Documentos de Trabajo

Nº especial FC/Oxfam Intermón (3)

Hacia una nueva ilustración digital europea

Marta Peirano
Escritora y periodista
martapeirano[@]gmail.com

Resumen

Europa mantiene una posición delicada en la configuración del nuevo paradigma digital global. Por un lado, lidera la creación de marcos regulatorios capaces de imponer valores democráticos que garanticen un entorno digital más seguro y más justo, y constituye uno de los mercados con más proyección e influencia internacional. Por el otro, carece de una industria propia capaz de competir con los grandes bloques antagónicos de China y EE.UU., y delega el desarrollo de las grandes infraestructuras digitales a las grandes plataformas tecnológicas que amenazan su soberanía. Este contexto viene agravado por tres crisis interconectadas: la crisis climática, la crisis energética y la crisis política. Las decisiones que ahora tomemos serán determinantes a la hora de posicionarnos como una fuerza política capaz de trascender las patologías del capitalismo y defender el Estado del bienestar con la creación de redes productivas basadas en la cooperación. O, por el contrario, nos enfrentaremos a los retos de los próximos años como subordinados de tecnologías ajenas que ejercen un poder sin responsabilidades sobre nuestro territorio y nuestra sociedad.

Palabras clave

Transición digital, Unión Europea, plataformas tecnológicas, gobernanza de datos, infraestructuras.

Fundación Carolina

AGENDA 2030

OXFAM Intermón

Abstract

Europe is in a fragile position face to the new global digital paradigm. On the one hand, it leads the creation of regulatory frameworks that impose democratic values and guarantee a safer and fairer digital environment; it's also one of the markets with the greatest projection and international influence. On the other hand, Europe doesn't have an industry that can compete with the big blocks of China and the US, and it delegates the development of digital infrastructures to the big technology platforms that threaten its sovereignty. This context is aggravated by three interconnected crises: the climate crisis, the energy crisis, and the political crisis. The decisions that are taken now will be decisive in positioning the European Union as a political force that overcomes the pathologies of capitalism, and defends the welfare state with the creation of productive networks based on cooperation. On the contrary, we will face future challenges as a subordinate actor of foreign technologies that exercise power without responsibilities over our territory and society.

Keywords

Digital transition, European Union, technological platforms, data governance, infrastructures.

Marta Peirano

Escritora y periodista. Escribe en *El País*, en la revista de ciencia *Muy Interesante* y conduce una sección sobre tecnopolítica en *Las mañanas de RNE*. Ha sido jefa de Cultura en *ADN.es*, adjunta al director en *eldiario.es*, comisaria de tecnología de la Bienal del Pensamiento de Barcelona y miembro del grupo de trabajo para la ciberdefensa del CESEDEN. Dirige (re)programming - Strategies for Self-Renewal, un programa de entrevistas sobre tecnología y cambio climático del Instituto de Arte Contemporáneo de Ljubljana. Su último libro es *Contra el futuro* (Debate, 2022), un análisis sobre las tecnologías climáticas. Anteriormente publicó *El enemigo conoce el sistema* (Debate, 2019), un ensayo sobre el capitalismo de plataformas elegido por el *NYTimes* como uno de los dos mejores ensayos publicados en castellano y *El pequeño libro rojo del activista en la red* (Roca Editorial, 2015), un manual de criptografía para periodistas prologado por Edward Snowden. Su conferencia "¿Por qué me vigilan, si no soy nadie?" (TEDxMadrid, 2015) ha superado los cuatro millones de visitas.

1. Introducción[1]

Nos encontramos ante una importante encrucijada. Por un lado, el impulso nacionalista de las democracias "aliberales"[2] y el impulso colonialista de las grandes plataformas tecnológicas amenazan la supervivencia de internet. Por otro, tres crisis refuerzan la interdependencia sistémica de nuestras economías, nuestras sociedades y nuestros futuros: la crisis de suministros, la crisis energética y la crisis climática. Los dos acontecimientos que marcan la agenda informativa y económica de los últimos años constituyen una clara demostración.

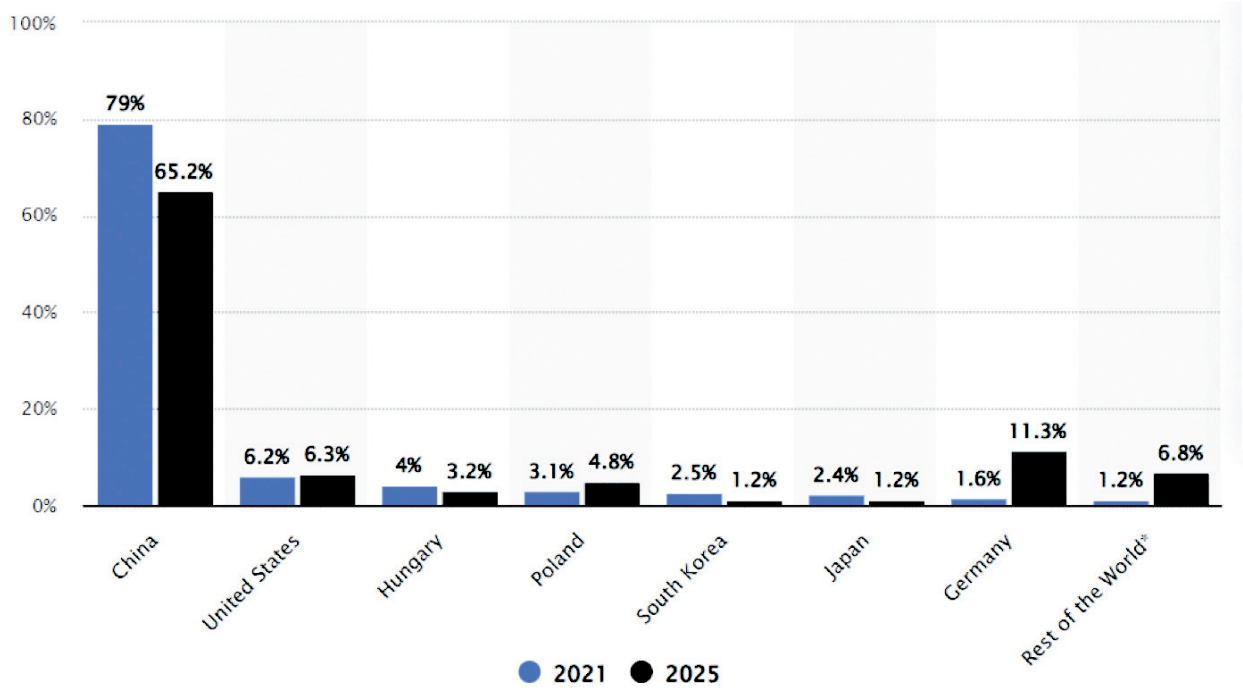
La pandemia de la COVID-19 y la invasión de Ucrania nos han enseñado que, bajo un régimen capitalista, la globalización es peligrosa. Por un lado, hemos descubierto que un virus que nace en Wuhan puede cerrar Bruselas en pocas semanas. Que las mascarillas que se fabrican en Shenzhen no están garantizadas en Lisboa. Que las vacunas fabricadas en Berlín solo sirven para ganar tiempo si la campaña no se universaliza y permitimos que haya cepas desatendidas en Manaus. Por el otro, la invasión del Dombás ha puesto en evidencia la dependencia alimentaria y energética de Europa, y la imposibilidad de esquivar nuevas crisis de refugiados. Especialmente esta última es una crisis que debemos afrontar, no solo económica y territorialmente, sino también desde la cultura.

A estas dos realidades, que están a punto de reventar las costuras de la sociedad del bienestar, se suma una tercera crisis en el horizonte: podríamos estar cimentando el desarrollo de la sociedad en procesos de automatización y energía que en ambos casos dependen de una reserva finita de materia prima. En su informe sobre el papel de los minerales críticos en la transición energética, la Agencia Internacional de Energía (IEA, por sus siglas en inglés) calcula que podría darse una escasez de materiales tan fundamentales como el litio tan pronto como 2025 (IEA, 2021). La escasez de materias primas para el desarrollo de las nuevas tecnologías ha sido anticipada por empresas como Tesla y Estados como la República Popular China, que concentran ahora la mayor parte de las minas y fuentes de explotación, en su mayoría no europeos.

[1] Este documento se enmarca en el proyecto conjunto entre Oxfam Intermón y la Fundación Carolina "Pactos sociales y transformación justa: visiones cruzadas desde América Latina y la Unión Europea sobre la triple transición".

[2] El concepto *democracia aliberal*, popularizado por el periodista indo-estadounidense Fareed Zakaria, se usa para denominar aquellos países cuyo gobierno sigue convocando elecciones, pero ya no garantiza ni respeta los derechos civiles de la población ni opera dentro de los límites establecidos por la Constitución.

Gráfico 1. Cuota de la capacidad de producción de baterías de iones de litio en todo el mundo por país, 2021 y 2025



Fuente: Statista, 2022.

En 2021, China produjo el 79% de las baterías de litio del mercado, superando a Japón y Corea, los países que dominaban hasta entonces la cadena de suministro. Según un informe de Bloomberg, "China controla el 80% del procesado de materias primas, el 77% de la producción de células y el 60% de la producción de componentes en todo el mundo"[3]. Este marco de inestabilidad y escasez nos coloca en un escenario de bloques en el que Europa podría quedar relegada a un papel estrictamente diplomático. Frente a la aceleración de las economías de EE.UU. y China, y en un contexto de escasez, Europa no tiene garantizados los suministros necesarios para afrontar los retos del cambio climático o las exigencias de la cuarta revolución industrial.

2. El papel de Europa

Hace diez años decíamos que EE.UU. inventa, China fabrica y Europa regula. Este proverbio ha sufrido importantes alteraciones. En el mundo de la microelectrónica, EE.UU. diseña el 65% de los chips, Asia (Taiwán y Corea) fabrica el 75% y Europa produce un 10%, pero consume mucho más[4]. La nueva directiva europea de semiconductores, lacónicamente llamada "Chips Act" (Comisión Europea, 2021), tiene como objetivo doblar la producción de chips para alcanzar el 20% del mercado en 2030. Incluso en el caso de que lo consiga —un reto casi imposible teniendo en cuenta los tiempos de construcción y producción de las fábricas—, la producción seguiría estando por detrás del consumo. Las dos nuevas leyes europeas, la Ley de Mercados Digitales (LMD) y la Ley de Servicios Digitales (LSD) adoptadas el 5 de julio de 2022, demuestran la voluntad de la Unión Europea (UE) de seguir legislando con propuestas pioneras que anteponen el conjunto de derechos que caracterizan las sociedades democráticas

[3] "Global Lithium-Ion Battery Supply Chain Ranking" (BNEF, 2020).
[4] "State of the U.S. semiconductor industry" (Semiconductor Industry Association, 2022).

sobre la expansión y el dominio de mercado de las grandes plataformas tecnológicas, a las que categorizan como "guardianes de acceso". La nueva nomenclatura incluye plataformas que conectan contenidos, servicios y productos como las redes sociales, navegadores, tiendas de aplicaciones o motores de búsqueda, con una capitalización de mercado superior a los 75.000 millones de euros y al menos 45 millones de usuarios mensuales. Claramente pensada para incluir multinacionales como Google, Meta, Apple o Amazon y Alibaba, la etiqueta excluye a las pymes para evitar su "sobrerregulación". Las nuevas leyes europeas están diseñadas para impulsar un ecosistema económico y legislativo que frene el crecimiento de las ballenas y permita prosperar a los demás, con especial atención a las empresas tecnológicas europeas. Una de sus estrategias más interesantes es obligar a las Big Tech a invertir grandes sumas de dinero para abrir un mercado que favorezca al resto, al menos si quieren seguir operando en Europa.

Por ejemplo, el requisito de interoperatividad obligará a los servicios de mensajería a compatibilizar sus servicios con los de su pequeña competencia. Eso significa que, en poco tiempo, los usuarios de WhatsApp o iMessage deberían poder enviarse mensajes y hacer videollamadas con usuarios de otras aplicaciones de mensajería. Aquellos que usan tres aplicaciones de mensajería, para el trabajo, la familia y su círculo social, podrán elegir una y tirar las demás. Más interesante todavía: el artículo 6.1 de la Ley de Mercados Digitales obligará a las empresas como Apple, que ejerce un control feudal sobre el mercado de aplicaciones para iPhone a través de su tienda iOS, que permitan que los usuarios se bajen las aplicaciones que quieran de otros lugares y tiendas, y también que estos usen pasarelas de pago dentro de las aplicaciones para iPhone sin cobrar su comisión del 30%[5]. En ambos casos, serán las grandes tecnológicas las que tendrán que establecer los protocolos que garanticen la seguridad y la privacidad de esas comunicaciones, como en su momento hicieron los padres fundadores de internet con las comunicaciones de la red, y con su primera aplicación de éxito: el correo. Los protocolos IMAP y POP3 garantizan la eficiencia y la privacidad de las comunicaciones por correo electrónico, independientemente del cliente de correo que los gestione. Las grandes tecnológicas tendrán que unificar protocolos o al menos asegurarse de que son compatibles entre ellos, para mantener la protección criptográfica de extremo a extremo en la mensajería y mantener un estándar de seguridad en el sistema para todos los jugadores.

En cuanto a los datos que generan los usuarios, y que constituyen uno de sus principales modelos de negocio, según las nuevas leyes del mercado digital, los "guardianes" ya no podrán reciclar las bases de datos personales que han extraído a través de un servicio para prestar otro servicio, como hace Amazon cuando usa los datos que recoge en exclusiva como tendero para competir con ventaja sobre las otras marcas del almacén. Tampoco podrán usar esos datos para hacer campañas segmentadas de publicidad personalizada sin obtener el consentimiento explícito del usuario.

Cuando entró en vigor, el Reglamento General de Protección de Datos de la UE (GDPR, por sus siglas en inglés) impuso la obligación de informar al usuario de forma explícita sobre los fines de las cookies para que pudiera aceptar su función y destino, inaugurando una nueva era de banners diseñados para obtener consentimiento a base de irritar las neuronas, consumir recursos e impedir el acceso al contenido deseado. Con la nueva ley europea, rechazar las cookies tendrá que ser igual de sencillo que aceptarlas, y rechazarlas no podrá de ningún modo impedir el acceso a la información. Finalmente, la normativa restringirá las "adquisiciones asesinas", evitando la práctica de adquirir rivales mientras son pequeños para evitar su competencia. Nunca sabremos en qué se habrían convertido Instagram, What-

[5] En uno de los casos más sonados de la industria, Epic Games y Apple se demandaron mutuamente porque Epic quería que los usuarios de su popular videojuego Fortnite pudieran comprar cosas dentro del juego ya instalado sin pagarle cada vez a Apple un 30%. Apple respondió sacando *todos* los juegos de Epic de su tienda iOS.

sApp o el proyecto Oculus si no hubieran sido engullidos y digeridos por Facebook, pero ninguno de los guardianes podrá hacer lo mismo con las empresas europeas que compitan en categorías similares.

Tanto la Ley de Mercados Digitales (DMA, por sus siglas en inglés) como la Ley de Servicios Digitales (DSA, por sus siglas en inglés) son leyes pioneras, con el potencial de convertirse en los estándares de regulación de internet en todo el mundo occidental. Lamentablemente, su implementación dependerá de la capacidad europea de establecer soberanía sobre la propia red dentro de su propio territorio, un desarrollo difícil de manifestar. De momento, los precedentes no auguran esa clase de resolución. Los obstáculos de implementación que han ido manifestándose desde la adopción de la GDPR demuestran que no es fácil legislar la "era de la información" sin los recursos, funcionarios y el acceso necesarios para fiscalizar a las grandes tecnológicas. En otras palabras, no podemos regular una infraestructura que no es nuestra, y que está blindada a la fiscalización de las autoridades por leyes de propiedad intelectual.

3. *Great power competition:* entre China y EE.UU.

La posición europea es cada vez más frágil con respecto a las dos grandes potencias que se disputan el siglo XXI. EE.UU. y China imponen dos modelos de gobernanza aparentemente antagonistas desde la perspectiva política, pero no muy diferentes en lo que se refiere a ambición extraterritorial. Ambos países ambicionan un mayor control de las grandes infraestructuras de telecomunicaciones a nivel planetario, incluyendo el acceso, gestión y explotación de los datos que derivan de su funcionamiento. En ese marco geoestratégico, es imprescindible que Europa afiance sus alianzas sin dejar de reforzar su autonomía. También es importante que proteja sus estándares para poder garantizar la protección de los derechos e intereses de los ciudadanos europeos, incluyendo el acceso, comprensión y optimización de las infraestructuras críticas de nuestro tiempo.

La Conferencia sobre el Futuro de Europa, celebrada en marzo de 2022, abrió el diálogo para la reforma de las instituciones europeas en los próximos años. Los países que forman la UE estuvieron de acuerdo en su voluntad de convertir a la Unión en líder de la conectividad digital. "La discusión es cómo lograrlo", apuntaba la eurodiputada belga del Partido Europeo de los Conservadores y Reformistas, Assita Kanko[6]. Como se verá en las próximas páginas, la voluntad europea de regular o liderar entra en conflicto con los intereses de las empresas que dominan, no solo el mercado digital, sino también su desarrollo. Es necesaria una revisión fundamental de las infraestructuras que sostienen la conectividad europea en términos de soberanía, que es lo mismo que decir derecho de acceso, intervención, regulación y fiscalización. Del mismo modo, también es necesario observar las instituciones que podrían constituir potencial de nuevos puntos para el desarrollo de nuevas infraestructuras en el contexto local.

Históricamente, los criterios que determinan la titularidad de las grandes potencias sobre el tablero geopolítico han estado centradas en la superioridad militar, la capacidad diplomática y el tamaño de la economía. En los últimos años, dos dimensiones del poder han aumentado fuertemente su valor gracias a una fuerte interdependencia interna: el desarrollo de infraestructuras técnicas y la capacidad de construir relato o realidad. En el nuevo escenario, las tres potencias que dominan el tablero internacional son EE.UU., Rusia y China. Europa mantiene su papel diplomático, pero necesita desarrollar sus valores y construir un relato propio que refuerce la cooperación interna de todos sus miembros.

[6] "Future of Europe: Conference debates proposals for EU action" (*EU affair*s, marzo de 2022).

Para conseguirlo, necesita establecer una nueva estrategia digital basada en la soberanía de sus infraestructuras. Para hacerlo, es imprescindible tener una perspectiva clara de cómo se desarrollaron las infraestructuras originales y en qué estado se encuentran actualmente.

4. Infraestructuras: el estado de la cuestión

4.1. Internet: el paciente

Internet es hijo de la Guerra Fría. Su cumpleaños es el 29 de octubre, el día de 1969 que Leonard Kleinrock y su estudiante Charley Kline enviaron el primer mensaje desde la Universidad de California en Los Ángeles al Instituto de Investigación de Stanford, en Menlo Park. Eran las 22:30 de la noche, y al otro lado de la única línea estaban Douglas Engelbart, el joven programador Bill Duvall y una SDS 940. Era la primera máquina con un sistema operativo de uso directo compartido y la futura sede de Community Memory, el primer boletín de noticias virtual. Para conectarlas, la empresa BNN les había fabricado dos enormes conmutadores de paquetes llamados IMP (*interface message processor*), que se conectaron entre ellos a través de la línea telefónica de AT&T.

En aquella noche de otoño, internet todavía se llamaba ARPANET. Todavía pertenecía a la Agencia de Proyectos de Investigación Avanzada que Eisenhower mandó crear en 1958, cuando Rusia puso en órbita Sputnik. Pero el Departamento de Defensa había perdido el interés en su desarrollo. El presidente era Richard Nixon y EE.UU. había puesto un hombre en la Luna, el Concorde había roto la barrera del sonido y 25.000 personas se habían juntado para hacer el amor y no la guerra en un festival de la Costa Este. Ni siquiera AT&T lo quiso. Cuando el gobierno estadounidense quiso vendérselo en 1973, la nueva red tenía ya 40 nodos y una cierta proyección internacional, pero era incompatible con los intereses de la operadora. El protocolo que conectaba los diferentes equipos era un sistema de conmutación de paquetes diseñado por Paul Baran, ingeniero eléctrico de la RAND Corporation, para afrontar los retos de la Guerra Fría: evitar la captura de información por parte del enemigo, impedir el control de las comunicaciones en caso de que las infraestructuras cayeran en manos enemigas y garantizar la transmisión de datos entre las agencias gubernamentales, incluso después de una bomba nuclear. Los ingenieros de AT&T declararon que, sin poder controlar directamente las transmisiones, no era un producto que pudieran usar o vender. Así fue como la red militar estadounidense diseñada durante la Guerra Fría se convirtió en una infraestructura pública, conectando instituciones científicas y educativas a lo largo del globo, hasta su privatización en 1995.

Fueron los académicos y no los militares los que diseñaron la red que usamos ahora, a través de nuevas instituciones y consorcios como el International Network Working Group. Allí se adoptó, en la última noche de 1983, la decisión más importante: los protocolos TCP/IP. El grupo de trabajo tardó una década en cocinar la lengua franca del sistema, pero lo hizo bien, y la prueba es que todavía funciona. El protocolo TCP/IP hace que los datos viajen de forma fragmentada por rutas recalculadas en función del tráfico existente, el ancho de banda disponible y la cantidad de nodos participando en la transmisión, y es lo que ha convertido internet en la infraestructura crítica y resiliente que conocemos ahora. Pero han pasado 52 años y nos adentramos en una nueva Guerra Fría, marcada por la amenaza nuclear. La supervivencia de esa red abierta, interoperativa e interconectada está fuertemente amenazada por dos fuerzas simultáneas y aparentemente opuestas: la privatización monopolista de sus infraestructuras y la balcanización de la pangea digital.

4.2. Privatización de internet: las grandes plataformas

Técnicamente, internet sigue siendo una red de máquinas interconectadas y regidas por los protocolos TCP/IP que garantizan el tráfico libre, atomizado y distribuido, de paquetes de información. En la práctica, la mayor parte del tráfico es gestionado de forma opaca, monopolista y extractiva por un pequeño puñado de empresas. Hablamos de las multinacionales estadounidenses que han hecho fortuna con el modelo de negocio que ahora llamamos "capitalismo de datos" y han facilitado el aparato de vigilancia masiva de las agencias de espionaje del gobierno de EE.UU. y de sus partners internacionales en la Alianza de los Cinco Ojos (FVEY), como revelaron las declaraciones y documentación aportadas por Edward Snowden en 2013[7].

Sus prácticas, basadas en la extracción masiva y deliberada de datos de miles de millones de personas para su explotación comercial e ideológica, están siendo contestadas por los nuevos marcos regulatorios europeos. Esos marcos incluyen propuestas pioneras como el citado GDPR o las recientes DMA y DSA, pero están siendo a su vez contestados por el desarrollo de nuevas infraestructuras privadas, que buscan reemplazar el esqueleto fundacional de la red, en sus tres aspectos fundamentales. Primero, su cuerpo. La red es un sistema nervioso de cables submarinos intercontinentales, cables terrestres de fibra óptica, antenas, satélites y puntos de intercambio. Los *data centers*, grandes concentraciones de servidores que almacenan y procesan los paquetes de datos, constituyen el hipotálamo o su memoria RAM. Después, su lenguaje. Los algoritmos de recomendación están sustituyendo de facto a los protocolos TCP/IP, alterando el tránsito de la información de forma interesada, discriminatoria, oportunista que contradice los principios de libertad, privacidad, seguridad y resiliencia que guiaron el diseño de los protocolos originales de la red. Tercero, su cultura. Las plataformas digitales imponen y amplifican su propia ideología a través de la distribución y edición de los contenidos mismos, con sistemas de moderación basados en oscuros manuales empleados de forma opaca y unilateral que escapan a los procesos de fiscalización democráticos (prensa, justicia) y vulneran derechos civiles de los usuarios (Amnistía Internacional, 2021).

Hay una directiva europea, con fecha del 8 de diciembre de 2008, que dice que una infraestructura crítica es "el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población, cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones" (Consejo de la UE, 2008). Nadie puede dudar que la infraestructura que nos ha permitido seguir trabajando, seguir consumiendo, seguir atendiendo a nuestros padres y escolarizando a nuestros hijos, y siguiendo las noticias durante la pandemia es crítica. Sin embargo, hemos delegado la responsabilidad de nuestro bienestar social y económico en media docena de multinacionales estadounidenses que durante años han esquivado sus responsabilidades con nosotros, desde el pago de impuestos al cumplimiento de la legislación de protección de datos. Predeciblemente, esta industria oportunista creció especialmente durante los dos años de la pandemia. Una crisis es el peor contexto para gestionar una crisis y, cuando llegó esta crisis, su infraestructura ya estaba allí.

En los últimos 15 años, las instituciones europeas han contemplado de forma pasiva (y en algunos casos asistido de forma activa, con oscuras ayudas gubernamentales y campañas de "nación emprendedora") la colonización de esas infraestructuras críticas. Los beneficiarios son el equivalente digital a

[7] Todos los documentos facilitados por el exanalista Edward Snowden sobre la red de vigilancia masiva de la NSA están recopilados en el Snowden Digital Surveillance Archive, accesible desde numerosas páginas web. Por ejemplo: https://cryptome.org/2013/11/snowden-tally.htm.

paraísos fiscales: infraestructuras financiadas por dinero público que esquivan la legislación local y los controles democráticos. Un ecosistema dominado por la explotación de los usuarios, la colonización de nuestras comunicaciones y la amplificación de campañas de propaganda cuyo discurso desafía nuestras leyes e instituciones democráticas, y altera el bienestar general.

5. Balcanización de internet: las grandes potencias

Como ya se ha explicado en la sección anterior, internet es un cuerpo que se compone de infraestructuras y de normas. Por un lado, un conjunto de cables submarinos y terrestres de fibra óptica, antenas y satélites; por el otro, los protocolos TCP/IP, el pegamento universal que unía todas sus piezas. Los protocolos diseñados por un consorcio internacional de científicos e ingenieros para garantizar que la información encontrará siempre el camino más corto, más seguro y más barato para llegar a su destino, independientemente de las circunstancias políticas y geográficas del mundo "real", no fueron adecuados para AT&T y tampoco lo son para los regímenes totalitarios o los líderes populistas. Por ese motivo, la libertad de información por diseño ha ido encontrando distintos grados de resistencia gubernamental.

Hasta hace poco, el bloqueo se ha realizado de forma mecánica sobre las principales infraestructuras, una tarea sencilla en países que dependen de un solo cable submarino. India lleva el récord de apagones informativos y Cachemira lleva sin acceso a internet desde agosto de 2019, salvo un centenar de páginas que el gobierno indio desbloqueó en 2020. Pakistán le pisa los talones, seguido de Siria y Turquía. Pero la incidencia más notable ocurrió el 15 de noviembre de 2019, cuando Irán bloqueó el acceso a internet al 97% de su población durante toda una semana. Fue la primera vez que un Estado ejecutó un apagón informativo casi total para desactivar manifestaciones e impedir la denuncia mediática de la vulneración de derechos civiles por parte de las autoridades. El apagón fue ordenado por el Consejo Supremo de Seguridad Nacional e impuesto por el Ministerio de las TIC para reprimir las protestas de 2019[8]. Poco después, el fenómeno se repitió durante las protestas por el precio de la gasolina en Kazajistán. El seguimiento de esta clase de apagones por parte de organizaciones como Netblocks.org[9] indica que la supresión del malestar popular y la cobertura mediática con apagones selectivos es una tendencia al alza, seguidas de las leyes mordaza y campañas de propaganda. En 2020, a esta tendencia se suma una nueva estrategia de gestión de internet: la secesión.

El 29 de octubre de 2020, Rusia aprobó la Ley de Soberanía de Internet[10], que autoriza a su regulador de telecomunicaciones local a bloquear los contenidos, servicios o aplicaciones que considere una amenaza para la seguridad del Estado sin previa orden, proceso o notificación. Los criterios sobre lo que constituye una amenaza son tan opacos como su plan de ejecución. Y los contenidos parecen ser internet en su conjunto. La ley contempla la necesidad de un botón rojo para apagar la red cuando moleste y un sistema propio de gestión de dominios.

Según la ley, firmada por el presidente Putin seis meses antes, la estrategia tiene dos objetivos principales: proteger a los ciudadanos rusos de contenidos tóxicos y proteger la infraestructura rusa de ciberataques del exterior. Un argumento interesante, cuando el gobierno ruso es uno de los principales productores de desinformación y de ciberataques, junto con India, China e Irán (Bradshaw, Bailey y

[8] El informe "A web of impunity", de Amnistía Internacional y The Hertie School, en colaboración con The Internet Outage Detection and Analysis (IODA) project, investiga las causas y consecuencias del bloqueo de internet durante las manifestaciones. Disponible en: https://iran-shutdown.amnesty.org/.

[9] https://netblocks.org/reports.

[10] http://publication.pravo.gov.ru/Document/View/0001201905010025.

Howard, 2021), y los dos últimos son los únicos países del mundo que han levantado su propio muro de contención digital. Inicialmente, la ley otorga poderes curatoriales a Roskomnadzor, el regulador de telecomunicaciones ruso, para bloquear los contenidos que considere una amenaza para la seguridad del Estado, sin requerir una orden ni advertir a los ciudadanos. Para plegarse a la ley, las operadoras de internet que operan en Rusia han tenido que instalar un software de inspección de paquetes capaz de identificar la fuente de los contenidos y filtrarlos, bloquearlos o redirigirlos. Este paquete de medidas es típico de los regímenes autoritarios como Irán o Arabia Saudí. Más interesante a efectos de la red global, Rusia está desarrollando su propio sistema de nombres de dominio (DNS). De conseguirlo, se convertiría en una isla independiente de la red general, y en un ejemplo a seguir para regímenes afines o similares.

El DNS es una base de datos distribuida y jerárquica que conecta los nombres de dominio con el lugar donde está alojado el contenido, un servidor en alguna parte del mundo con una dirección IP. Un poco como la operadora que conecta el número al que llamamos con el teléfono físico al que queremos llamar. Para agilizar los procesos, esa responsabilidad se distribuye de manera jerárquica entre el sistema operativo del usuario, las operadoras de internet locales y los *data centers* de las grandes plataformas tecnológicas. Su administrador central es una organización independiente llamada Internet Corporation for Assigned Names and Numbers (ICANN), y el repositorio central de todos los DNS está alojado en trece servidores distribuidos por todo el planeta, para garantizar su seguridad y eficiencia. El país que crea su propio sistema de dominios puede redireccionar cualquier dominio a cualquier lugar, sin que el usuario se dé cuenta: crear una internet paralela en la que los ciudadanos siguen leyendo la Wikipedia, buscando cosas en Google o leyendo las noticias del *New York Times*, sin darse cuenta de que los contenidos han sido alterados para satisfacer los propósitos del gobierno ruso.

Las ventajas de esa independencia para un régimen como el ruso estaban claras ya en 2020, antes de la invasión de Ucrania. "Ahora el gobierno podrá censurar el contenido de manera directa o convertir el internet ruso en un circuito cerrado sin informar a la ciudadanía de lo que está haciendo ni por qué", advirtió la directora de Human Rights Watch en Europa y Asia Central, Rachel Denber. Al comienzo de la invasión, que el régimen de Putin caracterizó como una "misión de mantenimiento de la paz", el parlamento ruso complementó el aislamiento con una ley que condena cualquier información falsa, como escribir la palabra *invasión*, o compartir vídeos de soldados rusos cometiendo crímenes de guerra en Ucrania o siendo derrotados por las fuerzas ucranianas, con penas de 15 años de cárcel o multas de 1,5 millones de rublos (12.000 euros).

6. Un nuevo bloque

Rusia lleva tratando de asignar sus propios nombres de dominio desde 2010, al igual que Cuba, Irán o Turquía, pero hasta finales de 2018, se encontraba con el obstáculo de las Naciones Unidas. Entonces, la Asamblea General de las Naciones Unidas aprobó una resolución titulada "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos" (Naciones Unidas, 2018). En ella se propone la creación de un tratado global contra la ciberdelincuencia que no defiende a los ciudadanos de ciberataques, el uso ilegítimo de sus datos o el robo de identidad, sino que defiende la potestad de los Estados y de sus leyes diseñadas para criminalizar y reprimir la disidencia política y otras manifestaciones ciudadanas legítimas. La resolución se aprobó el 17 de diciembre de 2018 con los votos a favor de 94 países, encabezados por Rusia, Bielorrusia, China, Irán, Nicaragua, Siria y Venezuela; 59 democracias votaron en contra.

La ambición comercial de China ha impedido que desarrolle su propio DNS, pero no por falta de pasión secesionista. En la segunda Conferencia Mundial de Internet en Wuzhen en 2015, el presidente Xi Jin-

ping defendió el derecho de cada país a gobernar su propio ciberespacio como le parezca. "Ningún país debería perseguir la ciberhegemonía ni interferir en los asuntos internos de otros Estados" (Human Rights Watch, 2020). Siguiendo esa máxima, China ha levantado su famosa muralla digital, con la ayuda de sus tres gigantes tecnológicos: Baidu, Alibaba y Tencent. El sistema cerrado y conjunto que constituyen las tres firmas ha facilitado el desarrollo de su famoso sistema de crédito social basado en la vigilancia y el castigo de sus ciudadanos.

"China está construyendo su propio Internet centrado en sus propios valores, y está exportando esa visión de Internet a otros países", dijo Mark Zuckerberg en un discurso a los estudiantes de Georgetown[11]. Es propio del mundo occidental no considerar que Mark Zuckerberg ha hecho exactamente lo mismo a través de sus campañas en Facebook, Instagram y WhatsApp. Irán lleva años trabajando en un internet halal, alineado con el islam, para escapar de su influencia. Se llama National Information Network. "La nación no tolera una red social que pone su llave en las manos de EE.UU.", dijo el ayatolá Ahmad Khatami. Europa forma parte de una isla, dominada por las plataformas digitales estadounidenses, vigilada por la alianza de los Cinco Ojos y acompañada del resto de países que participan en la alianza atlántica.

Esa isla tiene sombras, además del espionaje y la explotación. En los últimos años, ha afianzado su relación con regímenes similares al ruso, cuyos valores se imponen cada vez más sobre los principios colectivos, democráticos y humanitarios de la Unión. Turquía, un país que se ha posicionado como proxy, puente y al mismo tiempo guardián, entre Europa y Asia, no solo ha ejecutado sus propios "apagones" como medida de gestión civil a espaldas del mundo. En 2009, Turquía bloqueó la candidatura del primer ministro danés, Anders Fogh Rasmussen, como secretario general de la OTAN por haber sido demasiado tolerante con las caricaturas de Mahoma de 2006 y con los terroristas kurdos residentes de Dinamarca. Doce años más tarde, el Acuerdo de Madrid refuerza la posición de Turquía como agente distorsionador de los valores europeos, al obligar a dos miembros a "trabajar con Turquía en la extradición de individuos sospechosos de terrorismo" y "luchar contra la desinformación" a cambio de despejar sus candidaturas en la OTAN. Un pacto fáustico, sabiendo que los criterios de Erdogan sobre terrorismo y desinformación están más cercanos a los de Putin que a los de la UE. Al mismo tiempo, las democracias llamadas "aliberales" de países como Hungría y Polonia conviven con las democracias liberales de países como Francia o Alemania, desestabilizando los valores originales de consenso con realidades alternativas e incompatibles con los ideales democráticos.

7. Vulnerabilidad: soberanía y monopolios

El desarrollo de sistemas alternativos de gestión de red plantea un problema de valores, pero también de seguridad, tanto para Europa como para el resto del mundo: permite a Rusia ejecutar un ataque masivo e indiscriminado contra las infraestructuras de internet y blindarse contra él. Algo así casi ocurrió en junio de 2017, cuando agentes de Sandworm —uno de los grupos de hackers integrados en la agencia de inteligencia rusa (GRU)— lanzaron un ataque contra Ucrania que infectó al resto del planeta, convirtiéndose en el ciberataque más destructivo de la historia (The United States Department of Justice, 2020). NotPetya estaba diseñado para explotar una vulnerabilidad dentro del sistema Windows y secuestrar todas aquellas redes y centrales eléctricas, redes de transporte, aeropuertos, gasolineras, estaciones y bancos que la tuvieran. Pocas semanas antes, otro malware llamado WannaCry consiguió

[11] Mark Zuckerberg Addresses Students at Georgetown Event Kicking Off New Series https://www.georgetown.edu/news/mark-zuckerberg-to-host-conversation-at-georgetown-on-free-expression/.

infectar bancos escandinavos, la seguridad social británica o el servicio de trenes alemán. Los dos eran vulnerabilidades diseñadas por la Agencia de Seguridad Nacional estadounidense, que habían acabado en el mercado negro, antes de ser modificadas y utilizadas por el GRU. Pero un ataque es como un incendio: el Estado que lo activa sabe que, en cualquier momento, se puede volver contra él. Salvo que tenga un cortafuegos. La capacidad de atacar con ese tipo de armas sin sufrir sus consecuencias es como propagar un virus letal por el aire y ser el único país vacunado contra él.

En términos de malware, Rusia es una fábrica de virus. Se ha convertido en el centro del mercado de servicios para la extorsión online (Ransomware as a Service o RaaS), donde conviven grupos como REvil o DarkSide, cuyo negocio es vender códigos para atacar y encriptar sistemas y toda la infraestructura de comunicaciones necesaria para negociar el rescate, con acceso a foros y medios de noticias para volcar los datos cuando la víctima no paga. Esos carteles de la extorsión online operan en países cuyo gobierno hace la vista gorda, a condición de que no ataquen dentro de sus fronteras y estén disponibles para operaciones patrióticas. "Los hackers son espíritus libres, como artistas que se levantan una mañana de buenas y se ponen a pintar —dijo Vladímir Putin en una rueda de prensa con medios internacionales en 2017—. Hay días que se levantan, leen las noticias y, si se sienten patrióticos, tratan de hacer la contribución que consideran justa contra los que maldicen a Rusia". Si estos países, que incluyen también a Corea del Norte, Venezuela y los Emiratos, construyen un cortafuegos que les permita atacar por la red sin ser vulnerables a sus propios ataques, su capacidad de destrucción será impredecible.

Finalmente, las dos tendencias geopolíticas que marcan el presente de internet —la colonialista y la secesionista— se autoalimentan a la hora de elevar la vulnerabilidad del sistema. El monopolio de sistemas operativos comerciales —como Windows, Android o IOS, y de sistemas operativos industriales como CLP de Siemens o soluciones administrativas como Kaseya o SolarWinds— son la clase de monocultivo que promueve y acelera las infecciones, hongos y plagas, porque ofrecen un terreno uniforme para la propagación de los virus, que son "liberados" en busca de puntos débiles, y siempre los encuentran. Sobre todo cuando la empresa responsable puede dejar de actualizar y parchear su producto para obligar a los usuarios a comprar la siguiente generación de licencias. Han tenido que parar hospitales para que Microsoft publique un parche de emergencia para tapar un agujero que ya conocían[12]. El parche, como las vacunas, solo es útil si se aplica antes de la infección. Los monopolios son el sistema linfático de la red, un ecosistema poblado por trabajadores estresados, administradores remotos, ejecutivos irresponsables y drivers sin actualizar. Otro foco de infección es la galaxia de miles de millones de objetos presuntamente inteligentes diseñados por empresas sin presupuesto de seguridad que llamamos Internet de las cosas.

8. Más tablero, menos jugadores

La demanda de banda ancha se duplica cada dos años. En los últimos cinco años, la capacidad internacional total se ha triplicado, de 200 Tbps en 2016 a 600 Tbps a finales de 2020. El último Mapa Global de Internet de TeleGeography —un informe que refleja el estado de la infraestructura de internet a nivel global— muestra que los cuatro mayores centros de conexión a la red están en Europa. Hemos sido la región de mayor crecimiento: contábamos con una red de 45 cables submarinos, diez en España y nueve en Portugal que ha sido recientemente reforzada por la llegada de otros seis cables: Marea y Grace Hopper (en Sopelana, Vizcaya), y Equiano y 2Africa (en Lisboa y Barcelona). El sur de Europa se ha convertido en una de las regiones con más alta disponibilidad de zonas de servicio y puntos de acceso directo a la nube, con hubs principales en Marsella, Viena, Milán y Madrid.

[12] https://therecord.media/microsoft-confirms-dogwalk-zero-day-vulnerability-has-been-exploited/.

Históricamente, esta clase de operación ha estado ligada a consorcios de operadoras como Telefónica, France Telecom o Deutsche Telekom, que han desarrollado los canales de comunicación como servicio público incluso después de la privatización del sector, que empezó en Europa en 1997. En los últimos cinco años, sin embargo, el principal desarrollo ha llegado de la mano de un puñado de proveedores de servicios estadounidenses —Google, Facebook, Amazon y Microsoft—. En 2022, estos llamados Over-The-Top providers (OTT) lideran la demanda de ancho de banda, consumiendo el 64% del total de todo el mundo[13]. Consecuentemente, en los últimos años han liderado el desarrollo de infraestructuras de comunicación en el mundo occidental. Su prioridad, sin embargo, no es el servicio público sino garantizar la velocidad de conexión entre sus centros de datos y los grandes nodos de interconexión global.

Cuadro 1. Líderes de desarrollo de infraestructuras de comunicación

GOOGLE	AMAZON	META	MICROSOFT
-Apricot (part owner) -Blue (part owner) -Curie (sole owner) -Dunant (sole owner) -Echo (part owner) -Equiano (sole owner) -FASTER (part owner) -Firmin (sole owner) -Grace Hopper (sole owner) -Havfrue (part owner) -INDIGO-Central (part owner) -INDIGO-West (part owner) -Japan-Guam-Australia South (JGA-S) (part owner) -Junior (sole owner) -Monet (part owner) -Pacific Light Cable Network (PLCN) (part owner) -Raman (part owner) -Southeast Asia-Japan Cable (SJC) (part owner) -Tannat (part owner) -Unity (part owner)	-Havfrue (major capacity buyer) -Hawaiki (major capacity buyer) -JUPITER(part owner) -MAREA (major capacity buyer) -CAP-1 (part owner)	-2Africa (part owner) -AEC-1(major capacity buyer) -Amitie (part owner) -Apricot (part owner) -Asia Pacific Gateway (APG) (part owner) -Bifrost (part owner) -Echo (part owner) -Havfrue (part owner) -Havhingsten/CeltixConnect-2 (part owner) -Havhingsten/North Sea Connect (part owner) -JUPITER (part owner) -Malbec (part owner) -MAREA (part owner) -CAP-1 (part owner) -Pacific Light Cable Network (PLCN) (part owner) -Southeast Asia-Japan Cable 2 (SJC2) (part owner)	-AEC-1 (major capacity buyer) -Amitie (part owner) -EXA Express (major capacity buyer) -MAREA (part owner) -New Cross Pacific (NCP) Cable System (part owner)

[13] The State of the Network (Telegeography, 2021 Edition).

La comunidad internacional del desarrollo, con el notorio liderazgo de la UE, identifica en la transición digital un vector estratégico de innovación y generación de bienestar. En Europa, sin embargo, el principal desarrollo ha sido el crecimiento de las nubes de Amazon Web Services, Google Cloud, IBM Cloud, Microsoft Azure, Alibaba Cloud y Oracle Cloud. El sur de Europa ha sido la región más favorecida para la implantación de AWS, Google Cloud y Azure. Madrid ha sido la que más ha crecido en centros de datos, un 25% del mercado total europeo y 98.000 m^2 de territorio.

Los centros de datos tienen cada vez más protagonismo en el consumo energético y global del planeta. El último informe del Panel Intergubernamental sobre el Clima (IPCC, por sus siglas en inglés), publicado en abril de 2022, establece claramente que debemos reducir de forma radical nuestro consumo energético en los próximos dos años. En 2017, la UE ya había conseguido reducir sus emisiones casi un 22% con respecto a los niveles de 1990, tres años antes de lo previsto. El desarrollo de infraestructuras de nube privadas de las grandes empresas tecnológicas en suelo europeo es incompatible con la Ley Europea del Clima, y su plan de reducir las emisiones de gases de efecto invernadero al menos un 55% antes de 2030.

Los números no engañan: la reducción de emisiones es incompatible con el crecimiento de las grandes plataformas tecnológicas. Según su propio informe de sostenibilidad, las emisiones de Amazon aumentaron un 18% en 2021 (Amazon, 2022). El informe refleja un total de 71,54 millones de toneladas métricas de CO2, el equivalente a las emisiones anuales de 180 centrales de gas. Desde que lanzó *The Climate Pledge* en 2019, el "proyecto con el que la compañía se compromete a alcanzar las cero emisiones netas de carbono en toda su actividad para 2040"[14], las emisiones del gigante estadounidense han aumentado un 40%. Según la empresa, ha sido porque la demanda ha superado sus expectativas durante la pandemia de la COVID-19. "Mientras trabajamos para descarbonizar nuestra empresa, Amazon está creciendo muy deprisa —explica el informe—. Hemos escalado nuestro negocio a un ritmo sin precedentes para atender las necesidades de nuestros clientes durante la pandemia". AWS lidera la industria de la computación en nube, que ya está produciendo entre el 2% y el 4% del total de emisiones a escala planetaria. En sus casi 20 años de vida, su huella de carbono ha conseguido superar a la industria de la aviación (Freitag *et al.*, 2021). Todo indica que seguirá creciendo hasta alcanzar el 15%-30% en algunos países en 2030 (Kamiya y Kvarnström, 2019). Con el advenimiento de la inteligencia artificial, la demanda energética de la computación se duplica cada dos meses. Sociedades enteras se adentran ahora en la era de la información.

Los analistas del estudio *The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations* expresan estar "unánimemente de acuerdo en que las emisiones procedentes de ICT (Information Communications Technologies) no se reducirán sin un gran esfuerzo combinado de la política y la industria" (Freitag *et al.*, 2021). Es más, ofrecen razones para anticipar que crecerán, pese a los ambiciosos compromisos medioambientales de las grandes tecnológicas. Y concluyen: "Nuestro análisis sugiere que no todas las promesas de reducir las emisiones de carbono son lo suficientemente ambiciosas para alcanzar los objetivos climáticos; y que los mecanismos reguladores que deberían reforzar el cumplimiento de esos compromisos están ausentes" (Freitag *et al.*, 2021).

A la emergencia climática, en 2022 se suma la crisis energética derivada de la invasión de Ucrania. La UE ha propuesto recortes del 15% del consumo, ante la posibilidad de que Rusia cierre su grifo de gas natural. Los intereses de las grandes compañías tecnológicas no reflejan la realidad climática y energética europea, y el crecimiento de sus centros de datos es incompatible con la seguridad energética europea. Sin un refuerzo importante de la capacidad de fiscalizar esos centros de datos, también es incompatible con la protección de nuestra privacidad.

[14] Amazon Sostenibilidad (2019): *Más lejos y más rápido juntos.* Disponible en: https://sostenibilidad.aboutamazon.es.

9. Gobernanza de datos

Dos meses antes de que entrara en vigor el GDPR europeo, en mayo de 2018, el gobierno de EE.UU. aprobó la CLOUD Act, la actualización de una ley de 1986 sobre el uso legal de datos en el extranjero. Esta ley obliga a los proveedores de servicios estadounidenses a facilitar a las autoridades estadounidenses, si así los reclaman, todos los datos que tengan bajo su custodia. Esto implica los datos que almacena cualquier ministerio de cualquier Estado europeo en su nube, tanto si están alojados en EE.UU. como si lo están en otro país. Se deduce que cualquier información que los ministros franceses (o españoles) suben, intercambian o descargan de la nube de Microsoft (o de Google o de Amazon) es susceptible de acabar en manos del gobierno estadounidense, sin consentimiento, justificación, explicación o previo aviso. Aunque las comunicaciones están cifradas, la gestión incluye la clase de metadatos que genera cada transacción como, por ejemplo, la geolocalización de los miembros de un gobierno cada vez que se conectan.

Frente al monopolio de las grandes plataformas tecnológicas estadounidenses y sus leyes extraterritoriales, la UE propuso Gaia-X, un proyecto que nace en 2019 con la ambición de crear un ecosistema europeo de la nube que garantice la soberanía sobre los datos personales e industriales, y defienda los valores de la Unión. Su misión oficial es "crear un ecosistema digital abierto, transparente y seguro, donde los datos y servicios pueden estar disponibles, recopilados y compartidos en un ambiente de confianza", tal y como lo explicó la ministra de Economía Nadia Calviño en la Asamblea Constituyente de Gaia-X España en Talavera, en marzo de 2022. Y originalmente agrupa empresas, instituciones de investigación, asociaciones, y Administraciones públicas y políticas europeas. Sin embargo, en abril de 2021, Gaia-X abrió la puerta a Microsoft, Google, Amazon, Palantir, Huawei y Alibaba como miembros de confianza del consorcio, generando tensiones internas de las que nunca se ha recuperado. Desde entonces, las nubes de Amazon, Microsoft y Google han colonizado Europa, con un 69% del mercado, mientras que el principal servicio de nube local, servida por Deutsche Telekom, no supera el 2%.

Las grandes tecnológicas están limitadas en el voto y la asociación, frente a las nubes de pleno derecho como OVHCloud, Airbus, Orange y la ya mencionada Deutsche Telekom, pero su peso queda reforzado por la membresía de asociaciones como Digital Europe, CISPE y Bitkom, lobbies que representan los intereses de Amazon, Google o Microsoft. Como resultado de las tensiones, en 2021 nació Euclidia, un consorcio de jugadores de la industria europea como Nextcloud o Scaleway que se unen para conseguir que "Europa se convierta en un líder digital sin seguir el modelo americano o asiático"[15]. Por su parte, el gobierno francés tomó medidas unilaterales.

Emmanuel Macron ha prohibido a sus ministros el uso de Microsoft365, la plataforma de nube gratuita para usuarios de Microsoft donde se pueden usar aplicaciones como Word, Excel, PowerPoint, Microsoft Teams, Outlook Express y otros programas populares para trabajar en remoto que alcanzaron una gran popularidad durante la pandemia. También anunció una estrategia nacional para la nube, con medidas para garantizar la soberanía nacional o al menos la independencia francesa de las leyes extraterritoriales estadounidenses. Incluye la creación de un certificado oficial de "Nube de confianza" que solo podrán recibir las empresas europeas de empresarios europeos que tengan los servidores en Francia. El ministro de Economía Bruno Le Maire explicó que, si querían ofrecer sus servicios a las Administraciones de la República Francesa, Google, Microsoft y Amazon podrán licenciar su plataforma a los proveedores de nube franceses (*Le Figaro*, 2021).

[15] *23 European Cloud Technology Companies form the European Cloud Industrial Alliance (EUCLIDIA)*: https://www.euclidia.eu/publications/EUCLIDIA-Press.Release.Launch.Announcement.

10. Moderación de contenidos

Hizo falta un boicoteo de más de 400 anunciantes, una pandemia y una injerencia rusa que cambió el rumbo electoral de al menos un país para que Facebook dejara de negar el problema y anunciara medidas contra la desinformación. Y, sin embargo, los documentos internos filtrados[16] por Frances Haugen, exjefa de producto en el equipo de integridad cívica de la empresa, muestran que incluso entonces sus promesas fueron falsas. Mark Zuckerberg "sabía" que sus algoritmos premian los contenidos más tóxicos, favorecen la radicalización de personas inestables y amplifican especialmente las campañas de desinformación. Haugen mostró que los directivos de Facebook recibían informes internos sobre el daño que le hace Instagram a los niños, mientras la plataforma preparaba el lanzamiento de Instagram Kids. También demostró que la empresa estaba informada de las campañas de limpieza étnica y fraude electoral que Mark Zuckerberg calificó de ridículas en las entrevistas y negó ante el Senado. Y que Facebook tenía las herramientas para evitar el asalto al Capitolio y decidió no usarlas para no perder interacción.

Como Haugen explicó al Congreso estadounidense, Facebook financia públicamente programas de verificadores externos para garantizar la "limpieza" del contenido. En la página de la red social se puede leer:

> Tenemos el compromiso de luchar contra la difusión de información errónea en Facebook e Instagram. En muchos países y regiones, trabajamos con organizaciones externas de verificación de datos certificadas por la agencia no partidista International Fact-Checking Network (IFCN) para identificar y revisar este contenido, y tomar las medidas pertinentes.

Pero la plataforma mantenía un club exclusivo de 5,8 millones de usuarios VIP exentos de moderación (*Wall Street Journal*, 2021), incluidos varios que en aquel momento publicaban, amplificaban y promocionaban información abiertamente falsa y peligros sobre vacunas y tratamientos contra la COVID-19, o mentiras sobre la legitimidad de las elecciones, como Donald Trump. Pese a su papel protagonista en la amplificación de desinformación y propaganda en todo el mundo, queremos que diseñen los estándares, normas y límites de la libertad de expresión en internet. Peor aún, se quieren convertir en el monopolio de la verdad y de la legitimidad, formando un consorcio de plataformas —Facebook, YouTube, Microsoft y Twitter— para decidir quién es peligroso o terrorista. Se llama Global Internet Forum to Counter Terrorism (GIFCT).

GIFCT fue fundado en 2017 como una alianza digital antiterrorismo que operaba con una base de datos de fotos y de vídeos, principalmente de ISIS y Al Qaeda consensuados con la ONU. Igual que la gestión de la pornografía infantil, que se negocia en colaboración directa con las autoridades y siguiendo una normativa oficial, precedente y local, y se ejecuta con ayuda de algoritmos especializados en todas las plataformas. El asalto al Capitolio aceleró la expansión de nuevos ejemplos de terrorismo, más sutiles y locales, que podrían incluir todo tipo de grupos presentes en el Capitolio, desde los Bogaloo Boys y Oath Keepers a Black Lives Matter a los miembros de Qanon. El discurso del odio que aplican las plataformas se ha basado históricamente en una descripción vaga, abierta y cambiante, que se modera etiquetando de forma externa y "after the fact", cuando el contenido ya ha circulado y ha amplificado su mensaje. No obedecen a criterios preexistentes elaborados por organismos internacionales experimentados y capaces, como los del informe especial de la ONU, el "Rabat Plan of Ac-

[16] *Wall Street Journal* publicó la exclusiva en octubre de 2021, y todas las revelaciones están contenidas en su especial *The Facebook files. A Wall Street Journal investigation*. Disponible en: https://www.wsj.com/articles/the-facebook-files-11631713039.

tion", publicado en 2012, diseñado precisamente para proteger a las minorías del discurso de odio y la deshumanización[17].

La cultura de las grandes plataformas no solo ha invadido el ciclo informativo y la cultura de la red, también está intoxicando la academia. Una investigación del *New Statesman* reveló que al menos seis departamentos universitarios europeos de prestigio habían recibido cheques multimillonarios de Google, Facebook, Amazon y Microsoft "para investigar aspectos relacionados a los modelos de negocio de las propias plataformas, de la privacidad y la protección de datos a la ética de la IA y la competición en los mercados digitales" (Clarke, Williams y Swindells, 2021). Según dicha investigación, el Institute for Ethics in Artificial Intelligence de la Technical University of Munich (TUM) recibió 7,5 millones de dólares, y el Humboldt Institute for Internet and Society de Berlín ha recibido al menos 14 millones de euros de Google desde su fundación en 2012, la tercera parte de la financiación privada total de la institución (Clarke, Williams y Swindells, 2021). Dos factores ponen en crisis la independencia de las instituciones: las plataformas, financiando los estudios de los que son objeto, y la posible dependencia económica de las mismas instituciones que deberían buscar, proponer y gestar alternativas a esos mismos monopolios dentro de la UE.

11. Conclusión y propuestas para una nueva ilustración europea

La estrategia digital es una de las palancas clave para el posicionamiento de Europa en el mundo y el futuro de la UE como grupo. Los fondos NextGenerationEU suponen una oportunidad sin precedentes para establecer alternativas comunitarias al monopolio de las grandes tecnológicas chinas y estadounidenses, y para resistir las campañas de intoxicación política y desinformación que amenazan con dividir de forma irreparable a los países de la Unión. La historia fundacional de la red nos ofrece varias lecciones sobre resiliencia y comunidad. Necesitamos recuperar y garantizar los cuatro ingredientes que construyeron internet hace 50 años: redundancia, transparencia, globalidad y descentralización. Al mismo tiempo, la deriva de la red ofrece también moralejas: la privatización de infraestructuras críticas en la era globalizada genera dependencias y vulnerabilidades que no nos podemos permitir.

En los próximos años será de máxima importancia favorecer un ecosistema de soluciones europeas que mantengan los valores democráticos de la Unión y propongan una nueva visión de la red como infraestructura crítica dedicada a mejorar la vida de las personas frente a los retos políticos y climáticos de nuestro tiempo. La inversión debe ser grande y deliberada, enfocada en aquellas funciones que ayuden a anticipar, gestionar y mitigar los impactos de la crisis climática allí donde se manifiesten. Con una inversión ambiciosa, una visión colectiva, y la implicación constante y generosa de las instituciones más vinculadas a las comunidades locales, esta crisis ofrece la oportunidad de crear alternativas al capitalismo desastre. Se dan las condiciones para que Europa lidere el camino hacia una nueva ilustración digital.

Termina este documento de trabajo —diseñado para servir de base para el debate y la reflexión en torno al futuro digital europeo— con una propuesta de escenarios: "distopías" (riesgos) / "utopías" (oportunidades), en torno a algunos de los temas centrales: infraestructuras, gobernanza de datos, transportes y automatización.

[17] El "Rabat Plan of Action" fue adoptado por la Oficina de Derechos Humanos de Naciones Unidas (OHCHR) en Rabat, en octubre de 2012, tras los talleres de Ginebra, Viena, Nairobi, Bangkok y Santiago de Chile. Véase: https://www.ohchr.org/en/freedom-of-expression.

11.1. Infraestructuras

Distopía. Network States

En manos de las grandes plataformas digitales, el trabajo remoto, los pagos en criptomoneda y la ausencia de regulación, internet se consolida como un conjunto de Estados Digitales interconectados e interdependientes, donde las empresas, gobiernos, instituciones y otras entidades alquilan espacios, tiendas y expositores. Las Administraciones, organizaciones y empresas delegan la mayor parte de sus funciones en las grandes tecnológicas porque dan por hecho que son más seguras, que su gestión es más eficiente, que sus infraestructuras son más sólidas, que sus sistemas de automatización son los más vanguardistas y que sus ingenieros son los más brillantes de cada promoción. Las plataformas han asumido la gestión de la economía, el desarrollo de la industria, la protección de la seguridad nacional, los servicios educativos y sanitarios, y la gestión de recursos, basura, energía y transporte de las grandes ciudades. Cinco empresas lo gestionan todo. Se han convertido en Network States.

En el nuevo régimen, ya nadie quiere saber dónde vives sino para quién trabajas. Los ciudadanos pasan a ser miembros de esos Estados, como trabajadores, clientes o usuarios, y viven perfectamente segregados por plataforma. Ya nadie tiene que convivir con personas que votan opciones diferentes a la suya. Los trabajadores de élite son *jetsetters* que viven en ciudades *cool* como Berlín, París, Lisboa o Madrid, y suben el precio del alquiler, la energía y los servicios sin pagar impuestos ni contribuir al tejido o el bienestar local. Una segunda capa de trabajadores subcontratados malvive en otras grandes ciudades, pero menos *cool*, generando, moderando o manipulando contenido para campañas de marketing comercial o político, o manteniendo la automatización de servicios y productos como automóviles. El resto son usuarios y trabajadores del sector servicios. Todos son un punto que se mueve por el mapa, permanentemente identificado y vigilado gracias a las bases de datos biométricos, generando inteligencia para los gobiernos, oportunidad de negocio para las empresas y de extorsión para los grupos criminales. Es una versión acelerada de una realidad globalizada que ya vivimos.

Utopía. Internet de todos

En 2020, Trump firmó dos órdenes ejecutivas para obligar a la empresa china ByteDance a vender todas sus empresas en EE.UU. para poder seguir operando en el país. El argumento era que TikTok, su aplicación estrella y la primera plataforma digital china que trasciende las fronteras asiáticas, con 800 millones de usuarios en todo el mundo, era un problema de seguridad nacional. Trump no tenía pruebas de que espiara a ciudadanos estadounidenses, pero la Ley de Seguridad Nacional China de 2017 obliga a cualquier organización o ciudadano chino a "apoyar, ayudar y cooperar con el trabajo de inteligencia estatal". Esa ley, equivalente a la Ley Patriota estadounidense pero también parecida a la CLOUD Act, era razón suficiente.

Desde las filtraciones de Edward Snowden en 2013, Europa tiene pruebas incontestables de que el gobierno estadounidense y sus aliados han usado las plataformas digitales y sus sistemas operativos para espiar a ciudadanos, funcionarios y líderes europeos. Si obligan a Google, Facebook, Amazon, Microsoft y Apple a vender sus operaciones europeas a una cooperativa de tecnológicas locales, podrían recrear un internet al servicio de las necesidades de los países de la Unión, reactivando la industria local bajo principios de transparencia adecuados, garantizando la privacidad y la seguridad de los ciudadanos.

Utopía 2. Disaster Tolerant Networks

Internet se ha privatizado, pero hay cientos de miles de redes pequeñas y locales, modulares y comunitarias que funcionan de forma paralela y complementaria pero no dependiente de la red comercial. Son agnósticas en cuanto a la plataforma (incluyen packet radio, HAM settings, TCP/IP, UDP, SBIR) y coexisten distintos modelos de gobernanza bajo la responsabilidad de la propia comunidad que las genera y cumplen diferentes funciones (modelo Reddit, donde la moderación y las normas del foro son responsabilidad de los administradores del propio foro, o modelo presidente de la comunidad de vecinos, dependiendo de la comunidad). Algunas son temporales, otras son estructurales y algunas son contextuales (se activan "en caso de"). Algunas están asociadas a instituciones científicas, sanitarias o educativas que sirven a los barrios y colaboran con las comunidades. Otras están asociadas a redes de producción energéticas y de gestión hídrica, a laboratorios de investigación ciudadana, y protocolos de gestión y mitigación de desastres climáticos. Otras están asociadas a redes de servicios comerciales, como el transporte, el reparto de comida y paquetes, o los cuidados. Un millón de redes pequeñas en lugar de una sola grande en manos de cinco multinacionales.

11.2. Gobernanza de datos

Distopía. Monopolio de la revolución industrial

El capitalismo de plataformas ocupa todos los entornos de la sociedad y de la industria. Las plataformas digitales que habían dedicado los primeros 20 años del milenio a registrar los movimientos y preferencias de miles de millones de personas usaron su banco de datos para monopolizar el desarrollo de sistemas de inteligencia artificial. Su ventaja competitiva les permitió vender soluciones para la optimización de procesos, servicios y recursos a todas las demás industrias y entornos civiles, incluyendo transporte, agricultura, gobierno, sanidad, gestión de agua, energía y educación. Todos esos datos no solo afianzan su monopolio, sino que los convierte en la agencia de inteligencia más poderosa del mundo. Gaia-X se convirtió en el vehículo perfecto para legitimar su intrusión en marcos que hasta entonces estaban protegidos, como la sanidad y la educación a través de un mercado de datos en el que los ciudadanos pueden comerciar con su información a cambio de dinero, bonos o descuentos.

Utopía. Federación de datos para el bien común

Gracias a la gestión colectiva de las infraestructuras de comunicaciones, la captura de datos se negocia y aprueba en función de su utilidad, su necesidad y su potencial. El criterio que valida su flujo es transparente y está sujeto a la fiscalización de las instituciones científicas, de la justicia y de los medios de comunicación. Los primeros modelos experimentales, como la propuesta de Nesta (Element AI y Nesta, 2019) y el "city data commons" propuesto por la Ciudad de Barcelona en 2017, dan lugar a un nuevo régimen de datos. La desprivatización de la infraestructura de red y la creación de mil redes pequeñas, colectivas y locales, junto con el músculo para reforzar el cumplimiento de la legislación europea, permiten una nueva industria de datos basada en la gestión colectiva y la búsqueda del bien común. Se destruyen todas las bases de datos que no son compatibles con la protección de derechos civiles (por ejemplo, las bases de datos biométricas) y se crean comunidades de datos en torno a la gestión hídrica, la producción energética o los cuidados. Mil empresas tecnológicas pequeñas crecen apoyadas con dinero público para ofrecer soluciones locales a los retos climáticos, educativos y sanitarios. El Big Data es demasiado importante para dejarlo en manos de las Big Tech.

11.3. Transporte

Distopía. Electrificación privada

Los coches autónomos han ocupado el asfalto y los transeúntes llevan un dispositivo que los identifica como objetos no atropellables. El consumo eléctrico se dispara, el transporte público se derrumba, la vigilancia se masifica. Hay sensores en todas partes para garantizar la "seguridad" del tránsito. El propio coche registra las infracciones en el momento de cometerlas y las manda al fabricante, que las comparte con la policía (modelo Amazon Ring). Tanto coches como personas llevan cámaras permanentemente grabando cada minuto del día para defender su caso en un accidente o incidencia. Este futuro es una versión extrema de lo que ya pasa en ciudades como Atlanta: si no tienes coche eres un criminal. Esta realidad ofrece grandes oportunidades de expansión en el Metaverso.

Utopía. Electrificación comunitaria

Un despliegue de inversión pública capaz de distribuir la producción eléctrica cofinanciando redes energéticas que vuelcan sus excedentes sobre la red general. Con el tiempo, el entramado permite construir un ecosistema apropiado para la electrificación de una red de transporte público limpio, barato, capaz y silencioso, y el mantenimiento de sistemas de microtransporte para los trayectos cortos como bicis eléctricas o los trayectos especiales como car-to-go. Tener un coche en la ciudad queda relegado a personas con necesidades muy particulares. En el resto de los casos resulta excéntrico, está mal visto y además no hay donde aparcar.

11.4. Automatización

Distopía. La fábrica sin obreros

Con la industria 4.0 monopolizada por empresas que se han hecho ricas en la "economía colaborativa", la eterna promesa de la fábrica sin obreros que hacía las veces de amenaza para los que reclamaban sus derechos laborales no se ha hecho realidad. Siguen haciendo falta obreros, pero los trabajos que quedan son aquellos en los que el obrero es más barato que la máquina que lo sustituye: microtrabajos miseria exentos de derechos como los repartidores de Glovo y Uber Eats durante la pandemia, gestionados por un algoritmo sin oficina de Recursos Humanos, bajas por accidente, vacaciones y oficina de reclamación. Y, sin embargo, las herramientas de la eficiencia los mantienen vigilados 24/7, porque las ofertas de microtrabajos dependen de su "reputación".

Utopía. La creatividad como motor productivo

Las instituciones académicas desarrollan sistemas automáticos con dinero público y bancos de datos ciudadanos en un ecosistema diseñado para garantizar el acceso universal a sus beneficios y ampliar el margen del bien común. La sanidad se beneficia de la revolución de soluciones basadas en Big Data, la industria europea expande sus ambiciones, la educación deja de ser algo que se acaba en la veintena. La automatización barata permite una fuerte reducción de la jornada laboral que muchas empresas convierten en formación para sus trabajadores, como inversión en la propia empresa y aportación a la prosperidad nacional. También permite largas vacaciones, frecuentes sabáticos e intercambios con otras industrias. La combinación de tiempo, formación, motivación y recursos acelera nuevas revoluciones científicas.

11.5. Información

Distopía. Todo es mentira

Las grandes plataformas digitales han afianzado su doble vida. Por un lado, como distribuidores de desinformación, con algoritmos que amplifican los contenidos más escandalosos a costa de la propia realidad y artífices de campañas oscuras, diseñadas para garantizar que la desinformación de los candidatos populistas alcanza sus objetivos más vulnerables sin ser fiscalizada por las instituciones democráticas diseñadas para hacerlo, incluidas la prensa y la justicia. Por otro lado, como guardianes de la verdad, manteniendo redes de verificadores dependientes de su financiación, donando grandes sumas a las universidades en crisis para que apoyen su particular variante de la "libertad de expresión" y negociando criterios de publicación con el resto de los "guardianes" para su mutua protección y beneficio. En ausencia de un criterio unificado y estable de realidad, los ciudadanos se abandonan al cinismo y las conspiraciones, el sectarismo y el horóscopo. Al menos ofrecen las dos cosas que les faltan: una comunidad que los acepta y explicaciones sencillas en un mundo que ya no tiene sentido.

Utopía. Aterrizar en la comunidad

El desarrollo de comunidades locales capaces de generar su propia intersección de realidad con sus propios datos en torno a recursos críticos y el estado de las infraestructuras y servicio de su entorno ofrece una plataforma sólida y cercana sobre la que trabajar en objetivos comunes, capaz de trascender la polarización artificial generada por los partidos con ayuda de la red social. El proyecto común, que devuelve al ciudadano un lugar en su comunidad de cercanía —junto con un propósito que trasciende su papel como individuo— es la cura contra la pandemia de soledad, indefensión y rabia que tanto beneficia a los populismos, y el incentivo necesario para afrontar los retos de los próximos años con energía y esperanza. El surgimiento de colectivos, cooperativas y asociaciones en torno a las necesidades y potencialidades de los barrios es el detonante de una nueva era de acción colectiva capaz de corregir los excesos del capitalismo asumiendo la responsabilidad de producir mejores políticos y exigir mejores políticas para todos.

Referencias bibliográficas

Amazon (2022): *Delivering Progress Every Day. Amazon's 2021 Sustainability Report*. Disponible en: https://sustainability.aboutamazon.com/2021-sustainability-report.pdf.

Amnistía Internacional (2021): *The Facebook Papers: What do they mean for a human rights perspective* (noviembre). Disponible en: https://www.amnesty.org/en/latest/campaigns/2021/11/the-facebook-papers-what-do-they-mean-from-a-human-rights-perspective/.

Bradshaw, S.; Bailey, H. y Howard, P. N. (2021): "Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation.", Oxford University, Programme on Democracy & Technology. Disponible en: https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/.

Clarke, L.; Williams, O. y Swindells, K. (2021): "How Google quietly funds Europe's leading tech policy institutes", *New Statesman*.

Comisión Europea (2021): "European Chips Act: Communication, Regulation, Joint Undertaking and Recommendation", Bruselas (septiembre, 2021).

Consejo de la UE (2008): Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (texto pertinente a efectos del EEE). Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32008L0114.

Element AI y Nesta (2019): *Data Trusts: A new tool for data governance* (junio). Disponible en: http://hello.elementai.com/rs/024-OAQ-547/images/Data_Trusts_EN_201914.pdf.

Freitag, C. *et al.* (2021): "The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations", *Patterns*, vol. 2, Issue 9, 10 (septiembre). Disponible en: https://doi.org/10.1016/j.patter.2021.100340.

Human Rights Watch (2020): *Russia: Growing Internet Isolation, Control, Censorship*. Disponible en: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

IEA (2021): "The Role of Critical Minerals in Clean Energy Transitions". Disponible en: https://www.iea.org/reports/the-role-of-critical-minerals-in-clean-energy-transitions/executive-summary.

Kamiya, G. y Kvarnström, O. (2019): *Data centers and energy – from global headlines to local headaches?*, International Energy Agency.

Le Figaro (2021): "La France veut utiliser sous licence les technologies cloud américaines" (17 de mayo). Disponible en: https://www.lefigaro.fr/flash-eco/la-france-veut-utiliser-sous-licence-les-technologies-cloud-americaines-20210517.

Naciones Unidas (2018): Resolución aprobada por la Asamblea General. Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/57/PDF/N1845057.pdf?OpenElement.

Parlamento Europeo (2022): Digital Services Act: agreement for a transparent and safe online environment. Disponible en: https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment.

Parlamento Europeo y Consejo de la UE (2022): Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

The United States Department of Justice (2020): "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace" (octubre). Disponible en: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

Wall Street Journal (2021): "Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt" (13 de septiembre). Disponible en: https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353.

Fundación Carolina
Plaza del Marqués de Salamanca nº 8, 4ª planta
28006 Madrid - España
www.fundacioncarolina.es
@Red_Carolina

Fundación Oxfam Intermón
Gran Via de les Corts Catalanes, 641
08010 Barcelona
www.oxfamintermon.org
@OxfamIntermon

Fundación Carolina / Oxfam Intermón, septiembre 2022
ISSN-e: 1885-9119
DOI: https://doi.org/10.33960/issn-e.1885-9119.DTFO03

Cómo citar:
Peirano, M. (2022): "Hacia una nueva ilustración digital europea",
Documentos de trabajo nº especial FC/Oxfam Intermón (3),
Madrid, Fundación Carolina/Oxfam Intermón.