas sin revelar las contraseñas a los dueños de soporte telecomunicativo). Por otro lado, *The Tor Project* se prevale de la investigación del *US Research Laboratory* para legar a la ciudadanía inteligencia operativa de grado militar; y, por extensión, esta tecnología es usada por los criptoanarquistas emergentes para vehicular mercados (como el de las drogas) a través de canales que exceden la capacidad de las mismas fuerzas del orden para hacer valer la ley. Del mismo modo, las plataformas convergentes emergentes reciclan el *free software* de dominio público para construir espacios de información cuyo código es secreto, traicionando los presupuestos de las licencias GPL de los años 80. Y en lo relativo a la tecnología *blockchain*, utilizada a través de los espacios encriptados para conducir transacciones que evaden al estado, descubrimos que el propio mercado financiero tradicional encuentra en esta tecnología una forma de potenciar su tendencia especulativa más allá de la regulación; transformando la idea de una divisa horizontal en un mercado de divisas especulativo (traduciendo el interés por el beneficio de la libertad por el interés en beneficio económico). Con lo dicho, tampoco podemos obviar que la adopción de las criptodivisas por parte de las instituciones monetarias es un hecho que cimenta la utilidad de las tecnologías propuestas por los *cypherpunk*, reafirmando sus presupuestos.

En relación a las instituciones, el fenómeno más llamativo es que las previsiones atemorizadas de los *cypherpunk* terminan por hacerse realidad. Décadas más tarde, asistimos a programas de monitorización de la ciudadanía instaurados por gobiernos y compañías

privadas, justificados en pro de nuestros intereses (cuando no por seguridad, lo son por entretenimiento y *conexión*). Mientras que, en paralelo, los *cypherpunk* instauran asociaciones como la *Free Software Foundation*, la *Electronic Frontier Foundation* y los Partidos Pirata como respuesta a los cambios tecnológicos y legislativos condicionados por la tendencia convergente, y cuyo objetivo velado pasa por limitar las aspiraciones de esta tendencia por hacerse con la hegemonía de la red ("En nombre del futuro, le pido al pasado que nos dejen en paz").

Y en el ámbito legislativo, pese a que las leyes actúen como facilitadoras exclusivas de los intereses de la industria (*Computing Communication Act*, *Ley Anticrimen 266*, *Telecommunications Reform Act*, *Patriot Act*, *Stop Online Piracy Act*, *PROTECT IP Act*), encontramos que tanto convergentes como distribuidos terminan rindiendo cuentas ante el poder judicial. Es el caso de Zimmerman, acusado de exportar tecnologías de encriptación a potencias extranjeras; como es el caso de Mark Zuckerberg, CEO de Facebook, conminado a declarar ante el Senado de los Estados Unidos en 2018 sobre el papel que su empresa tuvo en el escándalo de Cambridge Analytica, y el 17 de noviembre de 2020, ante la sospecha de que su plataforma afectó a las elecciones norteamericanas de 2016. No obstante, la proporción de la responsabilidad no guarda simetría con su impacto social; pues Julian Assange y Edward Snowden son vivos ejemplos de cómo sus acciones minoritarias terminan con el exilio, mientras Zuckerberg se limita a escudar su responsabilidad en la corporación que lo ampara.

Para la segunda cuestión (*en qué medida se consolidan los cypherpunks como una acción colectiva capaz de influir en las decisiones políticas sobre la configuración de internet*), debemos retomar el planteamiento de Bennett y Segerberg sobre las diferencias entre acción *conectiva* y acción *colectiva*.

Conforme pasan los años, asistimos a una evolución de un grupo de individuos que señalan un problema común y que se reúnen en torno a BBSs y una lista de correo. Tan pronto como en los años 80, sus acciones individuales ("*cypherpunks write code*") y sus discursos motivan la creación de asociaciones como la *Free Software Foundation* y la previsora *Electronic Frontier Foundation*; que ven un avance en sus propuestas de mutualización con el nacimiento del *World Wide Web Consortium* y la *Internet Engineering Task Force* de los años 90, para estallar en una miríada de "Partidos Pirata", *The Tor Project, WikiLeaks*, etc. en los prolegómenos del siglo XXI.

Frente a estos, unos incipientes Amazon (1994) y Google (1998) allanan el terreno corporativo para las empresas convergentes que vendrán más tarde, como lo serán Twitter

(2006) o Facebook (2004), mientras la *Open Source Initiative* les provee con la justificación necesaria para cerrar su código, a expensas de canibalizar el código y los discursos de la *Free Software Foundation*.

Hechas estas consideraciones, podemos afirmar que el movimiento *cypherpunk* progresa desde el estado embrionario de individuos aislados tomando acciones solitarias hacia la consolidación de instituciones cooperativas; lo que lo sitúa, como mínimo, en un estadio conectivo *con poder organizativo* de acuerdo al planteamiento de Bennett y Segerberg. Lejos queda la idea de "clicktivismo"; de "reducir la acción política a dar *likes* o a expresar desagrado en una pantalla [...] Ni votos ni movilización, solo acción individual delante de una pantalla"[102].

El aspecto más cuestionable es hasta qué punto dicho potencial conectivo escala hasta un paradigma de acción colectiva. Queda claro que las tecnologías *cypherpunk* no tienen una aceptación social masiva inmediata, sino que se establecen en función de los distintos momentos de oportunidad política, como si las crisis en torno a la privacidad dotasen de motivación a actores que hasta entonces no se habían posicionado. Cuando los ciudadanos que utilizan tecnologías relacionadas con los planteamientos distribuidos (como lo es la red BitTorrent de compartición de archivos a la que *The Pirate Bay* ayuda indexando los contenidos) ven sus usos amenazados, tienden a la afiliación política; de igual manera que los casos de Julian Assange y Edward Snowden proveen a perfiles de corte geopolítico con la consideración de que su *status quo* podría verse amenazado, y que por lo tanto hay que tomar acción con la intención de que ni gobiernos ni corporaciones se conviertan en tiranías capaces de someter a quienes dicen servir.

Con lo dicho, también nos queda claro que la tecnología no determina de manera necesaria la cultura ni la acción, sino que provee de herramientas que los individuos usarán y reinterpretarán en función de sus circunstancias.

Además, encontramos dos fallos que comete el movimiento *cypherpunk* cuando intenta conquistar la hegemonía de la esfera pública y ganarse el beneplácito de la ciudadanía. El primero tiene que ver con su tecnofilia, que impide la participación en el movimiento de las personas sin un perfil técnico en la medida en que éstas no son capaces de entender el problema que se les expone ni las soluciones propuestas. El segundo se vincula al momento en el que estos activistas descubren que han estado enfocando el *issue* de la privacidad desde una perspectiva alejada del lenguaje común; ya tras el nacimiento de las grandes plataformas, cuyo diseño y funcionalidad han atraído a una masa crítica de internautas, que quedarán vinculados a ellas por costumbre y facilidad y servirán como embajadores-prescriptores para

[102] Mansilla, 2015, p. 60.

los nuevos usuarios que se irán incorporando. En este sentido podemos invocar el contexto de *lock-in* tecnológico del que habla Lanier, para inferir que las adopciones tecnológicas pretéritas limitarán las opciones futuras, y esta es la tesitura en la que los *cypherpunk* han de hacer valer sus argumentos.

Pese a no tener un calado social tan amplio como las tecnologías convergentes (en la medida en que se popularizaron los *smartphones*, y buena parte de ellos lo hicieron con la tecnología privativa de Apple o con Android de Google, que de forma natural espía las acciones del usuario), no se puede obviar el calado político del movimiento. A pesar de que la legislación hasta la *Patriot Act* de 2001 parece servir a los intereses de políticos y corporaciones, el nuevo siglo se inaugura con una serie de victorias en el terreno parlamentario, que terminan con *la SOPA* y la *PIPA* en los Estados Unidos, además de condicionar la agenda del Parlamento Europeo en la medida en que pueden actuar los parlamentarios del Partido Pirata dentro de la cámara.

Y en el orden tecnológico, tampoco podemos ignorar la penetración de las tecnologías *cypherpunk* que, aún canibalizadas por los intereses del paradigma anterior, inauguran nuevos espacios comerciales y políticos a través de redes como TOR. Por ejemplos, tomaremos el caso de cómo la industria de las drogas se reinventa mediante la tecnología criptográfica, y de cómo *WikiLeaks* utiliza la misma "encriptación cebolla" para poner en jaque los secretos políticos de Estados Unidos, entre otros países. El concepto de *blockchain*, por su parte, nos abre a posibles implementaciones futuras que exceden nuestra capacidad de predecir con certeza otros cambios de paradigma similares; aunque, hasta el momento, esta tecnología ya está redefiniendo las formas en las que nos relacionamos en el ámbito económico (engendrando un mercado de divisas fuera del control de los estados-nación, dotando a las empresas de nuevas formas de fiscalizarse entre socios, dando lugar al nacimiento de nuevos modelos de negocio, etc.) Con esto, cabe plantearse si el próximo gran cambio de paradigma (con una escala equiparable a lo que supuso la popularización de los *smartphones* o la presencia de Google en nuestras vidas) estará del lado de los planteamientos *cypherpunk-distribuidos* en lugar de obrar en favor de la convergencia.

Expuestas estas últimas consideraciones, habida cuenta de que la creación de instituciones *cypherpunk* consigue doblegar los intereses de políticos y empresas, podemos afirmar que el movimiento consigue avanzar desde una acción meramente conectiva a una colectiva, aunque su acción política todavía no logra ser hegemónica.

Consideración final

Los *cypherpunk* fallaron al no evitar las consecuencias de la explotación programática de los datos en red una vez la red estuviese dispuesta. Así las cosas, la humanidad ha engendrado un sistema de información global cuyo modelo de negocio se fundamenta en 1. espiar a la ciudadanía para 2. predecir sus momentos de mayor susceptibilidad en la toma de acciones determinadas 3. con el objetivo de condicionar sus decisiones en términos socioeconómicos.

Esta "modificación algorítmica de la conducta"[103] lesa la presunción de veracidad que la deontología periodística exige a los medios de información, y esconde los criterios de noticiabilidad que informan a la esfera pública tras incuestionables decisiones mecánicas cuya intención no es informativa, sino comercial (o propagandística), y cuyos efectos son impredecibles en la medida en que los algoritmos no seleccionan por criterios cualitativos sino estadísticos; cuyo dogma es incentivar la participación, no contar la verdad. Tal criterio se ha pagado con problemas como un aumento de la polarización política, la confusión entre cantidad y pluralidad de medios y discursos, fallos en la evaluación de la relevancia personal en la esfera pública, asesinatos motivados por la ira y el presumible aumento del suicidio entre adolescentes[104]; si obviamos aquellos asuntos que se derivan de una pérdida de garantías civiles por parte de gobiernos y organizaciones ávidos por utilizar nuestros datos.

Los efectos indiciarios de los medios convergentes que monitorizan, perfilan y tratan de condicionar a los usuarios empiezan a ser patentes. Cuando unos pocos nodos toman el control de la red también imponen su criterio, trazando una frontera que divide a los actores entre dominantes y dominados. Mientras unos se arrogan el beneficio, que generan mediante la explotación de los datos gratuitos de los otros, y rehuyen la responsabilidad civil de las acciones de aquellos a quienes coordinan; los otros quedan a merced de una marisma de información que se presupone buenista, pero que les aboca a una esfera subjetiva de manipulación que nada tiene que ver con la bondad.

Hasta la fecha, las consecuencias de la hegemonía del paradigma convergente han sido más lesivas que las supuestas ínfulas dolosas que los propios criptoanarquistas confesaron al considerar sus propuestas. Si bien algunos de estos efectos perniciosos ya fueron vaticinados hace tres o cuatro décadas, otros tantos están por suceder y no han sido predecidos. Ante tal tesitura, tenemos hoy más motivos que ayer para considerar nuestra

[103] Lanier, 2014, 2018.
[104] Orlowski, 2020.

relación con la tecnología y qué modelo preferimos que impere: si el incierto caos igualitario de la criptoanarquía, o el manipulador orden de la convergencia.

Anexo: notas sobre *blockchain*

(Las siguientes consideraciones fueron entregadas como 2ª Prueba de Evaluación Continua para la asignatura Culturas políticas, ciudadanía y democracia: procesos de transformación, que tutoriza el Decano Dr. Benedicto Millán.)

La génesis de un factor diferencial

¿Cómo puede cambiar la sociedad a través de la tecnología? Implicados en una revolución de la conectividad sin precedentes antes del siglo XX, la pregunta se enfoca en cómo la redefinición de los protocolos de la red tecnológica pueden suscitar cambios en los protocolos de la red social[105] con la que interactúa.

En 1994, Timothy C. May, uno de los fundadores del movimiento *cypherpunk*, escribía en su *Cyphernomicon* —un compendio de notas sobre el porqué de la criptografía y su epifenómeno social, la criptoanarquía—:

> Algunos de nosotros creemos que diversas formas de criptografía fuerte causarán el declive del poder del estado, quizá incluso colapse con bastante rapidez. Creemos que la expansión en el ciberespacio, con comunicaciones seguras, dinero digital, anonimidad y pseudoanonimidad, y otras interacciones crypto-mediadas, cambiarán profundamente la naturaleza de las economías y las interacciones sociales.[106]

Nos encontramos en un momento crucial de la génesis de internet, en el que se discute sobre qué efectos de la conectividad en red terminarán siendo hegemónicos. En términos jurídicos, entre la *High Performance Computing Communication Act* de 1991, que liberó el desarrollo comercial de internet, y la *Telecommunications Act* de 1996, que liberalizó el mercado de las telecomunicaciones y relajó los límites de la propiedad cruzada de medios y canales de comunicación.

Es un momento en el que son palpables tanto el celo de los hackers por mantener internet en forma de espacio colaborativo como el celo empresarial por ganar relevancia comercial dentro del ecosistema emergente. Es en 1996 cuando John Perry Barlow publica su

[105] No confundir aquí una red entre personas (una *red social*) con una "Red Social", entendida como una plataforma dentro de internet que aloja perfiles de personas a las que pretenden conectar (*conectividad*) dentro de esa misma plataforma.
[106] May, 1994. 2.13.1

Declaración de independencia del ciberespacio[107], y alrededor del año 2000 cuando crece y estalla la "Burbuja Puntocom"[108]. Napster nacerá en 1999 como una propuesta descentralizada de consumo cultural, como "el primer sistema P2P para intercambio de archivos masivo[, y] la presión judicial [conseguirá] cerrar la plataforma [...] en 2002"[109]; mientras, Steve "Jobs se [convertirá] en el intermediario de dos enemigos mortales[, las discográficas y los internautas,] con una plataforma de música digital [...] completamente centralizada, cuantificada y registrada por Apple"[110].

Empezamos a percibir roces entre las partes implicadas, intuyendo dilemas en torno al derecho de autor, la propiedad privada, la privacidad, etcétera. Queda patente que el diseño de las soluciones informáticas influye y se relaciona con las instituciones humanas. Cabe preguntarse entonces, como hará Jaron Lanier[111], en qué medida los diseños tecnológicos condicionan el futuro de las sociedades en las que se implementan, y de qué forma las decisiones pretéritas de una sociedad respecto a su consumo de tecnología acotan sus opciones futuras (los bloqueos en las opciones futuras, que él llama *lock-ins*):

> Merece la pena intentar descubrir cuándo las filosofías nos limitan al software bloqueado [*locked-in*]. Por ejemplo, ¿la anonimidad generalizada o la pseudoanonimidad son algo bueno? Es una pregunta importante, porque las filosofías correspondientes sobre cómo los humanos pueden expresar el significado han estado tan arraigadas en los diseños de software entrelazados de Internet que es posible que no podamos deshacernos de ellos por completo, o incluso recordar que las cosas podrían haber sido diferentes.[112]

Parafraseando al letrado y ciberactivista Laurence Lessig, que "la arquitectura en el ciberespacio es la verdadera protectora de la expresión; constituye la *Primera Enmienda en el ciberespacio*"[113] y que, por lo tanto, desatender a cómo las relaciones humanas se redefinen a través de la tecnología es sinónimo de desatender los derechos civiles mismos; equivale dejar al arbitrio de los ingenieros el *ethos* de los ingenios.

---

[107] Barlow, 1996.
[108] El País. 2010, March 10.
[109] Peirano 2018, p. 149
[110] Peirano 2018, p. 168-169.
[111] Lanier, 2011, 2014, 2019.
[112] Lanier, 2011, p. 13.
[113] Peirano 2018, p. 152. Cit. Lessig, Laurence, *El Código 2.0*.

En este sentido, Eric Hughes ya acuñó en su *Manifiesto Cypherpunk* de 1993 el famoso lema "cypherpunks write code"[114]. Si bien se puede discutir que el vector tecnológico sea el único factor determinante de la propuesta de éxito de un movimiento, dada la capacidad de la tecnología pretérita para condicionar la futura, es indudable que construir las herramientas que potencialmente definirán el futuro es una propuesta coherente si el objetivo es un presente asegurado por las comunicaciones cifradas.

Llegados a este punto, cabe preguntarnos por las implementaciones técnicas que, en forma de contrarrespuesta a la tendencia centralizadora de internet, hayan tenido un calado cultural suficiente como para enmarcarse dentro de un cambio de paradigma.

Cuando hablamos de sistemas cifrados descentralizados, me refiero a sistemas de votación, consumo, expresión, almacenamiento, etcétera, distribuidos entre todos los usuarios de la red; en oposición a conglomerados de servidores con un propietario único al que los usuarios acuden demandando fracciones de sus datos. ¿Pero cómo puede tener calado social un proyecto tecnológico de descentralización de la información? Estas implementaciones son posibles, aunque deben compensar la pérdida de eficiencia con actores en red más activos y con mayor inteligencia operativa que las que encontraríamos en un paradigma centralizado, donde un único dueño de la información arbitra las demandas del resto de miembros. Como ha sido también el caso del estudio de las "redes neuronales", las limitaciones de conectividad en red y la capacidad de cómputo de los actores han supuesto una frontera técnica que hemos ido ampliando conforme la informática se ha desarrollado en las últimas tres décadas.

En su mismo manifiesto de 1994, pese a ser propositivo, May calificaba el dinero digital de "material exótico"[115]. Hablaba de un sistema de transmisión de valor sin bancos centrales ni nacionales; una tecnología construida sobre internet que permitiese a los poseedores de dicho dinero operar al margen de cualquier estado o institución. Pese a las limitaciones técnicas de las que era consciente, es un requerimiento que repite en exceso, llegando a clarificar que los "agentes y objetos dentro de un sistema informático seguramente necesiten seguridad, credenciales, robustez e incluso dinero digital para transacciones"[116]. Su compañero Hughes[117] también subrayó que "debemos juntarnos y crear sistemas que permitan que transacciones anónimas tengan lugar". En 1991, el ingeniero Phil Zimmermann ya había implementado y regalado al mundo la tecnología de encriptación PGP (*Pretty Good Privacy*), que supuso un cambio sin parangón en la comunicación entre dos puntos dentro de una red monitorizada, por

[114] Trad. inglés: "Los cypherpunk escriben código".
[115] May, 1994 5.4.1.
[116] May, 1994 6.8.1.
[117] Hughes, 1993.

lo que era esperable que sucesivas aportaciones se relacionasen con más victorias en pro de la privacidad.

Guiado por este espíritu de anonimidad y descentralización, en 2008, alguien con el pseudónimo de Satoshi Nakamoto envió a una lista de correo sobre criptografía en metzdowd.com un artículo titulado *Bitcoin: A Peer-to-Peer Electronic Cash System*[118].

Blockchain: el factor diferencial

Tal y como proponía Satoshi Nakamoto en su artículo, la tecnología Bitcoin se definiría como "una versión puramente entre personas [*Peer-to-Peer*] de dinero electrónico [que] permitiría que los pagos se enviasen directamente de una parte a otra sin las cargas que implica hacerlo a través de una institución financiera"[119].

Sin desmerecer el haber sido la primera criptodivisa implementada, el aporte más relevante de Bitcoin fue dar con un sistema de certificación de transacciones entre iguales. Si el dinero avalado por los estados-nación lo está además por los bancos centrales en una relación de jerarquía, quienes permiten además a los bancos comerciales un entramado contable que consiste en traducir el dinero fiduciario en dinero anotado, y las relaciones de crédito o tenencia se ven afectadas por productos financieros, especulación y secretismo; la tecnología que propuso Bitcoin otorga la igualdad a cualquier tenedor: todos los actores tienen el mismo tipo de dinero, todos conocen las acciones de todos, ningún actor tiene más poder que otro para limitar el uso del dinero dentro de la red. En otras palabras, la implementación de Bitcoin no reinventa el dinero sino que inaugura el concepto de *blockchain*: una cadena de bloques (u operaciones) con una naturaleza común, compartida por todos los miembros de una misma operativa.

En términos computacionales, "definimos una moneda electrónica como una cadena de firmas digitales"[120]. Dando por hecho que el patrón oro ya no representa el dinero impreso por un estado, podemos extrapolar que una criptodivisa no tiene por qué representar, tampoco, un activo material como podría ser un metal precioso. Los "bitcoins" propiamente señalados como monedas son cantidades acuñadas colectivamente a través de la actividad de algunos nodos que se comportan como "mineros" dentro de la red Bitcoin. De hecho, una cantidad dada de criptomonedas se relaciona con las llaves criptográficas que permiten anotar operaciones legítimas con dicha cantidad en el registro compartido; no con la tenencia de cierto volumen de

[118] Nakamoto, 2008, November 1.
[119] Nakamoto, S. (2008)
[120] Nakamoto, S. (2008), p. 2.

monedas en sí. Así, se puede entender una criptodivisa como una serie de registros compartidos confiables adscritos a una forma también confiable de alterarlos.

En esta tesitura, una "cadena de bloques" (o *blockchain*) implementada no se ve en la necesidad de servir a un fin monetario. Si bien Bitcoin y otras criptodivisas (Ripple, Litecoin, Monero, Dash, Dogecoin, etc.) han articulado su funcionamiento en torno a la idea de que cualquier actor en su sistema pueda fiscalizar las acciones del resto de actores, un *blockchain* no presupone como condición indispensable definir una divisa. Es, incluso, frecuente que las acciones se asocien a un mero *token*[121]; que o bien representa una acción puntual o bien señala a otro *blockchain* con otra divisa.

De esta forma, un *blockchain* se convierte en un objeto tecnológico cuya ontología es compartida y cuya teleología es testimonial; es compartido por todos sus poseedores y cada operación se anota para que todos los miembros de la red conozcan lo que así ha ocurrido. Cuestiona el *status quo* hasta el presente, porque hasta este momento no existía tal connivencia de fuerzas; capaces de colectivizar los hechos con protocolos estandarizados que publiciten la información mediante un soporte de datos descentralizado fuera del error humano. La postura es opuesta a la idea de centralizar la información en un servidor cerrado al público y servirla a conveniencia de los clientes que la demandan. En esta tesitura, cualquier poseedor ostenta una copia de todo lo acontecido y puede tomar la acción siempre que haya otros nodos en la red dispuestos a actuar como testigos; no hay acciones veladas para el resto de miembros; y los conflictos se resuelven mediante procesos, no mediante política.

Aplicaciones de *blockchains* y sus cambios de paradigma

Habiendo ya introducido la pugna entre centralización y descentralización en el desarrollo de internet; y dejando claro que la búsqueda de sistemas criptográficos frente a las amenazas de la centralización ha dado, entre otros frutos, con la tecnología *blockchain*, llega el momento de aventurar las posibles implementaciones de dicha tecnología y cómo estas pueden alterar las estructuras sociales que las adopten[122]. Volvemos a la pregunta sobre cómo puede cambiar la sociedad a través de la tecnología.

La primera respuesta a esta incógnita es más que evidente: el surgimiento de criptodivisas no reguladas ha creado un ecosistema especulativo sobre el valor de estas, similar al mercado FOREX de monedas. A diferencia de la banca y la inversión tradicionales, estos sistemas son discretos (y con frecuencia anónimos), por lo que sirven a los

[121] Trad. inglés: ficha, vale, testimonial.
[122] Rosic, 2017, March 7. Daley, 2018, December 5. Viens, 2019, November 5.

especuladores como un contexto para sus prácticas alejadas del intervencionismo estatal. En este sentido, el mercado de criptodivisas representa una contraparte; donde antes teníamos estados de derecho gestionando sus monedas, ahora sumamos un entorno donde no hay más forma de gestionar el valor de las divisas que la propia homeostasis del sistema. Ambos escenarios parecen retroalimentarse, pues existen agentes de cambio que permiten comprar criptomonedas con dinero bancario y viceversa; y los indicios sugieren que los cambios sociales (en un contexto de crisis, por ejemplo) se reflejan en las valoraciones de cualquier divisa, independientemente de su naturaleza. Así, el mercado especulativo de las criptomonedas sirve de vía de escape al mercado regulado cuando sus condiciones estatales no son favorables, como el mercado regulado sirve de refugio de las inversiones cuando el entorno descentralizado se vuelve demasiado volátil. La *Mano Invisible* de Adam Smith estrecha la Mano del Estado a conveniencia, poniendo en jaque cualquier paradigma que abogue por decantarse por uno u otro modelo como solución última.

En este sentido, también hay que considerar cómo afecta al individuo la tenencia y uso de una criptodivisa. En las socialdemocracias liberales, la Hacienda Pública tiene poder para conocer el secreto bancario y embargar las cuentas de la ciudadanía, con tal de garantizar el cobro de impuestos y de vehicular las disposiciones de la judicatura. Este entramado se sustenta en la cooperación de instituciones en distinto orden de jerarquía, desde los Poderes Públicos hasta los bancos comerciales, quienes han de acatar las demandas del estado. Si retomamos las ideas de que la criptodivisa se maneja a través de una llave cifrada (que no necesita adscribirse a un número de identificación fiscal) y que las transferencias no requieren de organismos oficiales que las certifiquen, podemos afirmar que el uso generalizado de una criptodivisa cuestiona el poder estatal para fiscalizar y actuar en materia económica. Si bien los impuestos se han podido considerar como un acto de voluntariedad frente a la sociedad en que se vive, no es menos cierto que el pacto de la socialdemocracia se ha sustentado en el control estatal más allá del mero monopolio de la violencia; también lo empodera la vigilancia. Con una ciudadanía cuyo valor monetario escapa de la capacidad del estado para cobrarse el impuesto adeudado, infiero que una adopción en masa de esta forma de dinero legaría el pago de tributos a la buena voluntad, poniendo en jaque el sostenimiento de todo el aparato construido con dinero público.

Hasta el momento, la presencia de una forma anónima de pago, sumada a la implementación de otras tecnologías como The Onion Router[123] y PGP, ha dado por finalizada

[123] "El Enrutador Cebolla", que establece caminos de comunicación seguros entre pares, incluidos servidores cuya posición geográfica es desconocida.

la “Cruzada contra las drogas”. Poco pueden hacer las fuerzas del orden si el tráfico se traslada de la calle a los domicilios, siendo el agente que traslada las sustancias un operario de correos y el volumen de correo tal que la inspección de todos los envíos se mantiene como un problema irresoluble. Los pedidos se tramitan dentro de mercados similares a Amazon, donde las plataformas retienen el dinero hasta que ambas partes (ofertante y demandante) quedan satisfechas, y donde los usuarios aún siendo anónimos ven sus avatares evaluados en términos de reputación. Tras un proceso que implica traducir dinero bancario a criptodivisas, conectarse a una red cifrada y comunicar la dirección de envío codificada con una llave criptográfica dispuesta por el vendedor, el consumidor recibe en su buzón un paquete sellado herméticamente, tratado contra perros antidroga, con unas condiciones sobre la pureza de la sustancia y unos precios que no encuentran equivalente en el mercadeo tradicional; donde el traficante no muestra referencias de otros compradores y la sustancia puede estar más adulterada.

Con lo dicho, quedan cubiertos tres fenómenos de cambio cultural sustanciales relacionados con la implementación de criptodivisas: la especulación financiera, la relación de contribución de la ciudadanía con el estado, y la reconfiguración del mercado de las drogas hacia un nuevo paradigma que escapa del estado. No obstante, como se ha dicho, el concepto de *blockchain* excede la idea de un mecanismo efectivo de intercambio de valor, extendiéndose hasta la consideración de la fiscalización colectiva de todas las acciones.

Uno de los aspectos más prometedores de las “cadenas de bloques” más allá de la divisa se refiere a los llamados *smart contracts*. Siguiendo nuestra herencia de Derecho Romano, hasta ahora los contratos se han firmado a mano, en cada página y por duplicado. Si bien este formalismo ofrecía garantías en épocas donde los medios de reproducción eran más limitados, hoy en día se puede falsificar una firma o alterar un folio con relativa facilidad. Un registro compartido de contratos elimina el problema de la duplicidad (lo que dice la copia de un contrato frente a lo que dice su supuesta copia en discordancia) mediante redundancia (la constancia del contrato es absoluta en todo el sistema), y cancela el riesgo de pérdida de copias por alguna de las partes. Además, un registro no requiere una equivalencia formal con un contrato; donde el documento ha de explicitar cuanto se firma, una cadena de bloques es dinámica y por lo tanto puede adoptar configuraciones más elásticas en términos jurídicos, como podría ser suscribir una cláusula por registro y valerse de nuevos registros para actualizar cláusulas.

Otra potencial aplicación del *blockchain* tiene que ver con los cuestionados sistemas de votación electrónica. Si el cómputo de los votos depende de que cada una de las terminales

haya transmitido la información a un ordenador central, previa comprobación de la identidad de los votantes por términos analógicos-humanos, el sistema queda a merced de la incertidumbre: ¿existe coincidencia entre la identidad declarada y las personas votantes? ¿Es el código de una máquina igual en todas las máquinas, o pudo adulterarse? ¿Existe algún agente intermedio en el proceso de transmisión capaz de alterar el voto? ¿Cómo puede un votante certificar que su voto se computó correctamente? Con un sistema distribuido de votación electrónica, todas las máquinas poseerían una parte o la totalidad del registro de los votos, siendo estos públicos, y el problema del secreto del voto se podría solventar mediante una clave criptográfica personal similar a las que ya expide la administración pública (y que podría estar inscrita en el DNIe).

Esta última idea, que parece relegar a la ciencia ficción la idea de que cada máquina de voto contenga los votos de todo un país (existiendo tantas copias de los votos como cabinas en colegios electorales), no es descabellada. Si cada voto se comprime en un registro de unos 5KB (5120 caracteres, aprox.), la voluntad de un país de cincuenta millones de personas cabe en menos de 240GB. En términos de España, con unas 50.000 mesas de votación[124], cada mesa sería responsable de la producción y transmisión de sólo unos 4.8MB de información, y la contabilización de los votos sería tan inmediata como el cierre de las votaciones. Aunque este proceder plantee otras dudas, como qué sistema impediría consultar el *blockchain* a tiempo real (un equivalente a las encuestas “a pie de urna”), un sistema de votación descentralizado evitaría los fraudes tales como una adición hartera y súbita de votos o los fallos en el conteo.

Otro ejemplo de implementación de *smart contracts* alejado del imaginario jurídico tradicional tiene que ver con cómo se podrían financiar los creadores de contenido. Actualmente, un creador de YouTube prevé sus ingresos en función de una fracción de los ingresos por publicidad que generen sus vídeos. Con tecnologías como el BAT (*Basic Attention Token*), que inscribe sus movimientos en el *blockchain* de Ethereum, la relación de fuerzas cambia; los usuarios reciben *tokens* cuando ven anuncios, los creadores reciben *tokens* cuando son vistos y los anunciantes pueden usar *tokens* para promocionarse, pudiendo ser estos tres roles ejercidos por una misma persona. Como citan en su *whitepaper*, BAT supone un sistema “basado en blockchain de anuncios digitales”, una manera de medir la atención e intercambiarla como un bien. Con esta propuesta, el negocio de internet pasa de ser bicameral (entre quienes se anuncian a través de creadores, y los usuarios que obtienen contenido a cambio de publicidad) a convertirse en una relación retroalimentada. En términos de equivalencia, ya no hay distinción entre una “inversión” en publicidad y decir que un vídeo “te gusta”. La naturaleza de la atención, se use como se use (para vender, como creador, como audiencia), es la misma

[124] Riestra, 2014, May 24.

y se representa por un activo común: “el bono básico de atención”. Y así las cosas, de cualquier acción, ya sea iniciar una campaña promocional o darle las gracias a un autor, queda fe pública de que sucedió en un registro donde cada firmante tiene una identidad que lo avala (potencialmente anónima, pero concreta). De este modo, se hace también difícil falsificar la actividad en red; pues las cifras son más confiables si no hay un único ente que las gestiona, y se pueden evitar casos como que Facebook mintiese a sus anunciantes sobre el número de visitas de los vídeos subidos a su plataforma[125].

Este paradigma cercena los últimos veinte años de comercio en red. En oposición, los nodos centralizadores (a saber, Facebook, Amazon y Google en mayoría) han construido un negocio que se basa en monitorizar la actividad de los usuarios para venderles bienes y servicios en sus momentos más vulnerables. En el caso de las “redes sociales” y Google, el negocio pasa directamente por alterar el flujo de informaciones para manipular su voluntad. Como explica van Dijk[126]:

> Tal vez irónicamente, mercantilizar las relaciones sociales —convertir *conexión* [humana] en *conectividad* mediante las tecnologías de programación— es exactamente lo que las plataformas corporativas, particularmente Google y Facebook, descubrieron como el huevo dorado que su ganso había producido. Además de generar contenido, la producción colectiva genera un sub-producto que los usuarios no dan intencionadamente: datos conductuales y para perfiles.

En este modelo el dinero solo fluye en una dirección (de anunciantes a plataformas), esperando que se recupere la inversión fuera del canal de promoción. Con la propuesta del BAT, son los propios espectadores quienes costean la atención, poniéndose al nivel de los anunciantes y desoyendo a los intermediarios, obligando a las plataformas a replantear la diferencia entre quienes consumen el contenido y quienes lo costean, y a decidir su lugar dentro del nuevo paradigma. Es más; el hecho de que la atención sea tomada como referencia clave del valor de las interacciones, en lugar de serlo el dinero prometido a través de la esperada atención, constituye un incentivo para los creadores; que ven sus actos recompensados por un valor directo, no subsidiario de otro. Aunque, con lo dicho, hay que considerar también que la hegemonía la ostentan todavía las plataformas centralizadas, y que este modelo no se ha

[125] Moore, 2016, September 23.
[126] van Dijk, 2013. La cursiva es mía.

impuesto, entre otras razones porque en la especificación técnica de internet no se consideró un sistema de remuneración bidireccional desde su inicio (Lanier 2011).

Un sistema parecido es Mediachain, adquirido por Spotify en 2017, que utiliza una tecnología de contratos transparentes y descentralizados con tal de garantizar mayores ingresos para músicos, que además de poder tener una idea clara del contexto en el que firman también ven agilizados los medios de pago. Parece que una industria discográfica circunscrita a los despachos y los cazatalentos, a la idea de "firmar" con una discográfica, es demasiado ineficiente a la hora de gestionar un catálogo de artistas a escala mundial en la sociedad red (en términos de Castells[127], aquella sociedad "cuya estructura social está compuesta de redes potenciadas por tecnologías de la información y de la comunicación basadas en la microelectrónica.").

En otro orden de cosas, debemos considerar el impacto de las tecnologías *blockchain* en contextos donde las acciones de terceras partes deben ser monitorizadas. Es el caso de la industria de seguros, el transporte de mercancías y los dispositivos conectados a internet (*Internet of Things*). En cualquiera de estos escenarios, existen personas interesadas en que otros actores de su red circunscriban su conducta a unas limitaciones de naturaleza funcional o contractual que pueda ser revisada.

Si una agencia de seguros es capaz de certificar las acciones que sus asegurados han hecho públicas en un *blockchain* común, tanto las aseguradoras como los asegurados aumentan sus garantías contractuales y, en el caso de las aseguradoras, se protegen contra el fraude. Una implementación de tal magnitud podría considerar, por ejemplo, que la maquinaria de ciertas industrias comunicase por red cada una de las acciones de sus operadores, de la misma forma que Facebook o Google recopilan información cuando sus usuarios aprietan botones. Una monitorización técnica de todos los riesgos activos y de las acciones que se tomaron permite reconstruir los eventos con mayor certidumbre que la que ofrece un mero testimonio, o incluso una grabación.

Del mismo modo, un *blockchain* puede fiscalizar las acciones de aparatos más pequeños, y no necesita ser compartido fuera de la red de estos aparatos. Pongamos, por caso, una solución domótica donde cualquier dispositivo (persianas, electrodomésticos, puertas, cámaras, telefonillo, etc.) compartan en su red local las acciones que ejecutan. Esto crea una *interfaz* común sin duplicidades, que no depende de la relación de todos con todos sino de todos con un registro compartido. Así, los dispositivos podrían compartir recursos entre sí: encender el calentador cuando se abra la puerta pasadas las ocho de la tarde, pasar el

[127] Castells, 2011, p. 27

robot aspiradora cuando la alarma no detecta movimiento, utilizar la televisión como disuasión si se ha abierto la puerta de la casa pero no la del portal, etc. La información de cada aparato se guardaría en los demás y su comportamiento sería homeostático, sin depender de un coordinador central como puede ser el teléfono móvil (en el caso de altavoces, iluminantes, etc. controlados por BlueTooth), lo que añade una pátina de seguridad en la medida en que la red domótica se autogestionaría y no necesitaría conectar los dispositivos directamente a internet; y, en el caso de hacerlo, podría mediar otro dispositivo como el teléfono para inscribir órdenes en el *blockchain* en lugar de dejar los dispositivos enteros a merced de quien los encuentre. Sería como dejar en casa una lista de recados, y que los aparatos que reconocen tu letra le hiciesen caso conforme se ven capacitados. La alternativa, menos halagüeña, pasa porque cada dispositivo se establezca en la red como un nodo abierto susceptible de ser conectado desde cualquier parte del mundo, sin que las acciones que se le comandan queden inscritas, pudiendo así convertir dispositivos como una cámara en el dormitorio infantil en una herramienta al servicio de actores ilícitos. Si tal cámara transmitiese información cifrada sólo al dispositivo con una llave de cifrado válida, un potencial ladrón necesitaría antes hacerse con el teléfono móvil del atacado y deducir sus contraseñas; hoy en día, los “Google dorks” son instrucciones que se le pueden pasar a Google para descubrir cámaras privadas convertidas en públicas por estar mal configuradas.

A su vez, el comercio internacional puede beneficiarse enormemente de las “cadenas de bloques”. Asumamos la inherente complejidad en el entramado de empresas, bienes y transportes a nivel mundial. Hablamos de millones de cargas con infinidad de subproductos dentro, con distintas naturalezas (como por ejemplo, si son perecederos o no), que deben circular por multitud de actores entre sus puntos de origen y destino. Un *blockchain* aplicado a las exportaciones permitiría un seguimiento público de los contenedores, haciendo más fácil localizar extravíos, así como computar almacenamientos compartidos. Un aumento considerable de la trazabilidad significa un aumento considerable de la certidumbre, acrecentada aún más si consideramos que las malas prácticas de algunos comerciantes quedarán a la vista de sus socios. En un contexto definido por diversos idiomas, culturas políticas y empresariales, y agendas secretas, canalizar dichas transacciones en un registro común contrarresta la entropía del sistema.

En cuanto a la censura, los *blockchains* tienen un papel tan protagónico en el movimiento *cypherpunk* como la “encriptación cebolla” de la red TOR. Por una parte hablamos de evitar el borrado de ciertas informaciones, mientras que el otro trata la privacidad de quienes manejan dichas informaciones. Si hablar de TOR significa considerar que cada intermediario

entre dos ordenadores añadirá una capa de cifrado al mensaje con tal de ocultar los orígenes de los emisores, una "cadena de bloques" soluciona el problema inverso de este tipo de sistemas: la persistencia. Las tecnologías de cifrado han inaugurado formas de ocultar la información, pero a menudo obvian formas de que no se olvide nunca.

A tal fin, implementaciones como el IPFS (*InterPlanetary File System*) permiten subir archivos a un registro compartido, de forma que ciertos nodos puedan copiar la información y hacerla redundante, en una estructura creciente donde cada vez es más difícil hacer desaparecer algo. Los intentos de censura en dicha red sólo pueden tener dos consecuencias: el olvido de la información, o el "efecto Streisand"; ver la difusión de la información amplificada por los intentos de censura.

Con un sistema de tablas distribuidas, IPFS permite a los usuarios consultar las referencias a otros archivos, e incluso utilizar esas referencias para asociar los datos a otras plataformas que también se valen de tecnologías *blockchain*. Apoyado en otra "cadena de bloques" como Steem, que se define como "un blockchain social que hace crecer comunidades y hace posible el flujo inmediato de reventas para usuarios por premiarlos al compartir contenido", la plataforma D.Tube se postula como la antítesis de YouTube: un sistema de *streaming* de vídeo sin publicidad, curado por la comunidad, regulado por sus propias divisas (DTC ó DTube Coin, y el VP ó Voting Power), y cuyos servidores están sostenidos por miembros participantes. El valor monetario creado al participar se puede cambiar por dinero bancario, cuando no almacenarlo para generar "Voting Power" (poder de participación) o "destruirlo" oficialmente para canjearlo por promoción dentro de la red. La suma de estos factores crea un sentido de comunidad *junto a* la plataforma, en lugar de *frente a*; desdibujando la idea paternalista de que un usuario se adscribe a una serie de términos legales estipulados por un servidor monolítico e inhumano.

Al contrario que en el "internet de las plataformas", estos modelos distribuidos exigen consigo *compartir*, por lo que la cultura de las empresas y sus usuarios tiende a volverse más altruista. Uno de los primeros ejemplos lo encontramos en las redes de compartición de archivos P2P sin *blockchain*, como pueden ser las redes GNutella y Bittorrent, en las que compartir se volvía un requisito moral, evaluado por el ratio entre la información enviada y la descargada. Una red centralizada se puede mantener mientras se mantengan suficientes conexiones entre el servidor y los usuarios como para mantener los costes del servidor, mientras que una red descentralizada exige del compromiso participativo de sus integrantes, pues son a la vez usuarios y proveedores.

Como último ejemplo, conviene tratar los procesos industriales y su cadena de valor. Pese a que en el sector servicios resulte, con frecuencia, difícil ponderar el valor de las acciones específicas de las empresas, los sectores primario y secundario se regulan por firmes indicadores de eficiencia (en inglés, *Key Performance Indicators*): el volumen de materia prima obtenida o convertida, el porcentaje de materia prima perdida en el proceso, los distintos procesos de construcción de las distintas piezas, el ensamblaje, el almacenado, los costes de estructura, etc. Por lo tanto, los procesos industriales son susceptibles de ser fiscalizados al completo dentro de una estructura que refleje cómo se construye el valor desde la obtención de los recursos para un objetivo y la consecución del objetivo.

De puertas para adentro, ello supone que cualquier empresa deje de depender de un ERP (*Enterprise Resource Planner*) centralizado y lo distribuya. En términos prácticos, la empresa que decida monitorizar sus procesos mediante una "cadena de bloques", en lugar de mediante un servidor central, se libera de que un único actor (la empresa que instaló su ERP) sea la estructura que aloja toda la inteligencia de negocio. Ello se traduce en una mayor facilidad para implementar innovación dentro de la compañía, en la medida en que cualquier tecnología ha de adaptarse a un sistema consensuado de código libre, con protocolos compartidos, en lugar de necesitar adaptar las máquinas a un ERP que podría convertirse más adelante en una limitación debido a su naturaleza privada. Y en otro orden, también permitiría poner en un mismo espacio todos los indicadores estratégicos, lo que facilitaría la correlación de datos con el fin de tomar decisiones. En suma, la empresa pasa a ser dueña de su inteligencia de negocio y a poder poner en común todos sus subsistemas, con el consiguiente ahorro.

Aunque el mayor valor de la tecnología *blockchain* aplicada a la industria se encuentra en considerar el proceso industrial como la suma de la actividad de varias empresas cuyos procesos están interconectados. Los vicios que pueden aparecer en cualquier sector son infinidad: proveedores que no proveen, subcontratas con laxos controles, ahorro en las calidades, utilización conjunta de tecnologías que no se pensaron para trabajar juntas, amaños contables, impagos, accidentes, etc. Pero si un sector en su conjunto decide compartir la información del proceso que enriquece a todos, una importante cantidad de estos vicios desaparece.

Pongamos, por caso conocido, el de la industria tintométrica; donde hay una disparidad de opciones entre bases para pintura, pigmentos y máquinas. Con frecuencia, algunos tenedores de máquinas que venden pintura al público deciden utilizar pigmentos más económicos que pueden hacer fallar la máquina. Al tiempo, quienes proveen el *software* que

opera las máquinas también comercializan los pigmentos más caros. El conflicto surge cuando un vendedor al por menor que intentó ahorrar en los pigmentos pretende que el proveedor de pigmentos al que no le compró le solucione el problema; en algunas ocasiones es un defecto de la máquina, cuando en otras tiene que ver con que la licencia del programa informático con las fórmulas químicas expiró. Sea cual sea el origen del conflicto, el caso es que ambas partes sostienen versiones distintas sobre un acuerdo de negocio definido por elementos claros: máquinas, contratos, pigmentos, *software*.

Si el destino de cada partida de pigmento y pintura base fuese anotado entre los socios comerciales en un registro compartido, al tiempo que cada máquina de pinturas inscribiese en el mismo *blockchain* cada vez que hace pintura, el proceso sería diáfano para todas las partes. Sería posible inspeccionar la "cadena de bloques", escrutar paso por paso cómo un material ha sido extraído, transportado, tratado, vuelto a transportar, comercializado, recibido, mezclado, etc. No habría forma de intentar convencer a nadie de lo que debió pasar, porque cualquiera podría encontrar un conflicto de intereses inspeccionando las relaciones desde las materias primas hasta el consumidor final. Si una máquina falla y en una parte anterior del *blockchain* no existen registro de que se cargaron pigmentos legítimos, se puede aducir que se usaron materiales sin garantía; si el *software* expira y en el *blockchain* no hay huella de que se hayan usado los pigmentos de quien comercializa dicho *software*, no hay razón empírica que defienda que las licencias se han de renovar.

Sumado a este aumento de la transparencia y por ende de las garantías, cabe la posibilidad de concebir (ahora sí) cada una de esas acciones comunalizadas como la certificación de que se está creando *valor*, en términos monetarios. De esta forma, una empresa del sector primario o secundario podría acuñar una criptodivisa en paralelo a cada acción comercial. Este *token*, en lugar de medir la atención como el BAT o generar monedas resolviendo bloques de cómputo como Bitcoin, reflejaría la actividad industrial; y a mayor actividad, mayor potencial de generar valor, y más moneda creada. Y esta divisa, paralela a la actividad de su sector, podría usarse tanto como un valor especulativo dentro del mercado de las criptodivisas como una alternativa a concertar contratos con dinero bancario (esto es, que las empresas implicadas en procesos similares costearan sus acuerdos con la moneda que ellos mismos generan, cuyo valor se genera bajo criterios previamente consensuados, no arbitrarios).

Y en otra vuelta de tuerca, aún habría espacio para que la venta de las criptodivisas que estas empresas generasen pudiese servir para obtener capitalización en dinero bancario, con el objetivo de reinvertirlo en I+D.

Conclusiones sobre la cultura

Al margen de las merecidas consideraciones jurídicas, económicas y técnicas, la finalidad de lo expuesto es tratar los efectos culturales de las tecnologías *blockchain*.

Con lo dicho, cabe añadir que el planteamiento de las “cadenas de bloques” sigue siendo reconsiderado, por lo que no podemos asumir que sus efectos estén asentados. Con todo, sus distintas aplicaciones sugieren que los cambios sucederán en plural y en distintas áreas; no como un cambio unívoco de paradigma sino como una suma emergente de soluciones más eficientes, que irá modificando las relaciones en la medida en que compartir información las modifique.

Lo que queda claro es que, más allá de la complicación técnica de las implementaciones, las distintas aplicaciones humanas del concepto redefinen (y por tanto resignifican) las relaciones entre los actores de una red; mientras se mejoran los procesos y se hacen transparentes las funciones, los actores han de adaptar su efectividad a las exigencias colectivas, ahora compartidas como no lo eran antes. Y si hablamos de sistemas humanos, ello implica que los propios humanos se adapten al nuevo paradigma; en primera instancia, asumiendo que la imposición de una *blockchain* en sus mecanismos de acción obliga a asumir, axiomáticamente, esta tecnología como una nueva “institución cero” que replantea la forma de relacionarse con el medio.

Así, en términos culturales, las “cadenas de bloques” han alterado la forma en la que entendemos y nos relacionamos con el dinero, han puesto en cuestión la idea de valor tras el dinero fiduciario (una de nuestras instituciones hegemónicas), ponen en jaque la relación de los estados para con sus ciudadanos y diluyen el poder de las instituciones económicas para gestionar las divisas, amplían las relaciones civiles amparadas por el secretismo, mejoran las garantías en entornos compartidos, y dan cabida a una gran cantidad de aplicaciones industriales que desafían los aspectos de la cultura empresarial que se apoyan en decisiones políticas (fenómeno que, seguramente, se cobre con una gestión más tecnocrática).

En resumidas cuentas, la aparición de las tecnologías *blockchain* mejora las relaciones humanas en términos de transparencia y garantías.

Y por todo lo dicho, es preciso que nos cuestionemos como civilización el papel protagónico de la tecnología en la determinación de la naturaleza humana; dónde trazamos la frontera entre ser servidos y servir. Como propuesta, la visión crítica y el espíritu constructivo de Lanier (2014, p. 306-307, 362):

La actitud hacker suele ser algo así: “abrid vuestras vidas a la ‘net, vosotros gente ordinaria. El mundo está a punto de volverse transparente y la transparencia será el inicio de una era dorada. Compartir es bueno. *No obstante*, encripta tu vida como un loco. Una VPN, etc. Solo la gente más lista puede ser silenciosa en el bosque digital.”

Esta es básicamente una forma de decir que cuanto mayor sea tu habilidad con ordenadores, más derecho tienes de ser un individuo genuinamente en control de su propia vida. Pero nosotros los tecnologistas tenemos el deber de ayudar a la humanidad, en lugar de convertirnos en una clase privilegiada.

[...]

Conforme la tecnología mejora, la economía tendrá que volverse menos abstracta. La Economía solía tratar acerca de los patrones de resultados que emergían de reglas que influenciaban el comportamiento humano en sociedad. Se enfocaba en la forma en la que las políticas engendraban resultados.

Pero cada año que pasa la economía debe enfocarse más y más en tratar el diseño de máquinas que medien en la conducta humana. Un sistema de información guía a la gente de forma más directa, detallada y literal que las políticas. Otra forma de verlo es que la economía debería convertirse en una versión a gran escala, sistémica, del diseño de interfaces de usuario.

Fuentes

Amnesty International USA. (2010, June 15). *Civil Rights And The "War on Terror."* Web.Archive.org; Archieve.org. https://web.archive.org/web/20100615050209/http://www.amnestyusa.org/war-on-terror/civil-rights/page.do?id=1108209
El artículo ha sido rescatado del repositorio de internet Archieve.org, cuyo objetivo es velar porque no se pierda la internet del pasado.

Ashby, W. R. (1956). *An introduction to cybernetics*. Chapman & Hall.

Bennett, W. L., & Segerberg, A. (2012). THE LOGIC OF CONNECTIVE ACTION. *Information, Communication & Society*, *15*(5), 739–768. https://doi.org/10.1080/1369118x.2012.670661

Bradner, S. (1999, March 29). *Open Sources: Voices from the Open Source Revolution*. O'Reilly. https://www.oreilly.com/openbook/opensources/book/ietf.html

Castells, M. (2011). A Network Theory of Power. *International Journal of Communication*, *5*, 773–787.

Castells, M., & Francisco Muñoz Bustillo. (2011). *La sociedad red : una visión global*. Alianza.

cryptoanarchy.wiki. (n.d.). *What is the Cypherpunks Mailing List?* Cryptoanarchy.Wiki. Retrieved December 23, 2020, from https://cryptoanarchy.wiki/getting-started/what-is-the-cypherpunks-mailing-list

Daley, S. (2018, December 5). *25 blockchain applications & real-world use cases disrupting the status quo*. Built In. https://builtin.com/blockchain/blockchain-applications

Dijk, V. (2006). *The network society*. Sage Publications.

EFF. (2007, July 10). *About EFF*. Electronic Frontier Foundation. https://www.eff.org/about

El País. (2010, March 10). Reportaje | El día que la burbuja "puntocom" pinchó. *El País*. https://elpais.com/economia/2010/03/10/actualidad/1268209975_850215.html

Felt, A., Barnes, R., King, A., Palmer, C., Bentzel, C., & Tabriz, P. (2017). *Measuring HTTPS Adoption on the Web Measuring HTTPS Adoption on the Web*. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-felt.pdf
Parte de los documentos del "26th USENIX Security Symposium", del 16-18 de Agosto de 2017 en Vancouver (Canadá).

Free Software Foundation, Inc. (2016). *The GNU General Public License v3.0- GNU Project - Free Software Foundation*. Gnu.org. https://www.gnu.org/licenses/gpl-3.0.html

Funes Rivas, M. J. (2019). La dimensión individual de la acción colectiva. Activistas por la solidaridad y los derechos humanos. In M. J. Funes Rivas & R. Adell Argilés (Eds.), *Movimientos sociales: cambio social y participación* (pp. 225–254). UNED.

Humans Rights First. (2003, August). *Assessing the New Normal: Liberty and Security for the Post-September 11 United States*. Human Rights First.

https://www.humanrightsfirst.org/resource/assessing-new-normal-liberty-and-security-post-september-11-united-states

I2P. (2019). *Intro - I2P*. Geti2p.net. https://geti2p.net/en/about/intro

IETF. (n.d.). *About*. IETF. https://ietf.org/about/

Jan Van Dijk. (2012). *The network society*. Sage Publications Ltd.

Janet Horowitz Murray, & Press, M. (2017). *Hamlet on the holodeck : the future of narrative in cyberspace*. The Mit Press.

Jaron Lanier. (2011). *You are not a gadget a manifesto.* London [Etc.] Penguin Books.

Jaron Lanier. (2013). *Who owns the future?* Simon & Schuster.

Jaron Lanier. (2018). *Ten Arguments for Deleting Your Social Media Accounts Right Now.* Random House Uk.

Jenkins, H. (2008). *Convergence culture : la cultura de la convergencia de los medios de comunicación*. Paidós.

José María Lassalle Ruiz. (2019). *Ciberleviatán : el colapso de la democracia liberal frente a la revolución digital*. Arpa.

Lanier, J. (2014). *Who owns the future?* Simon & Schuster Paperback.

Levy, S. (2001). *Crypto : how the code rebels beat the government, saving privacy in the digital age*. Viking.

Levy, S. (2010). *Hackers : heroes of the computer revolution : 25th Anniversary Edition*. O'reilly.

Mitnick, K. D. (2019). *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*. Little, Brown & Company.

Moore, M. (2016, September 23). *Facebook has been lying about some VERY important statistics*. Express.co.uk. https://www.express.co.uk/life-style/science-technology/713624/facebook-lying-video-view-statistics-advertising-figures-discrepancy

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://satoshinakamoto.me/bitcoin-draft.pdf

Nakamoto, S. (2008, November 1). *Bitcoin P2P e-cash paper*. Www.Mail-Archive.com. https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

Orlowski, J. (Director). (2020). *The Social Dilemma*. Netflix Inc.

PAÍS, E. (2010, March 10). Reportaje | El día que la burbuja "puntocom" pinchó. *El País*. https://elpais.com/economia/2010/03/10/actualidad/1268209975_850215.html

Peirano, M. (2019). *El enemigo conoce el sistema : manipulación de ideas, personas e influencias después de la economía de la atención*. Debate.

Postman, N. (2007). *Amusing ourselves to death : public discourse in the age of showbusiness*. Methuen.

Riestra, L. (2014, May 24). *Lo que debes saber del día de la votación en España*. ABC. https://www.abc.es/elecciones-europeas/20140525/abci-elecciones-europeas-espana-201405241626.html

Rosenblueth, A., Wiener, N., & Bigelow, J. (1943). Behavior, Purpose and Teleology. *Philosophy of Science*, *10*(1), 18–24. https://doi.org/10.1086/286788

Rosic, A. (2017, March 7). *17 Blockchain Applications That Are Transforming Society*. Blockgeeks. https://blockgeeks.com/guides/blockchain-applications/

Serra, A. (2019, April 20). *El caso Snowden: historia del genio cyber que traicionó a su patria y huyó a Rusia protegido por Putin*. Infobae. https://www.infobae.com/america/mundo/2019/04/20/el-caso-snowden-historia-del-genio-cyber-que-traiciono-a-su-patria-y-huyo-a-rusia-protegido-por-putin/

Stoll, C. (1997). *Silicon snake oil : second thoughts on the information highway*. Tpb.

The Freenet Project Inc. (2013). *About*. Freenetproject.org. https://freenetproject.org/pages/about.html

The Tor Project Inc. (2010). *The Tor Project | Privacy & Freedom Online*. Torproject.org. https://www.torproject.org/about/history/

van Dijck, J. (2013). *The Culture of Connectivity*. Oxford University Press.

Viens, A. (2019, November 5). *Exploring the Practical Applications of Blockchain Technology*. Visual Capitalist. https://www.visualcapitalist.com/exploring-the-practical-applications-of-blockchain-technology/

VV.AA. (2020, June 17). *Anexo:Partidos piratas*. Wikipedia. https://es.wikipedia.org/wiki/Anexo:Partidos_piratas

Waters, D. (2009, April 17). Pirate Bay awaits trial verdict. *News.Bbc.co.uk*. http://news.bbc.co.uk/2/hi/technology/8002938.stm