Telefónica

DIGITAL POLICY LAB

La soberanía digital de Europa: de regulador a superpotencia en la era de la rivalidad entre EE.UU. y China

Índice

Resumen

- El COVID-19 ha puesto de manifiesto la importancia crítica de la tecnología para la resiliencia económica y sanitaria, haciendo de la transformación y la soberanía digital de Europa una cuestión de importancia existencial.
- Las crecientes tensiones entre Estados Unidos y China son un incentivo adicional para que Europa desarrolle sus propias capacidades digitales; estas tensiones corren el riesgo de convertirse en un campo de batalla en la lucha por la supremacía tecnológica e industrial.
- Los gobiernos democráticos, deseosos de preservar un mercado abierto de servicios digitales y, al mismo tiempo, de proteger los intereses de los ciudadanos, encuentran en el modelo europeo una alternativa cada vez más atractiva a los enfoques estadounidense y chino.
- La UE no puede seguir confiando en su poder regulador, sino que debe convertirse en una superpotencia tecnológica por sí misma. Los árbitros no ganan el juego.
- Europa se perdió la primera ola de tecnología, pero debe aprovechar la siguiente, en la que cuenta con ventajas competitivas como en el Edge Computing.
- Los Estados miembros de la UE no tienen una posición común sobre cuestiones tecnológicas ni una visión compartida sobre la importancia estratégica de las tecnologías digitales, como sucede con el despliegue de la banda ancha o la aplicación de la IA.

Prefacio

José María Álvarez-Pallete

Presidente Ejecutivo de Telefónica S.A.

En tiempos de incertidumbre, los valores humanistas deben servir de brújula que nos guía hacia el camino correcto. La pandemia del COVID-19 ha acelerado la transformación digital de nuestras sociedades y nuestras economías a un ritmo vertiginoso. En solo unas pocas semanas de confinamiento hemos visto avanzar el teletrabajo, el comercio electrónico y la educación online tanto como lo haría en un período de cinco años en condiciones normales.

Nuestra primera y principal contribución a esta emergencia sanitaria, social y económica ha sido mantener las comunicaciones en funcionamiento. De hecho, en España, Telefónica se ha convertido en uno de los soportes que ha mantenido viva la actividad empresarial, cultural, educativa, laboral y financiera de nuestra sociedad.

La infraestructura digital ha demostrado ser fundamental para el bienestar social, especialmente para la salud y la educación, así como para el funcionamiento de toda la economía. Frente a la crisis, la misión de Telefónica de "hacer nuestro mundo más humano conectando vidas" se ha vuelto más relevante que nunca. Hemos constatado que para alcanzar una digitalización inclusiva la conectividad es crucial y conscientes de ello, en base a nuestros valores y nuestra misión, esta crisis ha sacado lo mejor de nosotros.

El año 2020 será recordado como el año de la pandemia, pero también como el año en que nuestro mundo volvió a empezar con un nuevo rumbo. No hay vuelta atrás. Nos esperan tiempos difíciles en los que tendremos que hacer frente a un estancamiento económico y al aumento de las desigualdades como ya hemos experimentado en los últimos meses.

Ahora, más que nunca, necesitamos un nuevo Pacto Digital para construir una sociedad mejor. Los valores como la solidaridad y la cooperación han prevalecido en estos tiempos críticos. Esto debería inspirar los nuevos modelos de gobernanza ya que las fórmulas tradicionales no funcionan. La estrecha

cooperación y el diálogo entre los gobiernos, la sociedad civil y las empresas es de suma importancia para alcanzar compromisos sociales.

Este Pacto Digital se traduce por una parte en la defensa de nuestros valores y los derechos fundamentales en esta nueva era, y por otra en trazar las bases de una sociedad más sostenible, inclusiva y digital.

Los ejes principales de este nuevo Pacto Digital deberían ser los siguientes:

En primer lugar, y teniendo en cuenta que la desigualdad es el mayor desafío al que nos enfrentamos, debemos asegurarnos de que la mayoría de la población tenga acceso a la tecnología y a las oportunidades que ofrece el nuevo mundo digital, y así podríamos reducir la brecha digital. Por lo tanto, es fundamental invertir en las habilidades digitales de las personas.

Algunos datos son reveladores de los cambios que se están produciendo: el tráfico en nuestras plataformas educativas online ha crecido en más del 300 % y ya sabemos que el 85 % de los empleos necesarios en 2030 todavía no existen. Para garantizar que nadie se quede atrás es indispensable centrarse en la recualificación y formación profesional para responder a las necesidades del mercado laboral y al mismo tiempo en reinventar la educación adecuada para la era digital. A su vez, los sistemas de protección social y laboral deben hacer frente a la rápida evolución de la economía digital.

En segundo lugar, debemos conseguir que las sociedades y las economías sean más sostenibles a través de la digitalización, apoyando a los sectores clave, las tecnologías y la innovación para acelerar la transición verde y la digitalización de las pequeñas y medianas empresas (pymes) así como las Administraciones Públicas. Las pymes tienen un gran peso en la economía y en la creación de empleo por lo que, es necesario crear un fondo de reconstrucción digital a escala regional y local, que podría utilizarse para apoyarlas en su proceso de digitalización.

Además, necesitamos construir una mejor infraestructura. Las telecomunicaciones han demostrado ser un sector vital en las sociedades contemporáneas, pero solo pueden cumplir su función si se dispone de las mejores redes. En España hemos sido testigos de la relevancia que tiene contar con la red de fibra más potente de Europa. En este sentido, es fundamental reforzar las redes de muy alta capacidad e invertir en ellas, así como permitir nuevas formas de cooperación y facilitar un amplio despliegue de redes resilientes, fiables y rápidas. Así mismo, construir una mejor infraestructura también significa conectar a los que no están conectados, y ello contribuye de manera decisiva a reducir la brecha digital.

En este contexto, se debe incluir la necesidad de asegurar una competencia equilibrada. La hoja de ruta de las renovadas estrategias industriales debe afinarse y definirse para reducir al mínimo el proteccionismo nacional, modernizar las normas sobre la competencia y la supervisión de los mercados, y actualizar las políticas fiscales. Pedimos las mismas normas y las mismas obligaciones para los mismos servicios.

En paralelo, es necesario diseñar planes estratégicos nacionales y regionales a largo plazo que fomenten el desarrollo de industrias locales centradas en nuevas tecnologías como la Inteligencia Artificial (IA), el Internet de las cosas (IoT), la ciberseguridad, Cloud y el Blockchain. Planes como los incentivos fiscales y el desarrollo de Centros de Excelencia son fundamentales para avanzar en la transformación digital y para reforzar la soberanía digital.

Por último, debemos garantizar un uso ético y fiable de la tecnología, protegiendo la privacidad y otros derechos digitales. Las Administraciones Públicas y las empresas que utilizan las nuevas tecnologías deben aplicar las mejores prácticas para que su uso sea responsable y para incrementar la confianza de los usuarios. La gente necesita tener la opción de gestionar los datos y controlar su uso. Una relación basada en la confianza será, en última instancia, la base de un nuevo modelo de intercambio equitativo de datos y de tecnologías confiables del que se beneficie toda la sociedad.

En el futuro, cuando miremos hacia atrás en estos tiempos difíciles, nos daremos cuenta de que este fue el momento en que la tecnología, la cooperación y la infraestructura de las telecomunicaciones demostraron ser los grandes aliados que nos ayudaron a superar esta crisis a través de la innovación y la solidaridad.

Preámbulo

Anthony Giddens

Miembro vitalicio del King's College, Cambridge y profesor emérito de la London School of Economics

La revolución digital es la mayor fuerza transformadora de la sociedad actual a escala global, que se está desarrollando a un ritmo nunca visto en ningún período anterior de la historia y se caracteriza por ser intrínsecamente global. Se estima que el 45 % de la población mundial tiene smartphones y que un número aún mayor puede acceder ocasionalmente a uno. Esta es la primera vez que la tecnología de vanguardia ha penetrado en masa directamente en las zonas más pobres del mundo. Unido al impacto de la radio y la televisión, que ahora están en gran parte digitalizadas, un gran número de personas tiene acceso a noticias de última hora a lo largo de todo el día. Las redes sociales han hecho realidad la aldea global de Marshall McLuhan, donde las personas crean amistades personales y relaciones íntimas, pero donde también existen rumores, insinuaciones, engaños y violencia. ¡Twitter no es más que cháchara superficial! Sin embargo, es una red digitalizada y se entrelaza profundamente con el poder. Los rumores, las insinuaciones y los engaños son inherentes a las fake news, con todos sus efectos perturbadores en la política y otros ámbitos. Se dijo muy acertadamente que la aldea global tendría sus matones particulares y así ha sido.

Los líderes demagógicos pueden comunicarse directamente con sus seguidores de una forma que nunca antes había sido posible y pueden mantener a segmentos enteros de la población bajo vigilancia directa. Sin embargo, también surgen nuevas formas de resistencia e incluso de insurgencia.

Como señalan los colaboradores de esta colección de ensayos, la realidad de la era digital está muy lejos de las esperanzas y aspiraciones iniciales que muchos albergaron con el auge de Internet. Algunos de sus pioneros, como Tim Berners-Lee, figura principal en la creación de la red mundial, creyeron que sería principalmente un vehículo de colaboración y democratización. Sin embargo, como todos sabemos, su lado oscuro y destructivo también es muy grande. Las manifestaciones de la

Primavera Árabe fueron los primeros movimientos democráticos impulsados digitalmente y, en ese momento, a muchos les pareció que presagiaban un gran avance. La realidad resultó ser mucho más compleja y perturbadora.

El advenimiento de la era digital se equipara a menudo con el auge de Silicon Valley, pero, por extraordinario que parezca, sus verdaderos orígenes residen en la geopolítica y el poder político, a los que regresa constantemente. Los orígenes de la IA se remontan en gran parte a las contribuciones de Alan Turing durante la Segunda Guerra Mundial. Sin embargo, la fuerza motriz de la revolución digital en general vino del "Momento Sputnik". El primer ser enviado al espacio en el Sputnik 2, no fue un humano, sino Laika, una perra callejera encontrada en Moscú. El programa Sputnik causó gran conmoción en la psique americana. Provocó una respuesta masiva del gobierno de los Estados Unidos con la creación de la NASA y el ARPA (que más tarde se convirtió en DARPA) y la inversión de cientos de millones de dólares en investigación en la frontera militar. ARPANET fue el origen de lo que más tarde se llamó Internet. El auge de Silicon Valley y de las grandes empresas digitales es inseparable de las transformaciones geopolíticas de 1989 y del desencadenamiento de los mercados libres en todo el mundo. No hubo una investigación básica en la que cimentar su ascenso meteórico y no fue sino el resultado de un periodo muy particular de la historia.

Dividida, Europa aparece en gran medida como el telón de fondo de este escenario, más que como una de sus fuerzas motrices. Es precisamente esto lo que explica los dilemas explorados con cierto grado de detalle en esta colección de ensayos. 1989 fue también una época de transformación en China, y un punto de inflexión en la Plaza de Tiananmen. Para bien o para mal, la reafirmación del poder estatal posterior fue el trampolín para el "modelo chino": una economía de mercado acoplada a, y supervisada por, un Estado autoritario, pero que en términos económicos ha sido realmente exitosa. China tiene sus propias grandes empresas digitales y Huawei es una de ellas, quizás la más grande, que operan, sin embargo, dentro de la penumbra del Estado. El país tiene ahora la tecnología de computación cuántica más avanzada del mundo y está más o menos a la altura de los Estados Unidos en lo que respecta a la IA, incluyendo sus aplicaciones de uso militar.

Europa no se ha quedado totalmente atrás en la llegada de la era digital. Después de todo, Tim Berners-Lee, considerado el padre de Internet, trabajó en el CERN, radicado en Suiza. Sin embargo, en la "nueva Guerra Fría", si puede llamarse así, Europa se encuentra una vez más atrapada en medio del campo de juego, entre los EE. UU. y China, con una Rusia digitalmente maliciosa jugando en la banda. Al menos hasta ahora, el impacto del COVID-19 ha servido para intensificar estas brechas. Sus consecuencias podrían introducir toda una serie de nuevos desplazamientos y rivalidades en todo el mundo. Los artículos de esta colección de ensayos proporcionan un valioso análisis sobre la forma en que Europa, y específicamente la Unión Europea, debería responder. La panoplia completa de fortalezas y debilidades de la Unión está a la vista y no será nada fácil abrirse paso.

Introducción: La soberanía digital de Europa

Jeremy Shapiro

Director de Investigación del European Council on Foreign Relations

"¿Es posible revertir el toque de las campanas que alguna vez repicaron? ¿Podemos desaprender aquellas artes que, en aras de la civilización, queman el mundo? La ciencia avanza al paso. Pero ¿quién hará redoblar los tambores tocando retirada?"

Charles Lamb, 1830

El cambio es uno de los rasgos que definen nuestra época. En los últimos años, el ritmo del cambio ha sido desconcertante en casi todos los ámbitos. Nuevos movimientos políticos, Estados emergentes y nuevas enfermedades, parecen amenazar, como en los tiempos del ensayista inglés Charles Lamb, con "quemar el mundo". En la raíz de casi todos estos desalentadores cambios reside la enorme oportunidad y la peligrosa promesa de las tecnologías digitales. En las últimas décadas, estas han alterado radicalmente la forma en que las personas y las sociedades interactúan, en todos los niveles, desde cómo hacemos la guerra hasta cómo hacemos el amor.

Así, preguntas como, quién es el propietario de las tecnologías del futuro quién las produce o quién establece las normas y regula su uso, se han convertido en un tema central en la partida geopolítica. Los países de todo el mundo están tratando de dar forma a ese desarrollo tecnológico para obtener los beneficios, tanto económicos como geopolíticos, que surgen de esta era de cambios acelerados. En definitiva, están tratando de proteger su soberanía digital, es decir, su capacidad para controlar las nuevas tecnologías digitales y sus efectos en la sociedad.

Para los responsables políticos europeos, la idea de la soberanía digital forma parte de una lucha más amplia a la que se enfrentan, para mantener su capacidad de actuar y proteger a sus conciudadanos en un mundo de creciente competencia geopolítica. En una serie de cuestiones, desde la política de Irán hasta la defensa militar y la regulación de la desinformación, parece que la Unión Europea nunca ha sido tan soberana como pensaba. Una época de competencia geopolítica más feroz y una América más centrada en sus estrechos intereses han expuesto la falta de independencia de la UE en formas novedosas, y con singular importancia en el ámbito digital.

Ahora está claro que, si los europeos quieren obtener los beneficios económicos de las tecnologías digitales emergentes, garantizar que su política permanezca libre de desinformación divisiva y decidir quién puede conocer su información más personal, tendrán que proteger su soberanía digital y competir con otros actores geopolíticos en el ámbito digital.

El European Council on Foreign Relations (ECFR) ha propuesto un nuevo concepto de "soberanía estratégica" que puede ayudar a guiar a la UE y a sus Estados miembros a través de esta nueva era de competición geopolítica. La soberanía estratégica implica que la UE y sus Estados miembros necesitan preservar por sí mismos la capacidad de actuar en el mundo, aunque sigan siendo

profundamente interdependientes. La consecución de la soberanía digital europea es una parte fundamental de este esfuerzo. El propósito de esta colección de ensayos es contribuir a ese esfuerzo ayudando a los lectores a comprender mejor los desafíos y las oportunidades que las tecnologías digitales, y la pugna geopolítica por ellas, plantean y brindan a Europa y sus Estados miembros.

Los autores de esta colección de ensayos canalizan el contexto geopolítico en el que Europa opera en una variedad de cuestiones, entre ellas el 5G, el Cloud Computing o la política de competencia, y sugieren formas de proteger mejor la soberanía digital europea. El enfoque, que deriva de la nacionalidad de la mayoría de los autores, se centra en la situación de España, pero las lecciones pueden aplicarse a toda Europa. En el presente capítulo se resumen las cuestiones analizadas dividiéndolas en problemas que existen desde hace varios años, nuevos problemas que han surgido en los dos últimos años, y se evalúan los principales retos y oportunidades que la UE y sus Estados miembros deben afrontar para mejorar la soberanía digital europea.

Continuidad

El desarrollo tecnológico centra naturalmente nuestra atención en el cambio. Pero, en este torbellino de dinamismo, hay algunos elementos de continuidad, mucho menos llamativos, pero no menos importantes, que a menudo pasan desapercibidos. La tecnología puede engendrar cambios vertiginosos, pero, como destacan muchos de los colaboradores, varios aspectos de la pugna por la soberanía digital ya llevan años entre nosotros y podemos esperar que sigan dando forma a esa lucha durante muchos años más.

El primero se refiere a la **continuidad de la competencia bipolar entre los Estados Unidos y China** que está socavando la cooperación internacional, en particular en el ámbito tecnológico. Casi todos los ensayos subrayan que es probable que este conflicto perdure y que, de hecho, las relaciones entre Estados Unidos y China, especialmente en el ámbito de la tecnología, seguirán deteriorándose. Como muestran tanto Fran Burwell como Janka Oertel, la pandemia ha exacerbado las divisiones existentes entre EE.UU. y China. La mayoría de los autores ven su creciente conflicto como el germen de la lucha europea por la soberanía digital. Europa sigue siendo digitalmente dependiente tanto de los Estados Unidos como de China en una amplia variedad de campos, desde las plataformas de mensajería instantánea hasta los equipos de telecomunicaciones. La competencia entre los Estados Unidos y China significa que ambos consideran el mercado europeo de manera creciente como un campo de batalla crucial en la lucha global por establecer su dominio tecnológico e industrial mundial. Europa, en palabras de Oertel, ya está "atrapada en el fuego cruzado". Como demuestran los recientes debates políticos en Europa sobre cuestiones tan diversas como la tecnología 5G y la regulación de Internet, la rivalidad entre los Estados Unidos y China está empezando a afectar prácticamente a todas las cuestiones tecnológicas.

El segundo elemento de continuidad es el relativo a la **capacidad de las herramientas digitales, en particular las redes sociales, para difundir la desinformación y socavar las instituciones democráticas.** Como señala José Ignacio Torreblanca, la crisis del coronavirus ha puesto de relieve el grado en que los actores tanto extranjeros como nacionales pueden utilizar una combinación de tecnología digital y psicología social para influir en la agenda política en una amplia variedad de programas políticos y manipular los procesos democráticos agravando la polarización política nacional.

La creciente preocupación sobre este problema no ha disminuido todavía su prevalencia y cabe esperar que surjan conflictos en el seno de las sociedades sobre la forma de regular el contenido digital. El hecho de que en Europa las plataformas dominantes de redes sociales sean estadounidenses significa que la lucha por regularlas tendrá también consecuencias geopolíticas.

Un último elemento de continuidad se refiere **a la persistente brecha digital que existe dentro del territorio europeo.** Como enfatiza Alicia Richart, esta brecha no se correlaciona con el tamaño o el poder del Estado. Algunos de los Estados más grandes y ricos de Europa, como Alemania y Francia, están atrasados en el despliegue de infraestructura digital, mientras que otros como Lituania y Grecia lideran este campo. La brecha más crítica también se da dentro de los Estados: entre las zonas urbanas que tienden a tener un acceso efectivo a la infraestructura digital y las zonas rurales. Las brechas digitales tienen todo tipo de efectos perniciosos en la vida de los individuos y en la solidaridad nacional. Pero el coronavirus también ha puesto de relieve la importancia que han adquirido la tecnología y la infraestructura digital para que los países puedan sean resilientes, en particular en momentos de crisis. La fuerte implantación de la infraestructura digital en España, como señala Richart, fue esencial para su capacidad de gestionar el confinamiento y su respuesta general al COVID-19. Así pues, las brechas digitales también amenazan tanto la soberanía como la capacidad de recuperación de Europa cuando llegue la próxima crisis, independientemente de su naturaleza.

Cambio

A pesar de estos elementos de continuidad, las contribuciones a esta colección de ensayos también destacan algunos de los cambios más relevantes

que se han producido en los últimos dos años. El más destacado parece ser la creciente atención y actividad en torno a las cuestiones de soberanía digital en todos los niveles del gobierno en los últimos años. Como la mayoría de los programas de autoayuda sugieren, el primer paso para resolver cualquier problema es reconocer que tienes un problema. Casi todos los ensayos, y en particular el de Torreblanca sobre la desinformación, el de Andrew Puddephatt sobre la gobernanza de Internet y el de Ulrike Franke sobre la IA, documentan un creciente reconocimiento de que la tecnología digital se ha convertido en un campo de batalla crítico en la lucha geopolítica. Esto parece casi hasta cierto punto banal dado el constante goteo de noticias sobre ciberseguridad y desinformación. Sin embargo, es importante recordar que en fechas tan recientes como en 2016, la idea de que los europeos necesitaban concebir, por ejemplo, las plataformas de redes sociales como fuente de poder nacional, seguía siendo un asunto controvertido.

La preocupación por la soberanía digital hace que la competencia digital ya no sea solo económica. Esta toma de conciencia ha dado lugar a una reevaluación de los competidores digitales de Europa. El mayor cambio en la forma de pensar sobre la soberanía digital se debe a l**a creciente preocupación por el abuso de la posición digital dominante de los Estados Unidos.** Como señala Andrés Ortega, hay una creciente sensación de dependencia "neocolonial" de las compañías de Internet de EE. UU. Los esfuerzos europeos por, por ejemplo, imponer un impuesto digital, multar a las grandes empresas tecnológicas estadounidenses por prácticas anticompetitivas, o considerar nuevas políticas industriales para fomentar

a los campeones europeos en sectores clave, reflejan esta creciente incomodidad.

Esta dependencia de los EE. UU., al menos hasta la fecha, supera con creces la dependencia digital europea de China. Pero los ensayos esbozan **una creciente cautela frente a China como competidor económico y político en el ámbito digital.** Si desde la perspectiva de la soberanía digital, los EE. UU. son el mayor problema, China se ha convertido en el mayor temor. Como señala Ortega, China está cada vez más interesada en el mercado europeo y ha estado ascendiendo persistentemente en la cadena de valor. China desafía ahora a las empresas europeas (y estadounidenses) en prácticamente todos los sectores de alta tecnología. Pero, como señala Oertel, los chinos han comenzado a notar el desgaste tras el periodo de gracia de su bienvenida en Europa. La relación de Europa con China se estaba deteriorando rápidamente incluso antes de que la agresiva diplomacia china se convirtiera en un problema adicional durante la crisis del coronavirus. Las finanzas y los equipos chinos siguen siendo atractivos y baratos. Pero los esfuerzos de protección de las inversiones, así como los recientes intentos del Reino Unido y Alemania de replantearse permitir que los equipos de Huawei formen parte del despliegue de la red 5G, por ejemplo, demuestran una mayor preocupación por la amenaza que China puede representar para la soberanía digital europea.

Esta reevaluación de los problemas que tanto los EE. UU. como China representan para la soberanía europea también ha dado lugar a **una nueva forma de pensar en la tecnología del futuro, en particular en lo que respecta a la IA y el desarrollo de nueva regulación en materia de telecomunicaciones.** Tanto Franke como Andrea Renda señalan que muchos Estados miembros de la UE se han convencido recientemente de que la IA representa tanto una amenaza como una oportunidad para la soberanía digital europea. Renda reflexiona sobre el hecho de que, aunque las empresas europeas no aprovecharon recientes oportunidades comerciales derivadas del desarrollo tecnológico, esta nueva toma de conciencia significa que Europa se encuentra bien posicionada para la próxima ola tecnológica. Las empresas europeas poseen ciertas ventajas competitivas en algunas de las tecnologías de la próxima generación, como el Edge Computing, que distribuye la potencia de procesamiento y el almacenamiento de datos más cerca de los lugares donde se necesitan. Merece la pena tener en cuenta que, por ejemplo, cuando la lucha por el 5G termine, habrá una nueva lucha por el 6G.

Los desafíos europeos

Tanto los cambios como la continuidad de ciertos asuntos significan claros desafíos para los europeos en la protección de su soberanía digital.

Como señalan casi todos los expertos en esta colección de ensayos, una desventaja clave de Europa radica en **la falta de empresas digitales europeas con significativa influencia global.** A pesar de las avanzadas capacidades digitales de Europa, no existe un Google o un Tencent europeo. La creciente competencia geopolítica en el ámbito tecnológico ha dejado claro que esta falta de campeones nacionales supone una gran desventaja en la lucha por la soberanía europea. Dicho esto, está mucho menos claro qué hacer al respecto ya que, en el pasado, los esfuerzos para crear campeones europeos a menudo han sido inútiles.

Parte de la respuesta podría consistir en reconocer que Europa también se enfrenta al desafío de **reconciliar los impulsos** liberalizadores **del mercado único con la nueva lucha por la soberanía digital.** Una de las razones por las que Europa carece de campeones digitales es que las empresas más prometedoras a menudo son compradas por grandes competidores extranjeros en el mercado abierto. Además, como señalan tanto Ortega como Oertel, las adquisiciones extranjeras de empresas europeas permiten a los competidores digitales de Europa acceder tanto a la tecnología europea como a la infraestructura digital. La continua ola de esfuerzos por regular la inversión extranjera tanto a escala europea como en los Estados miembros da fe de la concienciación sobre este problema. Sin embargo, la dificultad de llevar a cabo esos esfuerzos sin caer en el proteccionismo, preservando la competencia intra europea que está en el corazón del mercado único, demuestra hasta dónde deben llegar la UE y sus Estados miembros.

El desafío principal para Europa resulta familiar y aunque está implícito en casi todos los ensayos, solo Torreblanca se centra realmente en él: cuando se trata de cuestiones de tecnología, **no está claro que exista una posición europea o incluso que la mayoría de los Estados miembros la quieran.** La multiplicidad de enfoques y posiciones sobre asuntos regulatorios, como la regulación de contenidos, por no hablar de la competencia intra europea por los empleos de alta tecnología, significa que la UE parte en desventaja al competir por la soberanía digital con actores políticos más cohesionados como China o los Estados Unidos. Por otra parte, es evidente que, en comparación con sus rivales, existe un enfoque europeo original sobre cuestiones como la privacidad de los datos. Y, como coinciden Ortega, Oertel, Franke, y Richart, si trabajan juntos, los Estados miembros de la UE pueden aumentar enormemente su influencia global para impulsar ese enfoque común. La necesidad de encontrar el equilibrio entre los compromisos que exige la formación de una posición común y la necesidad de proteger los intereses particulares de los distintos Estados miembros seguirá siendo, sin duda, un reto para los responsables políticos europeos.

Oportunidades europeas

Si bien todos estos desafíos son ciertamente desalentadores, los expertos en esta colección de ensayos también destacan considerables oportunidades, tanto tecnológicas como políticas, que los europeos aportan a la lucha por conservar la soberanía digital.

Como subrayan muchos de los autores, la oportunidad más clara de la UE es **ejercer su poder regulador para configurar el entorno internacional** sobre cuestiones digitales. El poder regulador se refiere a la capacidad de Europa de aprovechar el acceso al mercado de la UE, y su marco jurídico para crear y hacer cumplir las normas, a fin de alentar a otros Estados a seguir la práctica europea. En el ámbito digital, el ejemplo más destacado de este esfuerzo es el RGPD (Reglamento General de Protección de Datos), que ha obligado a las empresas de todo el mundo a cumplir con las prácticas europeas en materia de privacidad y ha fomentado la adopción de reglamentos similares en otras jurisdicciones, incluso en diversas partes de Estados Unidos. Franke sugiere que existe una oportunidad similar para ejercer el poder regulador en el sector de la IA. Sugiere que el hecho de centrarse en la creación de un marco regulador europeo para una IA ética podría inspirar a otros a emularlo y forzar el cumplimiento de las ideas europeas de cómo controlar esta industria del futuro. Torreblanca sostiene que los europeos tienen una oportunidad similar de liderar la regulación de los contenidos digitales.

Lo que es más polémico es que algunos de los autores sugieren que la UE también tiene la oportunidad de **utilizar sus conocimientos en materia de política de la competencia para obtener una ventaja en algunas tecnologías emergentes clave.** Renda, por ejemplo, señala que el próximo paso desde el control de la nube a la gobernanza de los datos distribuidos, en la que las normas para la gestión de los datos se establecen en la jurisdicción en la que estos residen, dan a la UE una ventaja competitiva. Del mismo modo, Richart ve una oportunidad de utilizar los próximos avances en Edge Computing para poner el almacenamiento y los flujos de datos bajo el control regulador europeo. Como se ha señalado, los resultados de este tipo de política industrial en Europa son muy variados, pero la constatación de que está en juego la soberanía digital de Europa ha inspirado una nueva voluntad de experimentar.

Finalmente, algunos de los autores ven incluso una oportunidad en la profundización de la competencia entre EE.UU. y China en cuestiones de tecnología. Las marcadas diferencias entre el anárquico enfoque estadounidense de la regulación digital y el pesado modelo de control estatal propugnado por China abren un vasto terreno intermedio para los actores europeos. Tanto Oertel como Burwell señalan que esto podría brindar **una oportunidad para que los actores europeos sirvan de mediadores en las controversias entre Estados Unidos y China.** El papel de mediador no es congruente con la idea de que los europeos tengan su propio enfoque, pero, por supuesto, el uso inteligente de la posición también brinda la oportunidad de dar forma al resultado. Sin embargo, la mediación no debería implicar una equidistancia entre EE.UU. y China. A pesar de las quejas sobre el comportamiento de EE.UU. en el ámbito digital, Oertel, Burwell, Renda y Torreblanca expresan un profundo escepticismo sobre la capacidad de la UE para encontrar el tipo de compromisos con China que a menudo maneja con EE.UU. Quizás Ortega y Puddephatt parecen algo más optimistas acerca de trabajar con China, aunque reconocen que su modelo autoritario planteará, sin duda, serias limitaciones.

No hay vuelta atrás

Desgraciadamente, no hay nadie que redoble los tambores anunciando la retirada de la tecnología digital. La lucha competitiva por la soberanía digital es, por lo tanto, el destino de Europa y de todos. Estamos avanzando, para bien o para mal, hacia un futuro cada vez más digital, probablemente lleno de IA más inteligente, comunicaciones más rápidas y desinformación más sofisticada. Esta colección de artículos representa un esfuerzo por aceptar ese hecho ineludible, pero también por darse cuenta de que ofrece a Europa tanto una oportunidad como un peligro. Los europeos no pueden dejar de avanzar, pero con un poco de reflexión, compromisos políticos difíciles y un liderazgo sabio, pueden dar forma a un futuro digital europeo.

Regulando Internet: la creación de un modelo europeo

Andrew Puddephatt
Presidente ejecutivo del Consejo Asesor de Global Partners Digital

En febrero de 1958, en respuesta al lanzamiento del Sputnik 1 por parte de la Unión Soviética un año antes, el presidente de Estados Unidos, Dwight Eisenhower, creó la Agencia de Proyectos de Investigación Avanzados (ARPA). El objetivo de la organización era invertir en tecnologías que fortalecieran la seguridad nacional. Su investigación sobre sistemas de comunicación que pudieran resistir un ataque nuclear llevó en 1966 a la creación de ARPANET. Mientras que las comunicaciones anteriores se basaban en circuitos (enlaces *end-to-end*, como las líneas telefónicas), ARPANET utilizaba la conmutación de paquetes. Esto permitió al sistema dividir los datos en paquetes y transmitirlos por diferentes canales, antes de reensamblarlos en el punto de destino. ARPA desarrolló el protocolo de control de transmisión (TCP) y el protocolo de Internet (IP) para determinar cómo se deben descomponer, direccionar, transmitir, enrutar, recibir y reensamblar los datos. La aplicación de estos protocolos a la radio, satélite y otras redes estableció un sistema en el que los datos se movían a través de medios muy diferentes. El término que se utilizó para describir el sistema, *inter-networking*, pronto se convirtió en Internet.

Una de las características clave de esta nueva tecnología era que su configuración no se determinaba de forma centralizada sino por el proveedor de la red. Las redes independientes se conectaban entre sí mediante un meta-nivel, una "arquitectura de interconexión", a pesar de que habían sido diseñadas por separado y tenían sus propias interfaces. A diferencia de los medios de comunicación de masas tradicionales (como los periódicos, la radio y la televisión), Internet funcionaba sin necesidad de coordinación nacional o mundial. Como tal, la gobernanza de Internet parecía inicialmente innecesaria. Aunque Internet funcionaba de acuerdo con sus propias normas, se consideraba que estas eran más funcionales que los marcos normativos existentes debido a su naturaleza técnicamente compleja.

A mediados de la década de 1980, Internet sustentó el trabajo de una creciente comunidad de investigadores y desarrolladores de ámbito académico. Funcionaba como un acuerdo informal entre grupos de personas con ideas afines que estaban dispuestas a cooperar para construir y desarrollar la red. Sin embargo, a medida que crecía más allá de unas pocas universidades, la red necesitaba cierta gestión (por ejemplo, para crear y asignar nuevas direcciones). En esta etapa, la administración de los registros de identificadores IP (incluyendo la distribución de los dominios de primer nivel y las direcciones IP) la realizó una única persona, Jon Postel, que pertenecía a UCLA. A medida que su carga de trabajo se hizo inmanejable, cuando más países empezaban a utilizar la tecnología, había que encontrar un nuevo sistema, y a medida que Internet se convertía en una red global, se hizo evidente que era necesario unos estándares tecnológicos universalmente aceptados.

Desde su creación, la gobernanza técnica de Internet había funcionado sin un control gubernamental directo. En la práctica, los ingenieros y las empresas con sede en los Estados Unidos tenían autoridad de

facto para desarrollar sus propios protocolos de ingeniería. Antes de 1998, la gobernanza de Internet no había sido una cuestión política relevante en Europa. Pero todo esto cambió cuando el gobierno de EE.UU. presionó con éxito para establecer la Corporación de Internet para Nombres y Números Asignados (ICANN), una organización privada sin fines de lucro que asumió el papel de Postel en la gestión de los dominios. Los gobiernos de todo el mundo comenzaron a mostrar interés y a posicionarse sobre el tema.

Para el gobierno de EE. UU, era crucial que Internet fuera gobernada por un conjunto de organizaciones no gubernamentales y privadas a través de ICANN. Washington prefería una solución orientada al mercado que implicara la autorregulación de Internet por parte del sector privado, en parte porque protegía los intereses económicos de los Estados Unidos. En cambio, la Unión Europea abogó por un sistema público-privado en el que los gobiernos tuvieran un papel más relevante: un marco institucional multilateral. China, Rusia y otros países querían un sistema de gobernanza de Internet basado únicamente en el Estado, preferiblemente uno anclado en las Naciones Unidas. La UE finalmente apoyó la posición de los Estados Unidos, pero consiguió que los gobiernos tuvieran un papel en la estructura institucional de ICANN, asegurando que los europeos formaran parte de los comités de la organización.

Sin embargo, esos asuntos técnicos eran solo uno de los aspectos de la gobernanza de Internet. Las cuestiones políticas eran más complejas. A medida que el poder de una red de comunicaciones interconectada a escala mundial se hacía evidente, los gobiernos comenzaron a darse cuenta de que estaban perdiendo rápidamente el control sobre las tecnologías de la comunicación. El uso de Internet aumentó de manera exponencial, pero la falta de un marco normativo general hizo que lo que se conoció como "innovación sin permiso" fuera predominante en su desarrollo. Internet utilizó la infraestructura de telecomunicaciones existente, la red telefónica, para crecer orgánicamente, sin necesidad de realizar importantes inversiones en aquellos países en los que había una sólida infraestructura de telecomunicaciones. Cualquiera podía conectar su ordenador a la red y formar parte de Internet: las empresas no necesitaban permiso para lanzar un servicio y no tenían que superar ninguna barrera regulatoria. En consecuencia, Internet creció más como un ecosistema orgánico que como una red planificada. La colaboración y el consenso entre los proveedores de servicios era el método de tomar decisiones.

Internet nació de un sueño libertario. Sus primeros creadores y defensores lo imaginaron como un espacio sin Estado, al margen de cualquier control gubernamental. De hecho, muchos creían que cualquier tipo de gobierno de Internet destruiría su naturaleza. En la fase inicial del desarrollo de Internet, los ingenieros, técnicos, empresas y usuarios que impulsaron el proceso se contentaron con desarrollar un gran espacio de comunicación sin preocuparse de cómo se utilizaría. No parecían imaginar los efectos nocivos que podrían surgir sobre la libertad de expresión anónima y sin restricciones, el abuso de menores, el trolling, el acoso de las minorías y la propagación del terrorismo. La cultura que rodea a la Primera Enmienda de los Estados Unidos, que fomenta la libertad de expresión y limita las responsabilidades de los operadores, fue crucial para el desarrollo de Internet. Muchos de los primeros innovadores y creadores del mundo digital procedían de los Estados Unidos, donde podían experimentar sin preocuparse de futuras responsabilidades. Como medio de comunicación en inglés en la mayor parte del mundo, que solo estaba disponible para las élites, Internet inicialmente pasó por debajo del radar de muchos gobiernos que se inclinaban a censurar y controlar las comunicaciones.

A principios del siglo XXI comenzó una nueva era. Los gobiernos de todo el mundo ya estaban muy pendientes de las disrupciones que podía causar el acceso a las comunicaciones digitales, ya fuera mediante mensajes de texto con teléfonos móviles, el uso creativo de plataformas sociales como Facebook y Twitter, la transmisión de vídeo directamente a la web o el uso de Internet para eludir la censura. Los gobiernos buscaban de manera creciente nuevas formas de controlar y vigilar el espacio online. Al mismo tiempo, en todo el mundo crecieron los llamamientos para que este entorno no regulado se sometiera al control de los gobiernos, llamamientos motivados en los Estados democráticos por el miedo al crimen y al terrorismo, y en los autoritarios por el deseo de los gobiernos de preservar su poder.

A medida que Internet crecía en tamaño y capacidad, se produjo un fuerte aumento de la capacidad de los Estados y los actores no estatales de usar las tecnologías digitales con el fin de perturbar y controlar las comunicaciones y, de ese modo, socavar los procesos democráticos. Las redes criminales explotaron estas capacidades y corroyeron la confianza en el entorno online. Los regímenes represivos utilizaron a los hackers para perturbar a los grupos prodemocracia y de derechos humanos. Las nuevas empresas de comunicación se volvieron cada vez más poderosas. Como ha documentado Timothy Wu, todos los medios de comunicación dominantes del siglo XX, ya sea la radio, la televisión, el cine o la telefonía, nacieron en un entorno abierto y libre. Todos tenían el potencial para un uso sin restricciones, pero con el tiempo todos cayeron bajo el control de los monopolios. Un patrón similar surgió en el mundo digital. Internet se enfrentaba a un desafío tanto del poder público como del privado y, a veces, a una combinación mortal de ambos.

Aunque muchos gobiernos condenan la aparente falta de normas en Internet, existe una gobernanza online. Esa gobernanza la llevan a cabo las principales empresas a través de sus condiciones de servicio, normas comunitarias y procedimientos de selección. Los algoritmos corporativos clasifican, evalúan, califican y recomiendan las elecciones de los usuarios, constituyendo un tipo de gobernanza del mercado. Por lo tanto, la cuestión para muchos gobiernos no es que Internet no tenga leyes, sino que sus leyes las deciden empresas privadas con sus propios códigos y algoritmos.

Países como China, que intenta ejercer un control total sobre su entorno nacional de comunicaciones, rechazan cualquier noción de una red de comunicaciones independiente fuera de la supervisión estatal. El objetivo general de la diplomacia china es promover la noción de soberanía cibernética (o de Internet). En palabras del Presidente Xi Jinping, esto significa "respetar el derecho de cada país a elegir su propio camino para el desarrollo de Internet, su propio modelo de gestión de Internet, [y] sus propias políticas públicas en Internet". El modelo chino de Internet da prioridad al control a través de una amplia gama de herramientas y tecnologías que bloquean, filtran o manipulan el contenido online. Tiene normas para el almacenamiento de datos en servidores en el país, lo cual (aunque Pekín lo presenta como una forma de limitar el poder de las empresas estadounidenses) ayuda a las autoridades a acceder a la información de los usuarios.

El objetivo deseado por China está muy lejos de la visión estadounidense de un Internet global dirigido por el sector privado. Pekín quiere ver una serie de "internets" nacionales interconectados en lugar de una infraestructura global, con cada Internet nacional gobernado por las leyes y valores de su Estado de origen. Considera que el modelo de adopción dirigido por el sector privado que ha dado forma al crecimiento inicial de Internet expresa el dominio de Occidente, en particular de los Estados Unidos, lo que se refleja en el apoyo que recibe de una coalición de empresas de tecnología y grupos de la sociedad civil. Los responsables políticos chinos quieren que la ONU desempeñe un papel más relevante en la gobernanza de Internet, ya que creen que pueden reforzar su influencia a través de la organización o de otros foros multilaterales de base estatal.

Europa se encuentra entre estos dos polos, aunque, diplomáticamente, normalmente se ha venido adaptando a EE.UU. A nivel interno, la UE y sus Estados miembros han comenzado a jugar un papel importante en la conformación de las normas de contenido de las plataformas. En Europa, un vasto conjunto de regulaciones de rango menor, usos y costumbres y procedimientos establecidos ("*soft law*"), que comprenden la autorregulación, los diálogos y los memorandos de entendimiento, las iniciativas *multi-stakeholder* y los foros de colaboración han contribuido a elaborar políticas y prácticas en materia de contenido *online*. Sin embargo, no existe un medio sistemático de incentivar a las plataformas para que evalúen y aborden los problemas de perjuicio e ilegalidad que puedan surgir en sus ecosistemas, cuando sus incentivos comerciales para hacerlo son insuficientes, o de evaluar la eficacia de sus respuestas.

Métodos de gobernanza

El establecimiento de ICANN no resolvió el problema de la gobernanza mundial de Internet. La preocupación por la posición de dominio de EE.UU. en Internet creció junto con la relevancia de la tecnología. A medida que Internet crecía tras la invención de la World Wide Web, con el fin de incluir una creciente diversidad de idiomas y contenidos, un pequeño número de empresas estadounidenses comenzó a dominar los servicios que se ofrecían (como Facebook en las redes sociales y Google en los motores de búsqueda).

La Unión Internacional de Telecomunicaciones (UIT), un organismo de las Naciones Unidas cuyos orígenes se remontan al desarrollo del telégrafo submarino en el siglo XIX, comenzó a liderar los esfuerzos para regular Internet a principios de la década de 2000 que, en esta etapa, se llevaba cabo mayormente sobre la infraestructura de telecomunicaciones existente. En respuesta a las solicitudes de los Estados miembros, la UIT convocó la Cumbre Mundial sobre la Sociedad de la Información (CMSI) para examinar, entre otras cosas, el futuro de la gobernanza mundial de Internet. La CMSI se reunió en Ginebra en 2003 y en Túnez en 2005. Este último evento se realizó bajo la tutela de grupos de presión autoritarios: los empleados del gobierno tunecino que se hacían pasar por miembros de organizaciones ficticias dominaban las reuniones que los grupos de la sociedad civil habían organizado al margen. El rencor generado por esta represión abierta de las voces independientes en Túnez socavó los esfuerzos por incluir a los gobiernos en el control de Internet. Como ya se ha dicho, Washington estaba decidido a evitar todo aquello que pudiera conducir a esa toma de control, posición que los Estados miembros de la UE apoyaron en última instancia.

Esto llevó a la creación del Foro para la Gobernanza de Internet (IGF, por sus siglas en inglés), una organización *multistakeholder* de las Naciones Unidas destinada a prestar asesoramiento o, en el mejor de los casos, a establecer normas. El IGF tiene un mandato de cinco años que ha sido renovado continuamente. Funciona principalmente a través de su reunión anual, aunque en otras ocasiones se coordina con grupos de trabajo y de asesoramiento. El IGF ha establecido oficinas regionales y nacionales, que se reúnen con diversos grados de participación

de organizaciones y empresas locales en diferentes países. Su falta de autoridad formal nunca iba a satisfacer a los Estados autoritarios que han presionado para establecer un sistema que les otorgue un mayor control sobre Internet. Por consiguiente, estos Estados raramente enviaron representantes al IGF. Y, a lo largo de los años, el nivel de asistencia de alto nivel de los gobiernos occidentales ha disminuido. Las grandes empresas ya no invierten recursos significativos en el IGF, mientras que la mayoría de sus asistentes pertenecen a grupos de la sociedad civil.

Por otra parte, se está promoviendo un sistema de gobernanza mundial de Internet con una mayor participación de los Estados. La Organización de Cooperación de Shanghái, una organización intergubernamental creada en 2001 por China, Kazajistán, Kirguistán, Rusia, Tayikistán y Uzbekistán ha actuado sistemáticamente como un vehículo para desafiar los modelos de gobernanza de Internet existentes. En 2015 esta organización presentó un código de conducta con recomendaciones sobre seguridad de la información a la Asamblea General de la ONU. Su objetivo era promover los derechos y responsabilidades de los Estados en ese ámbito y mejorar la cooperación intergubernamental abordando las amenazas y los desafíos comunes que incluían los que plantea la libertad de expresión en los estados autoritarios. Esta iniciativa se topó con la oposición de EE.UU. y sus aliados, incluyendo la UE. En el contexto geopolítico han ido aumentando los intentos de crear un marco global para la gestión de Internet. Ha resultado imposible llegar a un consenso incluso en temas como la ciberseguridad, en los que hay un terreno común sobre la necesidad de contrarrestar amenazas como el terrorismo, la explotación infantil y otros delitos graves.

No obstante, el concepto de gobernanza de Internet sigue siendo muy necesario. Se ha transformado en una multitud de cuestiones tratadas por diversos actores en diferentes foros. Si bien en algún momento pudo haber tenido sentido abogar por un marco global para regularla, Internet se ha convertido en parte de la vida cotidiana de las personas que afecta a todas las áreas de las políticas públicas, una tendencia que se ha visto reforzada por las políticas de distanciamiento

social que han seguido a la pandemia del COVID-19. Como Internet sustenta la mayor parte de la vida laboral y social de las personas, estos problemas de gobernanza aparecen en todas partes. En algunas áreas, como la propiedad intelectual, puede ser posible establecer un consenso mundial. En otros, la geopolítica bloqueará previsiblemente cualquier progreso, y los sistemas de gobernanza se delegarán en bloques regionales y nacionales.

Uno de los problemas del término "gobernanza de Internet" es que tiene diferentes significados para los distintos gobiernos. Para algunos, "gobernanza" significa "gobierno", un medio de comunicación omnipresente y un activo estratégico que requiere el control del Estado. Para otros, la gobernanza es una cuestión puramente técnica, relativa a los protocolos necesarios para garantizar que la infraestructura funcione y evolucione. Para otros, la gobernanza debería centrarse simplemente en mitigar los daños que se derivan de lo que es un medio esencialmente del sector privado. Y luego están los que lo ven como una forma de frenar el poder de las empresas estadounidenses y, cada vez más, chinas que únicamente responden ante los gobiernos nacionales.

La experiencia de la UE

La UE tiene una larga historia en el desarrollo de políticas de Internet, aunque no en la gobernanza. Desde mediados de los años 90, la UE se ha preocupado por los posibles daños causados por Internet. En un principio, la UE priorizó el soft law en su política digital, pero en los últimos dos o tres años, ha pasado a un enfoque más proactivo e intervencionista. Hoy en día, la UE tiene el marco político, jurídico y reglamentario más desarrollado sobre cuestiones de Internet en todo el mundo.
El poder de la UE se basa en su poderío económico. Su mercado único tenía un PIB de 15,9 billones de euros (18 billones de dólares) en 2018, el mayor del mundo. Aunque la salida del Reino Unido de la UE lo reducirá dependiendo de su grado de alineamiento con el mercado, el bloque regional seguirá ejerciendo una autoridad significativa sobre las empresas que deseen hacer negocios en su territorio. La UE representa un lucrativo mercado para las empresas de Internet: en marzo de 2019, se estimaba que el 90 % de la población de la UE utilizaba Internet, oscilando entre 98 % en Dinamarca y 67 % en Bulgaria.

Desde el primer momento, la UE reaccionó positivamente a Internet reconociendo su importancia social, educativa y cultural, y reconociendo al mismo tiempo su potencial para difundir contenidos nocivos e ilegales, y su capacidad para facilitar la comisión de delitos graves. El enfoque europeo en materia de política de Internet evolucionó para ocuparse de los proveedores de servicios de Internet que crean y gestionan la infraestructura en lugar de las plataformas que surgieron en el siglo XXI. En sus primeros años, la política europea de Internet tenía dos principios rectores desarrollados con los proveedores de servicios de Internet (ISPs) en mente. Uno de ellos era la neutralidad de la red, que requería que los ISPs no discriminaran los datos en sus redes. El otro era la limitación de responsabilidad, lo que significaba que ningún proveedor podía ser considerado responsable por albergar contenido ilegal, siempre que eliminara dicho contenido después de tener conocimiento de este. Esta limitación de responsabilidad figura en la Directiva sobre el comercio electrónico. Los artículos 13 y 14 de dicha Directiva establecen que, para estar protegidos, los proveedores que albergan contenido deben actuar "rápidamente para eliminar o desactivar el acceso" a la información cuando tengan "conocimiento real" de su ilegalidad, y los proveedores que almacenan contenido deben hacerlo después de recibir una orden a tal efecto.

El rápido crecimiento de las empresas de servicios estadounidenses, como Amazon, Facebook y Google, sus increíbles capitalizaciones de mercado y la falta de empresas europeas similares capaces de competir con ellas, llevaron a la UE a replantearse su política. A medida que el valor generado por Internet parecía acumularse cada vez más en las empresas estadounidenses, los responsables políticos europeos empezaron a cuestionar la idoneidad del principio de limitación de responsabilidad. Las plataformas de Internet no actúan simplemente como anfitriones neutrales de contenidos proporcionado por otros, sino que utilizan algoritmos para rastrear el comportamiento de los usuarios, y seleccionan o ajustan el contenido para reflejar sus necesidades. A este respecto, las plataformas se asemejan más a los editores que son responsables del contenido en el que trabajan, que, a una empresa de servicios telefónicos, que no es responsable de las conversaciones sobre sus líneas. Y la opacidad de estas empresas sobre los algoritmos utilizados, considerados secretos comerciales, ha hecho difícil para los observadores externos juzgar si dan forma o simplemente reflejan el mundo que los usuarios experimentan en Internet.

La UE no es un actor geopolítico importante que pueda imponerse a las superpotencias. Tampoco ha creado plataformas globales capaces de ejercer influencia en todo el mundo. Pero tiene una herramienta que le permite dar forma a la gobernanza de Internet: la regulación que aplica a su mercado y los requisitos que impone a las empresas que desean comerciar en la UE. Debido al tamaño y valor del mercado de la UE, las multinacionales quieren comerciar en Europa. Al hacerlo, están obligadas a cumplir con las regulaciones de la UE.

Otros países observan el enfoque del bloque regional en cuanto a la gobernanza de Internet y reproducen los aspectos del mismo que parecen tener éxito. Al descubrir que tienen que introducir nuevos procedimientos internos para hacer negocios en la UE, las empresas cambian su comportamiento.

La UE se centra actualmente en el ambicioso objetivo de crear un mercado digital único. Esto se establece en la Estrategia para el Mercado Único Digital de la Comisión Europea, que estima que podría aumentar el PIB de la UE en 415.000 millones de euros. La estrategia es considerablemente más intervencionista que otros enfoques anteriores, y tiene por objeto establecer un marco normativo armonizado que proporcione a las empresas y los consumidores un acceso sin restricciones a los bienes y servicios digitales en toda la UE. Aunque sus objetivos son nacionales, la estrategia tiene implicaciones de gobernanza para cualquier empresa que desee hacer negocios en la región.

Un ejemplo de ello es el Reglamento P2B, que tiene por objeto promover la equidad y la transparencia para las empresas que utilizan plataformas digitales. Este reglamento trata de dar respuesta a las reiteradas preocupaciones sobre la forma en que las plataformas favorecen sus propios servicios. Aunque todavía no se ha aprobado oficialmente, el Reglamento P2B refleja una serie de preocupaciones sobre el comportamiento de las plataformas americanas, a las que exigirá que se ajusten a normas específicas cuando operen en el mercado de la UE. La Comisión Europea ya ha multado a Google por abuso de su posición dominante en los mercados de publicidad digital y de compra online, así como por imponer restricciones a los fabricantes de dispositivos Android. Actualmente, la Comisión está llevando a cabo investigaciones tanto en Amazon como en Apple.

Otra iniciativa política que ha atraído la atención mundial es el Reglamento General de Protección de Datos (RGPD). Este entró en vigor el 25 de mayo de 2018 con el objetivo de proteger a los ciudadanos de la UE de las violaciones de la privacidad y los datos online. Se basa en los principios de protección de datos offline, pero aborda las implicaciones de los avances tecnológicos. Está diseñado para proteger la privacidad de datos de todos los ciudadanos de la UE y remodelar la forma en que los controladores de datos de las empresas de toda la región abordan la cuestión. Es importante señalar que el RGPD es aplicable a cualquier organización que tenga datos personales de personas que residen en la UE, independientemente de su ubicación. En virtud del reglamento, la UE puede multar a las organizaciones con hasta el 4 % de su volumen de negocios global anual o 20 millones de euros, la cantidad que sea mayor, por infracciones graves y hasta el 2 % de su volumen de negocios global anual o 10 millones de euros por infracciones de sus obligaciones de protección de datos.

Muchos países fuera de la UE están estudiando el desarrollo del RGPD para adoptar una legislación similar. Incluso ha tenido un impacto en Estados Unidos, donde algunos Estados están considerando adoptar disposiciones para proteger la privacidad que se asemejan mucho a los aspectos del reglamento. Es probable que la Estrategia para el Mercado Único Digital de la UE, que implicará mayores controles reglamentarios sobre las empresas digitales, tenga repercusiones mundiales similares.

Algunos observadores han sugerido que el mundo podría tener pronto tres “Internets”. Un Internet estadounidense en el que las normas establecidas por las empresas proporcionan una gobernanza de facto; un Internet chino controlado a escala nacional, que sirve a los intereses del Estado y facilita una vigilancia digital integral; y un Internet europeo en el que la UE actúa en interés público para regular las operaciones de los mercados y empresas digitales.

Dado el estancamiento geopolítico acerca de la gobernanza de Internet, es casi seguro que el debate sobre la cuestión se trasladará a las distintas iniciativas nacionales y regionales. Se considera que el modelo estadounidense fomenta los intereses propios de las empresas estadounidenses, una impresión que se ha visto reforzada por las declaraciones de las administraciones demócrata y republicana. El modelo chino, por su parte, atrae sobre todo a los gobiernos autoritarios. Así pues, el modelo europeo se perfila como un modelo que los gobiernos democráticos, deseosos de preservar un mercado abierto de servicios digitales al tiempo que protegen los intereses de los ciudadanos, encuentran cada vez más atractivo.

La gobernanza de Internet no se desarrollará principalmente en el Internet Governance Forum (IGF), ni en la Primera Comisión de las Naciones Unidas, ni siquiera en la Unión Internacional de Telecomunicaciones (UIT), por muy importante que sea cada uno de estos foros. Es probable que surja de iniciativas específicas, burocráticas y dolorosamente negociadas para dar forma al mercado e incentivar el comportamiento de las empresas, a partir de un enfoque respaldado por la amenaza de sanciones. Estas son cualidades que, para bien o para mal, la UE tiene en abundancia y de las que otros carecen.

China: confianza, 5G y el factor coronavirus

Janka Oertel
Directora del Programa de Asia del European Council on Foreign Relations

La actual confrontación entre EE.UU. y China no es sino una batalla por la supremacía global. Esta pugna por la influencia y el liderazgo se desarrolla simultáneamente en varios ámbitos económicos, pero ante todo en el sector de la tecnología. En los últimos años, se ha hablado mucho del surgimiento de una nueva "guerra fría tecnológica". Sin embargo, la analogía puede resultar engañosa: simplifica en exceso la dinámica en juego y no hay nada de frío en ella. Por el contrario, la confrontación es candente y feroz, y se desarrolla en tiempo real. Washington y Pekín experimentan enfrentamientos en distintos campos de batalla con diferentes grados de intensidad. Europa ya se ha visto atrapada en el fuego cruzado del 5G y muy probablemente las cosas empeorarán.

Las cadenas de suministro y de valor de la tecnología se diseñaron tanto para ser eficientes como rentables a través de una estrecha interdependencia y una producción mundial altamente especializada. Las empresas europeas son parte inherente de este modelo: están profundamente integradas en las cadenas de valor y desempeñan un papel relevante en momentos claves de esta, desde las redes de acceso radioterrestres (RAN) hasta la fotolitografía utilizada en la producción de semiconductores. En todo caso, el nacionalismo tecnológico aumenta a la vez que se desmantelan las actuales estructuras, un proceso que la crisis del coronavirus está acelerando. En la recuperación de una pandemia que ha impactado duramente a la economía mundial, los Estados deberán reordenar sus intereses y prioridades. Europa necesita encontrar un nuevo espacio en la dinámica emergente. Washington fracasó inicialmente en su virulenta campaña de presión a sus aliados para que prohibieran al fabricante chino Huawei y a su competidor estatal, ZTE, participar en el despliegue de las redes de telecomunicaciones 5G. Los líderes europeos, especialmente los que se encuentran en el corazón de la Unión Europea, se mostraron reacios a actuar con decisión contra las empresas que habían sido socios importantes durante años y que seguían siendo una parte clave de sus sistemas 3G y 4G.

Las políticas estadounidenses encendieron un acalorado debate en toda la UE sobre la futura composición de la infraestructura de telecomunicaciones y, en general, sobre las relaciones con China. Las autoridades estadounidenses defendían que los proveedores chinos representaban una gran amenaza de seguridad para la infraestructura de comunicaciones de Europa. Sin embargo, los campeones tecnológicos chinos, especialmente Huawei, representaban la fortaleza de un ecosistema tecnológico que podía rivalizar con el de Silicon Valley. Efectivamente, con frecuencia así lo hacían ya que se beneficiaban de los enormes subsidios estatales, las condiciones favorables del mercado interno de China, el robo de la propiedad intelectual, las transferencias forzadas de tecnología y las cantidades ingentes de capital destinadas a la investigación y el desarrollo respaldadas por el Estado que impulsaban la innovación autóctona.

A Washington le interesa muy especialmente tanto frenar el deterioro del dominio tecnológico americano

como ralentizar el ascenso del poder de China, especialmente en medio de una pandemia que ha paralizado gran parte de la economía de los Estados Unidos y que ha situado el desempleo en ese país en su máximo histórico, sin contar con que la emergencia sanitaria probablemente irá seguida de una recesión. Para minimizar las ganancias relativas de China, la administración de EE.UU. está dispuesta a maximizar la presión económica sobre Pekín.

En mayo de 2020, el Departamento de Comercio de EE.UU. presentó la última de una larga lista de medidas que ha ido aplicando para lograrlo: impuso estrictas restricciones a las ventas de microchips a Huawei y sus empresas subsidiarias. Con este movimiento, la Oficina de Industria y Seguridad (BIS) de dicho Departamento asestó un gran golpe al campeón tecnológico chino. Huawei rápidamente reconoció que se encontraba luchando por su supervivencia.

La BIS decidió que, además de imponer restricciones a las ventas directas a Huawei, también exigiría a la empresa que solicitara licencias para la compra de semiconductores que fueran "producto directo del diseño y la tecnología de los Estados Unidos". Los semiconductores son críticos para la cadena de suministro de Huawei y uno de los pocos puntos de estrangulamiento que quedan para las ambiciones tecnológicas de China, ya que la capacidad del país para producirlos en masa se limita a unas pocas empresas. Por ello, la última maniobra jurídica se dirige particularmente a la empresa Taiwán Semiconductor Manufacturing Company (TSMC), que representa más del 50% de las ventas mundiales. La empresa se ha convertido en el centro de la confrontación entre los Estados Unidos y China, ya que Huawei necesita acceder a microchips de alto rendimiento para alcanzar sus ambiciosos objetivos con respecto al 5G. Durante años, el argumento de peso para Huawei ha sido que puede proporcionar bienes de alta calidad rápidamente y a bajo costo. Ahora todo se ha complicado mucho más para la compañía.

Las consecuencias de la decisión de la BIS aún no están claras; sigue habiendo muchas lagunas. Pero, con este último bombardeo contra el sector tecnológico chino, Washington ha dejado claro que se toma el asunto muy en serio. Y la crisis actual también juega un papel muy importante, porque Estados Unidos teme que China, al terminar antes que otros países el confinamiento económico provocado por el coronavirus, obtenga un mayor beneficio. China es un competidor económico que está saliendo antes que otros de la primera fase de la pandemia; y ello gracias a la naturaleza autoritaria de su régimen, su alto grado de digitalización y unas estructuras de vigilancia ciudadana, que se extienden hasta el nivel de las comunidades más pequeñas. Estas estructuras sociales, anteriores a la era digital, capacitan al gobierno para tener un mayor control de los brotes obteniendo un éxito mayor que los gobiernos en Occidente. Incluso en el momento más álgido de la emergencia sanitaria, siguieron funcionando sectores de importancia estratégica, como la industria autóctona de microchips, aunque con una capacidad ligeramente más reducida. Y, a estas alturas, el sector tecnológico casi ha vuelto a su nivel de productividad anterior a la crisis.

Los dirigentes chinos han anunciado paquetes de estímulo muy sustanciales para compensar las pérdidas económicas creadas por el confinamiento, poniendo el despliegue de 5G y la construcción de centros de datos en el eje central de estas medidas. El despliegue a escala nacional del 5G con hasta 600.000 estaciones base, anunciada a finales de marzo, podría dar a las empresas chinas una enorme ventaja competitiva sobre sus rivales en su esfuerzo por digitalizar la economía. Y todavía hay más medidas previstas: China va a invertir 1,4 billones de dólares para impulsar su sector tecnológico en los próximos cinco años.

Si bien actualmente tiene la intención de abordar las solicitudes de licencia denegándolas sistemáticamente, la BIS todavía podría concedérselas a la TSMC para una producción limitada. Esto podría ser necesario para asegurar que la compañía siga siendo competitiva, ya que las ventas a China constituyen casi el 20 % de su negocio. Huawei llevaba tiempo esperando que se produjera un deterioro de las relaciones entre los Estados Unidos y China y por ello cuenta con casi toda seguridad con una importante reserva de los suministros más críticos. Sin embargo, dados los rápidos ciclos de innovación del sector tecnológico, estos solo serán útiles durante un tiempo limitado. En consecuencia, no está claro cuánto tiempo durarán estos suministros, o con qué rapidez las empresas chinas podrán encontrar soluciones autónomas al problema. Aunque el gobierno chino le da mucha importancia a esta vía, y está invirtiendo mucho dinero en ellas, no tendrá alternativas reales a los productos no chinos en la escala necesaria a corto plazo.

El último movimiento de la BIS hará que Huawei sea menos internacional y más china. La compañía tendrá que dar prioridad al enorme mercado nacional de 5G, incluso a expensas de los clientes de otros países. En consecuencia, la capacidad de Huawei para cumplir los compromisos adquiridos se ha convertido en un elemento de considerable importancia para los operadores y gobiernos europeos a la hora de decidir la composición de su nueva infraestructura de red. Confiar en Huawei podría ser una apuesta arriesgada no solo en términos de política y seguridad sino también en términos económicos.

El debate europeo sobre el 5G

En el debate sobre el 5G, los medios de comunicación han defendido que los operadores de telecomunicaciones europeos no excluirían a los fabricantes chinos, dando a entender que EE.UU. han perdido la batalla sobre este asunto. Pero, en realidad, el debate está lejos de haber terminado y estará fuertemente influenciado por el coronavirus. A finales de abril, se esperaba que los Estados miembros de la UE debían informar sobre las medidas que habían tomado para cumplir con las recomendaciones establecidas por la UE en conjunto de instrumentos y directrices políticas para la seguridad de las redes 5G en tanto que infraestructura crítica. Prácticamente todos los Estados miembros de la UE lo han hecho, aunque algunos de ellos además han tomado decisiones definitivas sobre el papel de los proveedores de alto riesgo.

Todavía está pendiente el debate sobre este asunto en los Países Bajos, donde el operador KPN ha anunciado que cambiará de Ericsson a Huawei para mantener su red de acceso. Otros países europeos han aprobado legislación nacional en este campo. Por ejemplo, las restricciones francesas sobre los equipos Huawei y ZTE en el núcleo de la red móvil son anteriores al debate del 5G, mientras que Suecia y Estonia han adoptado un enfoque basado en un análisis caso por caso con las empresas chinas en el que se ha involucrado a los servicios de seguridad. Todos ellos imponen restricciones significativas a los proveedores chinos en sus redes, pero también permiten cierto grado de ambigüedad estratégica. Es probable que Dinamarca adopte pronto un enfoque restrictivo. También se han hecho anuncios en esta dirección en Rumanía, la República Checa, Italia y Polonia que apuntan a la exclusión de los proveedores chinos. Sin embargo, los procesos legislativos a tal efecto no han concluido y, de hecho, han generado mucha controversia, como es el caso de Polonia. Todo ello ha conducido en repetidas ocasiones a retrasos en los procesos de licitación de espectro.

El enfoque más sofisticado tecnológica e intelectualmente en torno a este asunto se ha producido en el Centro Nacional de Seguridad Cibernética del Reino Unido. A diferencia de sus homólogos de Europa continental, esta entidad lleva años haciendo un análisis profundo sobre los equipos Huawei, y ha estado muy atenta a inminentes riesgos de seguridad durante más de una década en relación con el 3G y 4G. Ello explica que el Reino Unido haya dado el paso más decisivo en Europa al prohibir completamente ZTE, y al proponer importantes limitaciones al futuro papel de Huawei en su infraestructura 5G.

En la medida que la pandemia ha impulsado declaraciones a favor de la reevaluación de las cadenas de suministro de bienes críticos, algunos

parlamentarios británicos han aumentado la presión sobre el gobierno para que aplique más restricciones a Huawei. Es probable que esto conduzca a una eliminación controlada de la tecnología de Huawei en los próximos años, un ejemplo que muchos gobiernos europeos podrían seguir. Sorpresivamente, Noruega, país europeo no miembro de la UE, ha recibido poca atención ante la decisión de sus principales operadores de desplegar la tecnología 5G sin equipos chinos.

Alemania, por encima de cualquier otro Estado miembro de la UE, es clave en el resultado final de este debate en Europa. Y ello no se debe solo al tamaño de su mercado de telecomunicaciones, que es el mayor de Europa, sino también a su especial relación con China y a la importante presencia de equipos Huawei y ZTE en su infraestructura actual. El debate alemán ha sido especialmente controvertido, llevando a la división interna del gobierno, que no se puede explicar por la división entre los partidos de la gran coalición, sino entre los órganos competentes en materia de asuntos exteriores, de seguridad y cibernéticos y los que se ocupan eminentemente de la economía. Las leyes de seguridad informática y de telecomunicaciones de Alemania debían ser actualizadas a principios de este año. Sin embargo, hasta ahora solo se ha conocido un primer borrador de cambios en la ley de seguridad informática. La versión preliminar incluye una clara referencia al conjunto de instrumentos para la seguridad de las redes 5G de la UE y pide que los factores no técnicos, como la fiabilidad, sean pertinentes en la evaluación de un proveedor. Pero sigue sin estar claro cómo evaluará Alemania la fiabilidad de los proveedores.

Una cuestión de confianza

La confianza en China se ha convertido en un gran problema para los europeos. Los intentos de Pekín por ocultar información sobre el brote del coronavirus y su manejo inicial de la crisis han recibido críticas internacionales generalizadas.

Simultáneamente, la postura enérgica de China de conformar una narrativa mundial sobre la pandemia mediante la conocida "diplomacia de la mascarilla" o actos de intimidación abierta demuestran que sus dirigentes comunistas, que se encuentran entre la espada y la pared, no pueden perder el tiempo jugando limpio con Europa. China está centrada en resolver los problemas económicos internos que ha creado la pandemia, como la pérdida masiva de empleo y el aumento de los gastos en el hogar.

Los europeos parecen haberse puesto a la defensiva por el nuevo giro de Pekín. Aunque Europa, tras su evaluación general de las relaciones con China en 2019 modificó su enfoque, actualmente su relación se está deteriorando con una severidad y velocidad increíbles. La pandemia tendrá un impacto duradero en la imagen de China en el mundo. Desplazará aún más la atención de los dirigentes tecno-nacionalistas chinos hacia el interior de sus fronteras de manera que una cooperación mutuamente beneficiosa será cada vez más improbable. China avanzará hacia una mayor separación de los proveedores internacionales, apoyará a sus campeones nacionales y reducirá sus dependencias.

Para Europa, el momento no podría ser peor. El panorama económico posterior a la pandemia es sombrío. La recuperación será difícil. Como ha demostrado el confinamiento por la pandemia, hay deficiencias en la digitalización incluso de las principales economías de Europa. La inversión en la infraestructura digital, con especial atención a la rápida introducción del 5G, parece el camino lógico. La situación económica general podría inclinar a los operadores de telecomunicaciones hacia la opción más asequible. Y puesto que los proveedores chinos ya están presentes en el mercado europeo de infraestructuras de telecomunicaciones, podrían utilizar fácilmente un argumento económico para esgrimir una mayor confianza en ellos.

Pero el argumento compensatorio puede pesar más: la pandemia ha dejado claro que la dependencia de China para el suministro de bienes críticos, como mascarillas y equipos de protección individual, pone a los gobiernos europeos a merced del Partido Comunista Chino en tiempos de crisis. El coronavirus ha revelado a los ciudadanos europeos la importancia de la infraestructura crítica. La dependencia de China se ha convertido en parte del debate público en toda Europa, mientras que el escepticismo sobre la fiabilidad del país como socio comercial afectará al clima político en la mayoría de los Estados europeos durante meses, sino años, en el futuro. Como muestra una encuesta reciente de la Fundación Korber, el 85 % de los alemanes tratan de reorientar la capacidad de producción y la infraestructura crítica para aumentar la resistencia a la crisis, incluso si ello supone un mayor coste económico.

Es preocupante que, en la infraestructura digital básica, la mayoría de los países europeos no están actualizados en el sentido más amplio de la palabra. Esto podría dañar la posición del mercado de Europa a largo plazo. Dado que el 5G se convertirá en una tecnología habilitadora de un nuevo ecosistema digital en los próximos cinco a diez años a medida que alcance su plena funcionalidad, Europa tendrá que apoyar a sus principales empresas en el mercado protegiéndolas de la competencia desleal y de las adquisiciones chinas. A este respecto, la reglamentación de la UE está avanzando y ha demostrado ser un arma poderosa en una batalla que ningún Estado miembro puede ganar en solitario.

El Coronavirus como oportunidad

La crisis del coronavirus es un punto de inflexión en el enfoque de Europa en materia de tecnología y geopolítica. Aprovechando la necesidad de transformación económica, el continente debería dar un nuevo impulso a las soluciones europeas a los desafíos que superan las fronteras del Estado nación: las pandemias y las amenazas cibernéticas son los ejemplos más destacados, pero ciertamente no los únicos.

La conectividad ha sido un término de moda en Bruselas que nunca ha calado en el discurso público. Ahora que los ciudadanos han experimentado las desastrosas consecuencias de la ruptura de las conexiones internacionales en las que confían, la digitalización podría ocupar un lugar central en sus esfuerzos por recuperarse de la crisis. Europa necesita no solo reducir la deuda sino invertir en su competitividad futura.

Pekín se moverá rápidamente mientras el resto del mundo sigue enfrentándose a la crisis y no se limitará a la política interna. También es probable que se genere un renovado interés por la conectividad digital como parte de su Iniciativa de la Nueva Ruta de la Seda, acompañado de nuevas iniciativas para construir un orden internacional digital que atienda a los intereses del Partido Comunista de China. Los Estados miembros de la UE necesitan ajustarse a este nuevo entorno mientras toman decisiones sobre la recuperación económica.

Los debates europeos sobre la soberanía digital son un paso importante en esta dirección. Es necesario encontrar puntos de presión a través de los cuales se pueda influir en el debate sobre el tema y pasar de una actitud reactiva a la acción. Las empresas europeas, que forman parte de las cadenas de valor mundiales, dependen de un orden basado en reglas y normas comúnmente definidas. Antes de la reciente escalada de los enfrentamientos entre EE.UU. y China, la mayoría de los europeos tenían poca conciencia de las limitaciones potenciales a las que se enfrentaban en el acceso a la tecnología, la investigación y la innovación. Su compromiso con una integración profunda y un pensamiento en red dejaba poco margen para considerar las vulnerabilidades entre todas las oportunidades que existían. Se podría haber previsto la dinámica que se ha desarrollado en los últimos años, pero parece que Europa necesitaba un duro despertar de su profundo letargo geopolítico para comprender cómo está cambiando el mundo a su alrededor.

Se ha instalado la opinión de que Europa no tiene lo necesario para prevalecer en el mundo de la tecnología del siglo XXI y que, por lo tanto, solo puede elegir a qué amos servirá, ya sea en Silicon Valley o en Shenzhen. Cierto que Europa no tiene actualmente con quien competir con los grandes jugadores estadounidenses Amazon, Facebook y Google o sus equivalentes chinos Alibaba, Tencent o Baidu. Pero tiene lo necesario para convertirse en una fuerza a tener en cuenta en el espacio tecnológico. El continente cuenta con 6,1 millones de desarrolladores, frente a 4,3 millones en los Estados Unidos, y además tiene múltiples centros tecnológicos, desde los tres clásicos de Londres, Berlín y París hasta los vibrantes centros de Estocolmo, Ámsterdam, Barcelona, Dublín, Helsinki y Madrid.

Los miembros de la Unión Europea tienen una ventaja especialmente significativa a largo plazo en la libertad de circulación de personas y capitales a través de sus fronteras, así como su reglamentación común y su clima de inversión cada vez más atractivo, habida cuenta de la imprevisibilidad de las políticas y las condiciones de mercado de los Estados Unidos y China. La Comisión Europea ha establecido objetivos ambiciosos para asegurar que Europa no solo tenga un mercado poderoso, sino que también sea un líder innovador en tecnología. Para alcanzar estos objetivos, la Comisión necesitará el pleno apoyo de todos los Estados miembros y nuevas asociaciones con actores afines, como Japón, Australia y Corea del Sur.

Dado que la volátil relación entre Estados Unidos y China cambia casi a diario, Europa necesita urgentemente aumentar su resiliencia frente a las conmociones externas. Washington y Pekín están barajando varias medidas extremas relacionadas con el desacoplamiento tecnológico que, aparte de sus implicaciones para la seguridad, podrían desorganizar las cadenas de suministro mundiales. Entre ellas se incluyen posibles sanciones estadounidenses a empresas chinas que comercian en dólares, así como amenazas chinas contra el statu quo en el Estrecho de Taiwán. Si los acontecimientos de los dos últimos años han demostrado algo, es que esos escenarios de alto riesgo e improbables merecen mucha más atención de la que recibieron en el pasado.

La perspectiva desde España: la apuesta de la UE por la soberanía digital

Andrés Ortega

Investigador senior del Real Instituto Elcano, consultor independiente y director del Observatorio de Ideas

La idea de la soberanía digital europea sugiere el control por parte de los europeos de su entorno económico, en este caso el entorno digital, incluso cuando existe un alto nivel de interdependencia. En cualquier caso, este concepto es difuso.

La crisis del coronavirus tendrá un impacto en su definición de dos maneras. Por un lado, la pandemia ha dejado claro que Europa, la Unión Europea y sus Estados miembros, depende en exceso de los suministros, tanto tecnológicos como sanitarios, de China y otros países; algo que España, uno de los países que más ha sufrido por el COVID-19, ha experimentado de primera mano. El proceso de desglobalización y el incremento del nacionalismo dará lugar a un mayor esfuerzo por controlar, en algunos casos para reorientar, o incluso nacionalizar u "europeizar", partes de las cadenas de suministro.

Por otra parte, la crisis económica resultante llevará a un mayor control financiero por parte de los Estados miembros e instituciones de la UE en la reconstrucción, y esta reconstrucción tiene que conducir a una mayor inversión en investigación y desarrollo (I+D) en el campo digital, incluso en un momento en que habrá grandes presiones en la elaboración de los presupuestos nacionales y de la UE. Si los países europeos, incluida España, que va a la zaga en gasto en I+D, quieren competir con Estados Unidos y China en este campo, necesitan aumentar la inversión tanto pública como privada. Esto tiene que ser parte de la estrategia industrial y comercial de la UE. Las consecuencias de la crisis también llevarán a replantearse la necesidad de contar con "campeones europeos" y la consiguiente renovación de la política de competencia de la UE. Visto desde el sur de Europa, esos campeones no pueden ser solo franco-alemanes. Puede partir de una iniciativa franco-alemana, como en el caso de GAIA-X o la red virtual de IA. Pero para ser verdaderamente europeas, esas iniciativas deben incluir a otros Estados miembros, no solo a Francia y Alemania.

Cuando el filósofo español, José Ortega y Gasset, escribió en 1911 que "España es el problema y Europa la solución", pensaba principalmente en la ciencia y en lo que ahora llamamos tecnología. Dijo: "Europa es la ciencia por encima de todo". Más de un siglo después, podríamos decir que Europa debería ser ciencia y tecnología por encima de todo. Además, los esfuerzos de España en este campo tienen una ambición claramente europea, en el sentido de que España, junto con otros Estados miembros de la UE, es demasiado pequeña para competir por sí misma y, en cierto modo, incluso para cooperar, más allá de ser un cliente o un usuario, con EE.UU. y China. Incluso EE.UU. es demasiado pequeños en muchos sentidos, y debería cooperar más con los europeos en este campo.

España es una economía avanzada que lidera algunos sectores tecnológicos y cuenta con algunos centros de investigación punteros. Pero la inversión

en I+D es insuficiente en España: se redujo en los años de la "Gran Recesión" y tardó en empezar a recuperarse. Además, todavía sigue arrastrando el débil crecimiento del PIB. Veremos qué pasa ahora. La inversión pública y privada total en investigación, desarrollo e innovación se sitúa en el 1,24 % del PIB (2018), lo que supone una disminución con respecto al 1,4 % del PIB en 2010, pero sigue estando por debajo de la media de la UE, que es del 2 %. En 2016 y 2017, el sector privado aumentó sus inversiones en I+D en un 3 %. Si bien esto es positivo, la inversión del sector público se redujo en una cantidad similar en 2016, por un total de 3.260 millones de euros. A diferencia de otros países, España, a pesar de contar con un "Plan Estatal de Investigación Científica y Técnica y de Innovación 2017- 2020", no tiene una estrategia general definida sobre cuáles deben ser sus sectores tecnológicos prioritarios, en general y con respecto a China. Como país, España todavía tiene que esbozar una estrategia de tecnología y digitalización. Esto debe formar parte de una nueva política industrial más amplia, sobre todo teniendo en cuenta la manera en que la crisis del coronavirus ha puesto en evidencia el papel de la digitalización para mantener la economía en funcionamiento durante el confinamiento, y el hecho de que los países con un sector industrial fuerte, como Francia y Alemania, han superado mejor dicha crisis.

Las empresas españolas, y europeas, se quejan de que se encuentran en una situación de dependencia excesiva, incluso "neocolonial", respecto de las grandes empresas digitales estadounidenses y chinas. La noción de soberanía digital europea supondría una forma de liberación para el sector tecnológico, aunque la cooperación con estas empresas estadounidenses y chinas sea inevitable y deseable. España ahora entiende su política europea de una manera pragmática. En el campo tecnológico y digital, España se podría beneficiar de una mayor financiación de la UE y de alianzas industriales más fuertes con países y empresas europeas. Espera que estas oportunidades crezcan con las políticas que se están poniendo en marcha en la UE a través del Fondo de Recuperación de la UE *Next Generation EU* y el presupuesto del marco financiero plurianual de la Unión para 2021-2027, en el que la digitalización y la sostenibilidad serán prioritarias. Esto podría llevar a una mayor participación de España en ese impulso hacia una mayor autonomía europea.

Pero mientras persigue un enfoque europeo, España ve la cooperación con las empresas tecnológicas de EE.UU. como algo necesario e inevitable. Ve la cooperación con China de manera similar, aunque quiere ver un mayor grado de equilibrio y reciprocidad tanto en el frente bilateral UE-China como en el España-China. La "Agenda Estratégica para la Cooperación UE-China 2020", aprobada en noviembre de 2013, abarca la cooperación en materia de ciencia y tecnología. Se renovó en 2017 para hacer hincapié en la innovación, la transferencia de los resultados de la I+D y una mayor reciprocidad en el acceso a los centros de investigación, exigencias que la UE había formulado desde 2016.

Para España, América Latina proporciona una dimensión adicional a sus relaciones tecnológicas con China. Podríamos hablar de un "triángulo tecnológico". Esta dimensión, especialmente la digital, se presenta en las Cumbres Iberoamericanas. China también está muy presente en la región, con inversiones y comercio, aunque principalmente en las materias primas, pero también con intereses en el campo de la tecnología. Por esta razón, el enfoque de España hacia América Latina también deberá tener en cuenta a China y su implicación tecnológica en la región. Esto se puede ver en el ejemplo de la cooperación tecnológica entre empresas y centros de investigación españoles, chinos y latinoamericanos. Así pues, existe una relación tecnológica entre España y América Latina, otra entre China y la región, y otra entre China y España. Este "triángulo tecnológico" podría resultar interesante y beneficioso para cada una de las tres partes.

El 19 de febrero de 2020, la Comisión Europea publicó tres importantes iniciativas, que en general fueron bien recibidas en España: una declaración sobre el futuro digital de Europa, un Libro Blanco sobre la IA y una "Estrategia Europea de Datos". En ellas se esbozaron las principales prioridades en este campo para el presente mandato de la Comisión, y se han complementado con otras declaraciones pos-COVID-19 como la del Consejo Europeo titulada *Configurar el futuro digital de Europa*. Los anuncios de la Comisión llevaron a Andrea Renda, del Centro Europeo de Estudios Políticos y Sociales, a vislumbrar el amanecer del "Día de la Independencia Digital" en Europa. Esto es discutible. Aunque el impacto del coronavirus con toda seguridad va a obligar a cambiar estas estrategias. Inicialmente, la Comisión había asignado un presupuesto anual de 20.000 millones de euros para la IA europea. Aunque genera un efecto multiplicador, a modo de comparación, Alphabet, la empresa matriz de Google gasta más anualmente en su I+D. Para ser eficaz y creíble, y así poner fin a la noción de "neocolonialismo digital" o "dependencia tecno-oligopólica", la soberanía digital europea debe ir acompañada de recursos suficientes.

En 2000, cuando fue aprobada la desafortunada estrategia de Lisboa, la UE se propuso convertirse en "la economía basada en el conocimiento más competitiva y dinámica del mundo" en diez años. Veinte años después, el objetivo es menos ambicioso: "convertirse en un líder mundial en innovación en la economía de los datos y sus aplicaciones". EE.UU. no controla las grandes empresas tecnológicas de América, mientras que el Partido Comunista Chino ejerce un férreo control sobre las empresas chinas. Y el hecho es que, según Forbes, ninguna de las diez empresas

tecnológicas más grandes del mundo es europea. El Brexit también podría repercutir en el peso, la investigación y la capacidad de innovación de la UE, ya que el Reino Unido es uno de los países de la UE más avanzados en el campo de la investigación y desarrollo. Aprender a hablar el "lenguaje del poder" y de la geopolítica también implica que la UE adquiera capacidades e instrumentos, y no solo del tipo militar. Un objetivo claro sería que, antes de que finalice el actual mandato de la Comisión Europea, al menos dos empresas europeas figuren entre las diez primeras en el campo de la tecnología. Dado que no es posible crear un motor de búsqueda europeo ni una empresa comparable a Alphabet, será necesario inventar algo nuevo, de ahí las propuestas de la Comisión centrándose no solo en el futuro inmediato sino de mirar más allá.

Capacidades y regulación: Inteligencia Artificial, datos y servicios de Internet

Según un informe del Centro para la Innovación de Datos que examinó seis métricas, talento, investigación, desarrollo, adopción, datos y hardware, EE.UU. "sigue siendo líder en términos absolutos". China está en segundo lugar, aunque, en los próximos años puede ocupar el primer lugar, con la UE detrás de ambos.

Hay algunos aspectos cruciales en los que la UE, incluyendo España, sigue los pasos de EE.UU. y China. En los documentos de la Comisión se esbozan algunos enfoques que se pueden seguir en ese sentido. La primera es la IA, una tecnología transversal que ya está cambiando el paisaje industrial y la vida personal. Florecerá con el advenimiento de tecnologías como el *deep learning*, las redes neuronales y las comunicaciones 5G. Como ha declarado Anthony Mullen, un experto de la consultora de TI Gartner: "En este momento, la IA es una carrera entre dos caballos: China y EE.UU." Europa es un campo de batalla, pero ser un campo de batalla entre dos superpotencias no implica soberanía. Todo lo contrario.

Europa podría llegar a depender de la IA y de otras tecnologías, sin ningún control. En parte como respuesta, la Comisión Europea está diseñando una estrategia europea de IA. España también está elaborando su propio modelo, pero este trabajo se ha retrasado debido a los cambios de gobierno y posteriormente a la crisis del COVID-19. Existe la opinión generalizada de que Europa está demasiado atrasada para la primera e incluso la segunda generación de IA, y debería concentrarse en las próximas generaciones.

Según la Comisión, el éxito de la labor de la Unión Europea en relación con la IA se basa en tres pilares: el aumento de la inversión pública y privada en IA, la preparación para los cambios socioeconómicos y la garantía de un marco ético y jurídico apropiado. Ninguno de estos pilares puede ser construido por los gobiernos por sí solos; requieren una combinación de actores, por ejemplo, gobiernos, regiones, instituciones europeas, empresas y el mundo académico que trabajen juntos coordinadamente en toda Europa.

El acuerdo inscrito en el Tratado de cooperación bilateral franco-alemán firmado en enero de 2019 crea un centro virtual conjunto de investigación e innovación para la IA y una plataforma digital de contenidos audiovisuales e informativos. Si bien esa cooperación es bienvenida, no es exhaustiva ni habla en nombre de Europa en su conjunto,

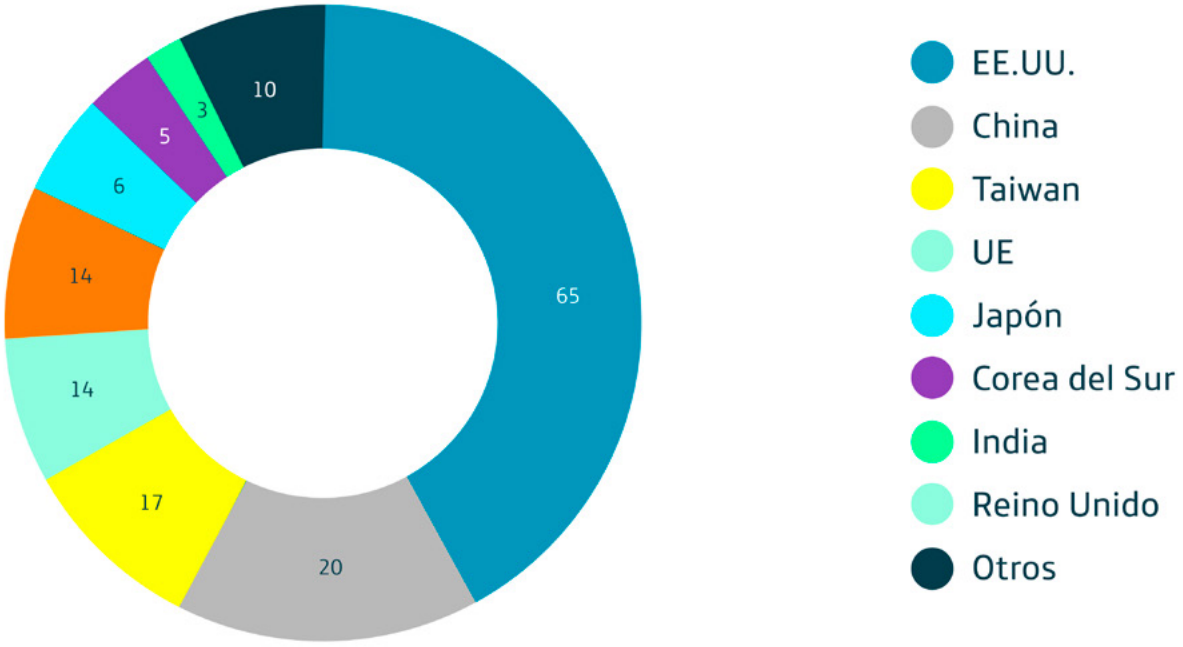
aunque ambos gobiernos apoyen los objetivos de la Comisión. A España le gustaría unirse al esfuerzo franco-alemán en este campo, pero busca también un enfoque más europeo.

El *big data* y los servicios de datos son otro espacio para lograr la soberanía europea. La "Estrategia Europea de Datos", que está estrechamente relacionada con la IA, tiene por objeto "crear un mercado único de datos que asegure la competitividad global y la soberanía de Europa en materia de datos". Sugiere que "los espacios comunes europeos de datos asegurarán que se disponga de más datos para su uso en la economía y la sociedad, manteniendo al mismo tiempo el control de las empresas y los individuos que generan esos datos". Esta es también una forma de asegurar que los datos europeos sean controlados y monetizados por empresas europeas bajo normas europeas. Por ello, la Comisión está haciendo hincapié en el Cloud y los centros de datos europeos y está introduciendo financiación para ellos. En la actualidad, estas empresas pertenecen en su inmensa mayoría, incluso en Europa, a empresas estadounidenses con China progresando en el mercado de servicios de datos, pero Europa está atrasada debido a la diversidad de reglas locales, nacionales y europeas. China, por ejemplo, puede integrar todos sus inmensos datos sobre cuestiones médicas, gracias a la soberanía que ejerce en el ámbito de los datos en todo su territorio. Los EE.UU. están algo cerca de poder hacerlo. Europa, sin embargo, está muy atrasada; no puede aprovechar su tamaño debido a la compartimentación de sus datos y a la prioridad que da a la privacidad.

Existen tres formas principales de abordar el control de los datos. En los Estados Unidos, grandes empresas como Facebook, Apple, Netflix, Google y Amazon tienen acceso a grandes cantidades de datos de consumidores y los monetizan, y ofrecen grandes servicios de cloud. En la UE, gracias al RGPD (Reglamento General de Protección de Datos), los derechos de los ciudadanos y los consumidores son una prioridad, eventualmente a expensas de la competitividad de las empresas, los países o determinados sectores. China tiene un modelo muy diferente: la tecnología es patrocinada por el Estado y el gobierno ejerce el poder de adquirir los datos de los ciudadanos. La pugna entre estos tres modelos tendrá tremendas implicaciones para el futuro de la economía mundial y para la geopolítica.

La regulación, que está íntimamente relacionada con esto, se ha convertido en un importante campo de confrontación geopolítica. Como Anu Bradford argumenta de manera convincente en su reciente libro *"El efecto Bruselas"*, Europa se ve a sí misma como una superpotencia reguladora[1]. Ha tenido éxitos de alcance mundial en lo que respecta a la imposición de sus normas, por ejemplo, en el ámbito de la protección de datos (mediante el RGPD) y la seguridad de los vehículos de carretera, y pronto volverá a hacerlo mediante el establecimiento de

Ubicación de las mayores empresas de tecnología del mundo



Fuente: Forbes

[1] Anu Bradford, The Brussels Effect (Oxford: Oxford University Press, 2020).

los impuestos sobre el carbono y la regulación sobre el comercio digital. Ahora quiere repetir estos éxitos en la IA y los datos, entre otros campos. Dicho esto, es improbable que mantenga esa influencia a menos que preserve o aumente sus capacidades. Como Guntram Wolff señala acertadamente, "los árbitros no ganan los partidos". Es necesario que haya un diálogo entre Europa y Estados Unidos sobre el tema de la regulación. El objetivo principal de ese diálogo no tendría que ser el logro de reglas idénticas, sino el de lograr sistemas interoperables que puedan funcionar juntos. Un buen ejemplo podría ser las aplicaciones de rastreo del COVID-19 desarrolladas en un sistema común (Interfaz de Programación de Aplicaciones - API) conjuntamente por Google y Apple. No obstante, esta inusual colaboración entre los dos gigantes de la tecnología no fue bien recibida políticamente por algunos europeos, especialmente porque el dúo tiene en conjunto más del 90 % del mercado de sistemas operativos. De hecho, la Comisión respondió con algunas orientaciones que deben ser respetadas, por ese y otros sistemas, para preservar los "valores europeos". Algunos Estados miembros, como Francia, optaron por otros sistemas.

Los servicios de Internet, incluyendo el comercio electrónico, podrían ser el próximo campo de batalla, no solo entre EE.UU. y China, sino también entre Europa y EE.UU., y, eventualmente, China. Estados Unidos domina el sector que incluye los servicios de *cloud* mencionados anteriormente a través de algunas grandes empresas de tecnología, como Amazon, Alphabet, Microsoft y Apple, además, en menor escala, empresas como Netflix y HBO. Aunque China tiene sus propias grandes empresas de tecnología, por ejemplo, Tencent y Alibaba y está tratando de penetrar en el mercado europeo, la competencia entre Estados Unidos y China ha sido limitada hasta ahora.

En los servicios de Internet, como en la IA y los datos, Europa se está quedando atrás y depende de los sistemas de los Estados Unidos y China. Con algunas pequeñas excepciones, como Spotify, carece de la capacidad de crear empresas lo suficientemente grandes en este campo. En ese sentido, las estrategias industriales de Francia, Alemania y la Comisión Europea serán vitales. La cooperación entre las empresas europeas y estadounidenses sigue siendo inevitable y esencial si los europeos quieren seguir siendo relevantes para la próxima generación de tecnología.

Si no pueden ponerse al día, los Estados miembros de la UE y las empresas podrían terminar teniendo que elegir entre los servicios de Internet de EE.UU. y China. Aunque se pueda tomar una decisión por motivos económicos, en el plano político, no existe realmente alternativa, ya que los valores y el comportamiento tecnológico de China difieren demasiado de los de Occidente. Aun así, los gobiernos e instituciones de Europa no quieren verse atrapados en medio de un desacoplamiento tecnológico de EE.UU. desde China. Parece inevitable un cierto desacoplamiento selectivo y que Europa mantenga la tecnología china a cierta distancia, incluso mientras intenta evitar una guerra fría, una guerra fría tecnológica. Europa, en el campo de la tecnología, como en otros, no quiere tener una relación equidistante con Washington y Pekín ya que son demasiadas las cosas que unen a los europeos con los americanos, pero tampoco quiere estar atrapada entre los EE.UU. y China. En cambio, Europa quiere, y necesita, tener un tipo de relación diferente con ambos. ¿Podría la competencia en estos sectores conducir a una alianza tecnológica contra China entre Estados Unidos y Europa, una a la que otros podrían unirse? Es posible, pero esa alianza no puede llegar a costa del desarrollo tecnológico de Europa.

Las batallas por el 5G

El caso del 5G ilustra bien la complejidad de los problemas a los que Europa y España se enfrentan con respecto a la soberanía digital. Esta tecnología es crucial porque sustenta una serie de otras industrias y procesará enormes cantidades de información entre personas, empresas, gobierno y máquinas, el Internet de las cosas (IoT). La carrera por el dominio del 5G será probablemente la más importante de los próximos cinco años. Los europeos, y en particular España, dependían en gran medida de la tecnología china para el 4G, principalmente Huawei, pero también ZTE. Se dirigían hacia la misma situación para el 5G, ya que las diferencias de coste eran significativas. Sin embargo, cuando el proceso estaba llegando al final, EE.UU. que no tenía empresas involucradas en la fabricación de equipos 5G, percibió una amenaza económica y de seguridad por esta dependencia de la tecnología china. La presión de EE.UU. tuvo cierto éxito, aunque América también quería que Europa se deshiciera de los equipos 4G chinos; un objetivo que no era financieramente viable para las empresas.

El gobierno y las empresas españolas están siguiendo el camino europeo que es, en realidad, el camino británico de no tener hardware o software Huawei en las funciones "centrales" del 5G sino solo en las secundarias y periféricas. Incluso el Reino Unido está estrechando su posición y debería influenciar en ese sentido a otros jugadores europeos. En octubre de 2019, la Comisión Europea y el Grupo de Cooperación de la Agencia de la Unión Europea para la Ciberseguridad publicaron un informe en el que se afirmaba que "las amenazas planteadas por los Estados o los actores respaldados por el Estado se consideran de la mayor relevancia" para el sistema 5G. Esto "a su vez aumentará el número de vías de ataque [sic] que podrían ser explotadas por los responsables de la amenaza, en particular los actores no

pertenecientes a la UE o respaldados por otro Estado, debido a sus capacidades, incluidas también intención y recursos, para realizar ataques contra las redes de telecomunicaciones de los Estados miembros de la UE, así como la potencial gravedad de los efectos de dichos ataques". En el informe no se señalaba ningún país o empresa; su objetivo era servir de base para la preparación de una serie de medidas de control de riesgos.

La Comisión ha recomendado a los Estados miembros de la UE que excluyan de sus redes a los proveedores de "alto riesgo". Europa tiene dos empresas, la finlandesa Nokia y la sueca Ericsson, que son capaces de fabricar equipos para redes 5G, y competir con Huawei y otras empresas chinas como ZTE, aunque a un coste mayor. El surcoreano Samsung también es un aspirante. Pero más allá del 5G, la Comisión Europea ahora pretende centrarse en no perder la próxima carrera hacia el 6G.

Europa sigue buscando una estrategia de certificación para evitar las puertas traseras, es decir, puntos de entrada ocultos para espiar o atacar. Esto es más fácil para el hardware 5G que para el software, que se actualiza constantemente con parches de seguridad y de otro tipo. Una autoridad europea de certificación, al menos para los equipos básicos, sería la solución correcta, aunque prefieren algunos Estados miembros prefieran un enfoque nacional.

En España y en otros países, hay preocupación por la falta de proveedores de 5G: en la última década ha bajado de 15 a solo 3: Huawei, Ericsson y Nokia además de algunos proveedores de nicho. Esta situación distorsiona la competencia de precios. El mayor y más barato proveedor es chino; los europeos son más caros. Esto se aplica no solo al mercado europeo, sino también a otros como el latinoamericano. Las empresas españolas como Telefónica, así como otras firmas europeas, también están muy presentes en América Latina, donde la inversión en tecnología Huawei 4G y luego 5G ha sido importante, pero donde sería bienvenida una mayor competencia en términos de hardware y software para 5G.

En España, existe la percepción de que la oposición de EE.UU. a Huawei está impulsada por el deseo de ganar tiempo para algunas de sus principales empresas, como Cisco y Maverick, para desarrollar una base industrial para los equipos 5G en el transcurso del próximo año, tal vez mediante la adquisición de una de las dos empresas europeas. Puede que sea bienvenida una mayor competencia, pero esto podría llegar a costa de socavar la base industrial europea de 5G, dado que Ericsson y Nokia ya son más caros que Huawei. Por lo tanto, existe una contradicción entre la mayor competencia, los proveedores y la soberanía europea.

Defensa contra adquisiciones indeseables

Los temores en torno a las adquisiciones adicionales de empresas europeas estratégicas por parte de inversores indeseables, ya sea de China o del Golfo, han aumentado con las consecuencias económicas de la crisis del coronavirus. Pero ya estaban allí antes. Esto también es parte del argumento de la soberanía. El "momento Sputnik" llegó en 2017 con la adquisición de Kuka, un fabricante alemán de robots avanzados, por el fabricante chino de electrodomésticos Midea. En respuesta, Margrethe Vestager, la Comisaria de Competencia de la UE, dijo que los Estados europeos deberían comprar participaciones en empresas estratégicas para evitar las adquisiciones chinas u otras. Además, la Comisión Europea ha instado a los países a que endurezcan su examen de las ofertas de adquisición extranjeras, advirtiendo que la pandemia de coronavirus había dejado los "activos estratégicos" del bloque vulnerables a la adquisición en el extranjero. Phil Hogan, el comisario de comercio, dijo que Bruselas estaba dispuesta a asumir un papel central en la coordinación de la vigilancia y el intercambio de información. "La vulnerabilidad económica podría dar lugar a la venta de infraestructuras o tecnologías críticas", advirtió. Incluso antes de la crisis, la Comisión anterior estaba diseñando un plan para un fondo soberano europeo de 100.000 millones de euros que podría invertir en sectores estratégicos en los que la UE va a la zaga de sus rivales mundiales y que podría intervenir para proteger esos sectores, por ejemplo, comprando empresas relevantes cuando no haya capital europeo disponible. Sin embargo, no está claro si los nuevos comisarios impulsarán este plan.

Aunque el gobierno español, y otros, alienta una mayor inversión china, también apoya un mayor escrutinio o revisión estratégicos por parte de la UE. Y con el impacto económico de la crisis del coronavirus, España, como otros países europeos, ha tomado medidas para evitar que las empresas estratégicas caigan en manos indeseables. Incluso podríamos ver nacionalizaciones temporales para evitarlo.

Bruselas está tratando de reforzar un sistema de intercambio de información sobre el examen de las inversiones que los gobiernos acordaron el año pasado. El sistema estaba previsto que estuviera activo en octubre de 2020, pero la Comisión Europea ahora quiere que los Estados miembros se muevan más rápido y vayan más allá. España es uno de los 12 miembros de la UE que tiene un sistema de control de seguridad nacional. Madrid es más cuidadosa con la inversión estratégica después de la adquisición en 2017 por parte de China Ocean Shipping Company (COSCO) de Hong Kong del 51% de los puertos de contenedores de Bilbao y Valencia.

Competidores estratégicos y soberanía

Europa, incluida España, quiere y necesita seguir haciendo negocios con China y no desea librarse completamente del ecosistema tecnológico de China ni desconectarse de él y de su economía. Como resultado, en marzo de 2019, la Comisión Europea, en una declaración que luego fue apoyada por el Consejo Europeo, anunció una política que reconoce que "China es, simultáneamente, un *socio de cooperación* con el que la UE ha alineado estrechamente los objetivos, un *socio negociador* con el que la UE necesita encontrar un equilibrio de intereses, un *competidor* económico en busca de liderazgo tecnológico, y un *rival* sistémico que promueve modelos alternativos de gobernanza". Las cuatro calificaciones van juntas.

Pero Europa también se ve a sí misma en una competencia diferente con EE.UU., una que, como hemos visto, ha sido descrita como "neocolonial" en el campo de lo digital. Angela Merkel, la canciller alemana, ha apoyado la idea de la soberanía digital y la competencia con Silicon Valley, cuando, por ejemplo, instó a Europa a tomar el control de sus datos de los gigantes tecnológicos de EE.UU. La economía de la información y la competencia tecnológica se están convirtiendo claramente en el centro de la relación entre la UE y los Estados Unidos, aunque, como se ha visto, Europa no se plantea la equidistancia entre Estados Unidos y China, y tiene que depender de las grandes empresas tecnológicas estadounidenses.

Muchos países de Europa como, por ejemplo, Alemania, Francia y los países nórdicos, tienen una fuerte cooperación tecnológica con China. Este es menos el caso de España, aunque esto está cambiando. La cooperación entre España y China en el campo científico y tecnológico tiene un gran potencial de desarrollo, en beneficio de ambos países. Pero requiere un enfoque menos competitivo y más cooperativo y una actitud similar en ambos países respecto a los acuerdos tecnológicos. España también necesita desarrollar una estrategia específica para sus relaciones con China, tanto en general como en el campo tecnológico en particular. España quiere actuar en el marco de las relaciones entre Europa y China, pero también promover un marco institucional bilateral. Por lo tanto, España todavía necesita una estrategia más clara de cooperación científica y tecnológica con China.

Conclusión

La integración europea no fue una dilución de la soberanía, sino más bien un **compartir la soberanía** para crear una soberanía colectiva mayor. Esta es una noción que no es bien recibida en Pekín ni en Moscú. En *El rescate europeo del Estado Nación*, Alan Milward sostuvo en 1993 que la integración europea había servido para fortalecer los Estados miembros de la UE[2]. Esto ya no es así y, por lo tanto, para un país como España, es necesario pasar a un enfoque verdaderamente europeo en cuanto a la política tecnológica en general, y en particular hacia China. En cuanto a los temas digitales y tecnológicos, Europa no quiere verse atrapada en una posición definida por la competencia entre EE.UU. y China. Pero, aunque no opte por la equidistancia entre Washington y Pekín, necesita tener herramientas para alcanzar algún tipo de soberanía digital relativa o al menos autonomía. Para lograrlo, debería alentar una mayor inversión pública y privada en la próxima generación de IA, servicios de Internet (incluidos los datos), semiconductores y el 6G. Esto no solo fomentaría el crecimiento, sino que también ayudaría a Europa a ser, como debe ser, más autónoma en un mundo post-COVID-19.

[2] Alan Milward, The European Rescue of the Nation State (Oxford: Oxford University Press, 2020).

Las relaciones entre EE.UU. y la UE: una agenda digital transatlántica post-COVID-19

Frances G Burwell

Miembro distinguida del Atlantic Council y directora senior en McLarty Associates

El brote de coronavirus en la primavera de 2020 fue devastador para muchos individuos, sociedades y economías. Pero también tuvo un impacto significativo en el estado de la relación transatlántica, aumentando los niveles de incomprensión y desconfianza incluso cuando tanto Estados Unidos como Europa se enfrentaban a decenas de miles de muertes. Las súbitas restricciones impuestas por Donald Trump a los europeos para viajar a Estados Unidos y sus amenazas de cortar la financiación de la Organización Mundial de la Salud durante la pandemia fueron muy impopulares en toda Europa. Muchos miembros de la comunidad política de los Estados Unidos consideraron que el aumento de los controles fronterizos internos de la UE y las luchas para acordar un apoyo financiero para toda Europa eran una muestra de la incapacidad de la región para hacer frente al virus y, potencialmente, la sentencia de muerte para la propia Unión Europea.

De este modo, tanto en EE.UU. como en toda Europa, la experiencia del COVID-19 también demostró la importancia del mundo digital. Con millones de personas trabajando desde casa y a veces en cuarentena, y conectadas a amigos, familiares y compañeros por Internet, la importancia de la política digital para la economía moderna era evidente. Incluso cuando la desinformación sobre el virus se extendió a través de las redes sociales, los gobiernos recurrieron a potenciales aplicaciones de rastreo y análisis de datos médicos para encontrar una forma de salir de los confinamientos. Al mismo tiempo, países como China y Rusia utilizaron Internet para difundir noticias falsas y aumentar la vigilancia e incluso el control de sus poblaciones. El virus reveló claramente las diferencias en los enfoques gubernamentales en relación con Internet y sus ciudadanos.

Pero en este nuevo contexto, ¿podrán los EE.UU. y la UE aprovechar la experiencia del COVID-19 para establecer una cooperación más sólida en el espacio digital y garantizar así que sus ciudadanos y economías e incluso su gobernanza democrática sigan siendo seguros en la futura era digital? Las impresiones iniciales no son muy prometedoras. El virus reforzó dentro de Europa el deseo de una mayor soberanía digital, basada en una infraestructura digital fuerte y fiable, controlada por Europa y resistente frente a la desinformación y otras perturbaciones. En Estados Unidos, así como en algunos otros países, el virus exacerbó un enfoque nacionalista de la economía que ha ido creciendo durante la presidencia de Donald Trump.

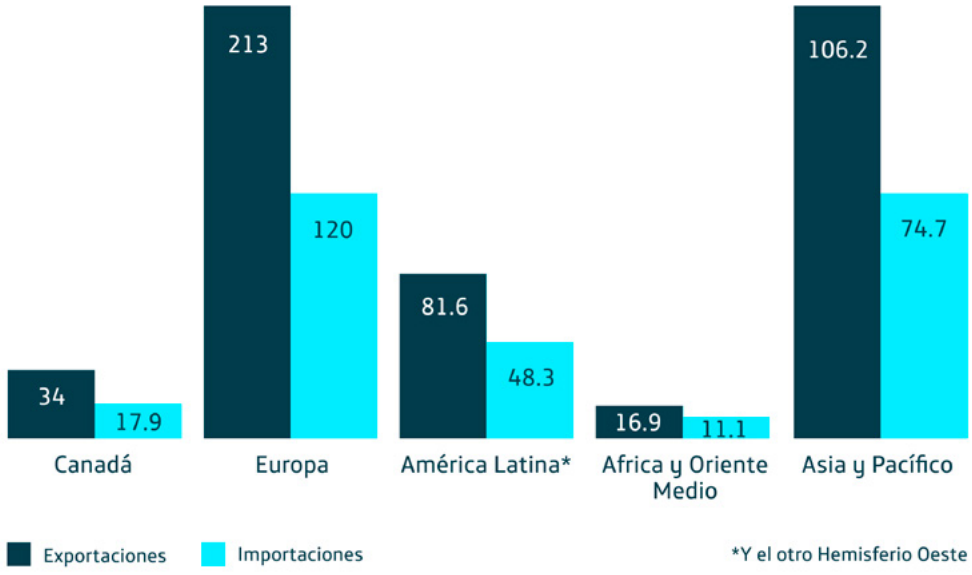
La elección que enfrentan EE.UU. y la UE

Tanto EE.UU. como la UE se enfrentan ahora a una difícil elección. La UE ha iniciado un ambicioso plan para regular la economía digital, pero en este momento debe garantizar, en medio de los esfuerzos por estimular una recuperación económica post-COVID19, que este impulso de soberanía digital no se convierta en proteccionismo. Por el contrario, la UE debería aprovechar esta oportunidad y oleada de concienciación acerca de la importancia de la digitalización para liderar un esfuerzo multilateral que pueda domar los peores excesos de Internet y fomentar la innovación y la creatividad. Estados Unidos debe volver a participar en el sistema económico multilateral, si no a liderarlo, y al mismo tiempo mantener una conversación interna más estratégica sobre la economía digital, que no sea simplemente una reacción a la última violación de la privacidad o seguridad. Si Estados Unidos y Europa no toman las decisiones correctas, el principal beneficiario será China, que ha mostrado sistemáticamente sus ambiciones mundiales durante la crisis del COVID-19. El resultado será un mundo digital con tres enfoques distintos (el estadounidense, el chino y el europeo) y es más probable que China convenza a muchos mercados emergentes de que se adhieran a su enfoque más autoritario, impulsado por el estado tanto en lo que respecta a la gobernanza, como al comercio digital. Pero si Estados Unidos y la Unión Europea son capaces de desarrollar conjuntamente normas de comercio y comportamiento en el mundo digital, pueden llegar a ser los líderes mundiales, garantizando que la mayoría de los países se adhieran a las normas que apoyan la privacidad individual y los mercados abiertos.

Los debates transatlánticos sobre política digital suelen parecer muy alejados de las preocupaciones estratégicas mundiales, con sus debates sobre los diferentes enfoques de Estados Unidos y la Unión Europea en temas como la responsabilidad de los intermediarios y las decisiones de adecuación. Para los que se dedican a la vanguardia digital, especialmente desde las trincheras de las empresas, estas diferencias parecen enormes y ciertamente pueden significar sumas importantes para las empresas. Pero para muchos responsables políticos, incluidos los que han sido el pilar de la relación transatlántica, estos debates parecen técnicos y oscuros. Esto es especialmente cierto en EE.UU., donde la asociación EE.UU.-Europa se ve predominantemente como una alianza para la seguridad, basada en la OTAN, y donde la ciberseguridad es la cuestión digital preeminente.

En realidad, las cuestiones digitales son fundamentales para la salud de la asociación transatlántica. La economía digital es una parte clave de la relación económica entre los Estados Unidos y la Unión Europea. La economía transatlántica es la asociación de comercio e inversión más fuerte del mundo, generando 5,6 billones de dólares en ventas comerciales y manteniendo 16 millones de empleos en 2018. Si bien la medición de la

Comercio de servicios digitales de EE.UU. (miles de millones de dólares) 2018



Fuente: Cámara de Comercio de los Estados Unidos; John Hopkins SAIS ECFR ecfr.eu

economía digital sigue siendo más arte que ciencia, algunos indicadores reflejan su alcance. Los cables que llevan datos digitales a través del Atlántico transportan un 55 % más de datos que a través del Pacífico, y se prevé la instalación de ocho nuevos cables transatlánticos en los próximos años. Tanto para la UE como para los Estados Unidos, el principal destino de las importaciones de sus servicios digitales es el otro, que representa alrededor de un tercio de esas exportaciones. En 2017, las exportaciones de servicios digitales de los Estados Unidos a la Unión Europea ascendieron a 190.000 millones de dólares, y las importaciones a 118.000 millones de dólares, lo que proporcionó a Estados Unidos un superávit de 72.000 millones de dólares. Los servicios digitales son difíciles de medir. Esta cifra combina las estimaciones del gobierno de Estados Unidos sobre el comercio de servicios de tecnología de la información y las comunicaciones, así como de los servicios adicionales que podrían ser posibles gracias a ellos. Ese mismo año, las empresas estadounidenses, a través de sus filiales locales en Europa, suministraron 180.000 millones de dólares en servicios de información, mientras que solo suministraron 3.000 millones en China y 21.000 millones en América Latina. De todas las inversiones de Estados Unidos en el extranjero en la industria de la información, el 73 % se efectuó en Europa en 2018.

Sin embargo, aparte de los datos económicos, la economía digital impregna ahora casi todos los elementos de la vida cotidiana tanto en Europa como en Estados Unidos. Ya sea comprando, teniendo citas online, viendo películas, estudiando cursos online navegando por la red, o con la banca personal, los americanos y europeos están constantemente conectados a Internet. Cuestiones como la privacidad online, la violación de los derechos de autor y la confianza sobre las fuentes de información de las noticias online se han convertido en claves para el funcionamiento de la sociedad.

Sin embargo, al mismo tiempo, tanto europeos como estadounidenses están preocupados por la seguridad de su información personal y financiera en Internet. Una encuesta del Eurobarómetro de 2019 reveló que solo el 32 % de los europeos confían en Internet y que el 43 % de los europeos creía que sus datos podían ser utilizados indebidamente a través de Internet. Los estadounidenses no son inmunes a estas preocupaciones: según una encuesta realizada en 2019, los estadounidenses están preocupados por la forma en que se recogen y utilizan sus datos, y el 79 % está preocupado por la forma en que las empresas utilizan los datos, y el 64 % expresa la misma preocupación sobre el gobierno. Dado que el uso de Internet supera ya el 70 % tanto en los Estados Unidos como en Europa, estas preocupaciones generalizadas en materia de seguridad serán inevitablemente una cuestión delicada.

Iniciativas europeas

En el último decenio, la UE ha tratado de dar respuesta a la creciente importancia económica y política de la economía digital y a las preocupaciones de sus ciudadanos, poniendo en marcha una serie de iniciativas regulatorias. La Estrategia para el Mercado Único Digital puesta en marcha en 2015, tenía por objeto reducir o eliminar las barreras a la actividad digital entre los estados miembros y mejorar el acceso de los ciudadanos y las empresas a los servicios y productos online. Aunque todavía está lejos de ser completa, ha abordado las diferencias en las tarifas de *roaming* y el acceso a las descargas de películas, cuestiones aparentemente mundanas pero que impactan sobre la ciudadanía.

Tras las revelaciones de Edward Snowden en 2013 acerca de la puesta en práctica de un sistema de vigilancia del gobierno estadounidense sobre las comunicaciones de ciudadanos europeos (incluido el teléfono móvil de la canciller alemana Angela Merkel) la UE aprobó el Reglamento General de Protección de Datos (RGPD). Se trata, sin duda, de la legislación sobre privacidad más desarrollada del mundo, que impone condiciones estrictas al tratamiento de la información personal de los ciudadanos de la Unión Europea, incluso si esos datos o ese ciudadano se encuentran físicamente fuera de la Unión Europea. Cuando entró en vigor en mayo de 2018, las empresas de todo el mundo se vieron obligadas a adaptar sus prácticas para cumplir con el RGPD. Aunque el fortalecimiento de la soberanía digital de la UE se mencionó en raras ocasiones en su momento, tanto el plan para el mercado único digital como el RGPD tenían el claro objetivo de mejorar las capacidades digitales de la UE y proporcionar a los ciudadanos una forma de soberanía, o control, sobre sus propios datos personales. En el momento de la toma de posesión, en diciembre de 2019, de la Comisión Europea presidida por Ursula von der Leyen, la idea de una mayor soberanía europea sobre la economía digital había adquirido la suficiente importancia como para figurar en la declaración política en la que se exponían sus prioridades. En ella, pidió que la UE "alcanzara la soberanía tecnológica en algunas áreas tecnológicas críticas". Además, en su discurso inaugural ante el Parlamento Europeo, la política digital fue identificada como una de las principales prioridades de la Comisión, junto con el "Green Deal", y volvió a afirmar que Europa "debe tener el dominio y la propiedad de las tecnologías clave".

La atención de la Comisión se ha centrado en gran medida en avanzar en esa soberanía tecnológica, es decir, en garantizar que la UE disponga de una infraestructura digital segura y de alta calidad, y con

la capacidad de desarrollar y mantener tecnologías clave en sectores estratégicos. Para ello es necesario apoyar la investigación y la innovación, pero también crear un entorno normativo adecuado. La Comisión anterior ya había tomado medidas para abordar la seguridad de la infraestructura frente a los crecientes ciberataques. La Directiva sobre la Seguridad de las Redes y Sistemas de Información de 2016 obliga a los estados miembros a identificar a los operadores de redes esenciales y luego les exige que adopten las medidas de seguridad cibernética adecuadas y que informen de las infracciones. En 2020, a raíz de la creciente preocupación por las inversiones chinas en Europa, la UE advirtió a los estados miembros que los proveedores no comunitarios de tecnología 5G y de otro tipo podían plantear riesgos importantes, especialmente si estaban estrechamente vinculados con gobiernos extranjeros. Aunque la UE no prohibió a Huawei de forma categórica (a pesar de la presión ejercida por los Estados Unidos), varios gobiernos europeos han restringido el papel de Huawei en sus redes. Al mismo tiempo, la Comisión subrayó la importancia de un servicio de *cloud* europeo, y comenzó las conversaciones con los gobiernos alemán y francés, que ya habían puesto en marcha el proyecto de *cloud* "GAIA-X". Estas medidas tienen el claro propósito de promover una infraestructura resiliente como elemento clave de la soberanía tecnológica.

El segundo elemento para lograr la soberanía tecnológica se basa en la capacidad europea para desarrollar tecnologías emergentes clave. En ese sentido, la Comisión ha identificado una serie de tecnologías, entre ellas la inteligencia artificial (IA), la supercomputación, el *blockchain* y las comunicaciones cuánticas, en las que Europa podría convertirse en líder mundial. Se espera que un nuevo programa de investigación de la Europa Digital apoye este esfuerzo con 9.200 millones de euros de financiación, a la espera de la aprobación final del próximo presupuesto de la UE. En consonancia con esta ambición, en febrero de este año, la Comisión publicó una propuesta legislativa preliminar sobre la IA. También publicó una estrategia para la gestión de datos, señalando la importancia de la recopilación de datos y la gobernanza para casi todas las tecnologías clave.

Hay un tercer elemento en el proyecto de la UE; uno mucho más político y también un rasgo definitorio del enfoque europeo. Desde la aprobación del RGPD, la UE se ha considerado un líder mundial en el establecimiento de normas relacionadas con las actividades *online* que tienen por objeto proteger a sus ciudadanos y garantizar un enfoque ético de los dilemas que plantea el mundo digital. Esto no solo se aplica a la privacidad, incluido el "derecho al olvido", sino también a los contenidos *online*, en los que algunos países de la UE tienen restricciones al discurso ilegal de incitación al odio. El hecho de que las normas de la Unión Europea cumplan los mencionados objetivos y de que sean mejores que otros arreglos, es menos seguro y una cuestión de juicio político.

Tanto la estrategia de datos como la propuesta de la IA incluyen normas que tratan de asegurar que los datos sean recolectados y controlados en Europa, que esta tecnología sea utilizada en Europa y se gestione de acuerdo con normas éticas y "centradas en el ser humano" (aunque aún no sean definidas con precisión). Como dijo Thierry Breton, comisario europeo para el mercado interior: "Mi objetivo es prepararnos para que los datos sean utilizados por y para los europeos y con nuestros valores". También se prevé que la Ley de Servicios Digitales, que se espera que la Comisión esboce a finales de 2020, proponga normas destinadas a reforzar las normas europeas en materia de c contenidos, protección del consumidor y responsabilidad de las plataformas. Esas normas van mucho más allá de la soberanía tecnológica, haciendo énfasis en la infraestructura y las industrias clave, y en su lugar utilizan un conjunto emergente de normas europeas sobre el comportamiento y las responsabilidades en el mundo digital para elaborar normas que tendrán un impacto extraterritorial, si no mundial. Al el regular, la UE espera obtener un mayor control sobre la forma en que se llevan a cabo las actividades digitales en Europa y sobre cómo se trata a sus ciudadanos online, y así mejorar su soberanía digital en sentido amplio.

El enfoque de EE.UU.

Estados Unidos no ha adoptado un enfoque tan amplio en materia de política digital. Pero, a nivel federal, se han hecho esfuerzos esporádicos para abordar cuatro preocupaciones distintas: la privacidad, la protección del consumidor, la seguridad y el contenido *online*.

Los esfuerzos se han dividido entre un grupo de organismos federales, entre ellos la Comisión Federal de Comercio (FTC), la Comisión Federal de Comunicaciones y el Instituto Nacional de Normas y Tecnología. En el Congreso, las ocasionales ráfagas de interés en la regulación del sector tecnológico se han materializado por lo general en una escasa legislación. Dada la ausencia de regulación a nivel federal, algunos estados han tomado la iniciativa. Lo más destacado es que California ha adoptado la Ley de Privacidad del Consumidor de California (COPA), que tiene muchas similitudes con el RGPD y entró en vigor en 2020.

La legislación nacional de privacidad de EE.UU. data de 1974, cuando la *Privacy Act* proporcionó ciertas garantías a los ciudadanos cuando sus datos estaban en poder del gobierno federal. En 1996 y 1999 respectivamente se aprobaron leyes que abordan la privacidad en los sectores sanitario y financiero. Ninguna de estas leyes estaba destinada a tratar específicamente de la protección de datos online. La protección de datos en Estados Unidos no solo ha sido sectorial, sino que también se ha centrado en la protección del consumidor. La FTC es responsable de garantizar que las empresas no incurran en "prácticas desleales o engañosas" y ha utilizado este poder para examinar si Facebook u otros han engañado a los usuarios sobre cómo se tratan sus datos. Sin embargo, la privacidad no se ha ignorado totalmente en EE.UU., como lo demuestra la COPA y el interés que algunos otros estados han mostrado con medidas similares.

La seguridad ha sido la gran preocupación del gobierno de EE.UU., especialmente después de los ataques del 11 de septiembre. La respuesta inicial fue que los organismos de inteligencia estadounidenses emprendieran una vigilancia masiva de las actividades *online*. Esta práctica suscitó importantes preocupaciones no solo en los Estados Unidos, sino también en Europa. Las revelaciones de Snowden dieron un impulso considerable a los esfuerzos europeos por crear una legislación integral sobre la privacidad, un esfuerzo que conduciría aprobación del RGPD. La vigilancia de la NSA se redujo en cierta medida por la *Freedom Act* de 2014, que protegía a los ciudadanos estadounidenses de la recopilación masiva de datos, y a cambio exigía a la NSA la presentación de solicitudes muy específicas cuando requiriera datos a las empresas. Por supuesto, en tiempos de amenazas de terrorismo y extremismo, algunos de esos datos son útiles para la aplicación de la ley a ambos lados del Atlántico. La *Cloud Act* de 2018 exige que las empresas tecnológicas de Estados Unidos proporcionen los datos solicitados por los organismos en aplicación de la ley a través de una orden o citación, incluso si esos datos se almacenan fuera de los Estados Unidos. Reino Unido ha firmado un acuerdo bilateral que prevé la reciprocidad y la UE ha iniciado negociaciones con ese fin. Por último, un elemento adicional del enfoque de EE.UU. sobre la seguridad *online* es la preocupación por los proveedores extranjeros, ya sean productos de seguridad cibernética de Kaspersky o Huawei en las redes 5G.

Desde la llegada de las redes sociales, EE.UU. y Europa se han enfrentado a contenidos terroristas, a veces espantosos, online. Más recientemente, ha aumentado la preocupación por el papel de las redes sociales en la difusión de información falsa o engañosa que puede tener consecuencias políticas o para la salud y la seguridad. Mientras que Europa ha tomado medidas para restringir y vigilar ese uso indebido, Estados Unidos no ha tomado medidas significativas, ya que la mayor parte del discurso está protegido por la Primera Enmienda de la Constitución de los Estados Unidos. Solo unos pocos temas como la pornografía infantil o aquella identificada como "apoyo material" a los terroristas se han hecho ilegales. Desde las elecciones de 2016, ha aumentado el debate, especialmente en el Congreso, sobre el papel de las redes sociales en la difusión de información falsa o engañosa. Las plataformas de redes sociales han respondido exigiendo una mayor transparencia en la identificación de los anunciantes, pero no se ha aprobado ninguna legislación significativa.

Diferencias de perspectiva

Como revela esta comparación entre los enfoques de Estados Unidos y la Unión Europea en materia de política digital, hay dos grandes diferencias de perspectiva. En primer lugar, Estados Unidos ha tratado en general la economía digital como una extensión de la economía tradicional y han aplicado la reglamentación existente en materia de privacidad, contenidos, protección del consumidor, política de competencia y otros temas. La Unión Europea (y la mayoría de los estados miembros) ha considerado que la economía digital plantea nuevos desafíos, tanto a los consumidores como a las empresas, que requieren nuevas reglamentaciones. En particular, la preocupación por la seguridad de los datos de los ciudadanos, el papel de las plataformas al vincular a compradores y vendedores, y la posibilidad de que haya contenidos perjudiciales en las redes sociales ha impulsado un esfuerzo por diseñar un régimen normativo amplio para el mundo *online*.

En segundo lugar, si bien las autoridades europeas y los líderes de opinión suelen presentar este esfuerzo como del camino para lograr la soberanía digital europea, estas palabras casi nunca se escuchan en Estados Unidos, y con razón. La búsqueda europea de la soberanía digital tiene su origen en la percepción de que hasta la fecha Europa ha estado dominada por empresas ajenas a la UE, especialmente empresas estadounidenses y chinas, en el espacio digital. Esto no es una percepción errónea. De las 100 principales empresas digitales identificadas por *Forbes* en 2019, solo una empresa de la Unión Europea (Deutsche Telekom) ocupó los 20 primeros puestos, mientras que las empresas de los Estados Unidos se adjudicaron 12 puestos; China y Japón, dos cada uno; y Hong Kong, Corea del Sur y Taiwán, uno cada uno. Menos del 4 % de la capitalización del mercado de las 70 plataformas más grandes del mundo es europea. En enero de 2020, solo Apple estaba valorada en 1,42 billones de dólares, más que todo el índice DAX de las 30 principales empresas de Alemania.

Para EE.UU., hogar de los llamados GAFA (Google, Apple, Facebook, Amazon), no ha habido necesidad de recuperar la economía digital de la influencia de las empresas no estadounidenses. La presencia de grandes actores chinos online se ha convertido recientemente en una preocupación, principalmente en los ámbitos de la infraestructura y la seguridad. Como resultado, la preocupación europea sobre las empresas tecnológicas de EE.UU. ha parecido desconcertantes e incluso fuera de lugar para muchos círculos de la industria y el gobierno de EE.UU. Algunos han cuestionado la capacidad de Europa para alcanzar sus objetivos, mientras que otros han argumentado que se trata de un simple proteccionismo, destinado a establecer una "Fortaleza Europea" digital. Además, la retórica europea sobre la soberanía ha levantado sospechas entre algunos en el sector tecnológico y la comunidad política de Estados Unidos: ¿soberanía de quién y con qué propósito? Muchos en la UE describen la soberanía digital como la versión tecnológica de la "autonomía estratégica", la ambición de la UE de lograr la resistencia y capacidades más significativas en los ámbitos tradicionales de la defensa y la seguridad. Sin embargo, muchos en Estados Unidos, incluso en la comunidad política transatlántica, se hicieron preguntas similares sobre la autonomía estratégica: ¿autonomía de quién? y se interpretó que su objetivo final era distanciar a la UE de EE.UU.

La administración Trump ha sido particularmente desconfiada de las ambiciones de la UE en el sector

de la defensa, en comparación con los gobiernos anteriores. La administración ha sido menos expresiva en cuanto a la preocupación por la política digital de la UE, en parte porque las cuestiones digitales simplemente no han sido una prioridad. Con pocas excepciones, esta administración ha mostrado poco interés en la tecnología o la política digital, ya sea en los Estados Unidos, en el G7 o en el G20, o en relación con los principales socios comerciales y de inversión. La única excepción es la perspectiva de un impuesto sobre los servicios digitales, que ha causado mucha preocupación. Francia aprobó ese impuesto, que habría afectado a las empresas (principalmente a las plataformas estadounidenses) que generan 750 millones de euros en servicios digitales globales y 25 millones de euros en Francia. La administración Trump amenazó con imponer aranceles a las mercancías francesas, hasta que Emmanuel Macron aceptó no aplicar el impuesto mientras se estaba llevando a cabo el esfuerzo de la OCDE por encontrar una solución de consenso. Se espera que ese proceso concluya a finales de 2020, pero la administración Trump ha suspendido recientemente su participación en el esfuerzo, alegando que "no se estaba avanzando".

Sin embargo, EE.UU. no puede ignorar eternamente el impacto de la búsqueda de la soberanía digital de Europa. La aplicación generalizada del RGPD (incluso por muchas empresas de los Estados Unidos) demostró a Europa que podía crear regulación de alcance mundial. A medida que la UE vaya ampliando su agenda digital, es probable que las empresas estadounidenses se enfrenten a normas adicionales, especialmente en lo que respecta a la gobernanza de los datos, el uso de la IA, la responsabilidad de las plataformas y otras cuestiones digitales. Estas normas pueden afectar, por ejemplo, a la capacidad de las empresas estadounidenses para importar a la UE bienes o servicios que utilizan IA, o a la forma en que gestionan los paquetes de datos derivados de los datos de la UE.

Por lo tanto, EE.UU. y la UE se enfrentan cada uno a un dilema. La UE debe decidir cuán restrictiva será en nombre de la protección de los ciudadanos europeos y del apoyo a la innovación y a las empresas europeas. ¿Discriminará a las empresas no comunitarias? ¿Sus normas, por muy bien intencionadas que sean, impedirán el comercio internacional de servicios digitales y quizás incluso ahogarán la capacidad de Europa para innovar y crecer? A medida que el mundo busca una recuperación económica post-COVID-19, el crecimiento económico europeo, incluido el sector tecnológico, es de interés para todos. Europa debería buscar construir su soberanía digital sin convertirse en una fortaleza digital.

Para EE.UU., la elección se basa en si se compromete o no con Europa a medida que avanza en su agenda digital. La negativa a comprometerse o incluso la continuación de la negligencia de los últimos tres años, no impedirá el avance de la UE. Las empresas estadounidenses tendrán que cumplir con las normas de la UE o perderán un mercado relevante. La elección inteligente para Estados Unidos es comprometerse con la UE y trabajar conjuntamente para dar forma a su emergente legislación. Ese compromiso será más eficaz si se lleva a cabo en una atmósfera de cooperación constructiva, que ha estado ausente de la relación entre Estados Unidos y la Unión Europea durante algún tiempo. Los Estados Unidos deberían buscar un compromiso ante la próxima legislación de la UE en la gobernanza de datos, la IA y los servicios digitales. Debería volver a participar en el proceso de la OCDE sobre la tributación de los servicios digitales. Construyendo su propia ley federal de privacidad, EE.UU. se pondrían al mismo nivel que Europa y eliminarían algunas de las incertidumbres que rodean la continuación del flujo transfronterizo de datos a través del Atlántico. Por último, los Estados Unidos y la Unión Europea deberían inaugurar conjuntamente un Consejo Digital para proporcionar a sus máximos dirigentes un foro para debatir la rápida evolución de la economía digital y la forma en que los Estados Unidos y la Unión Europea pueden adoptar el mejor enfoque para sus ciudadanos y la prosperidad común.

Inteligencia Artificial: hacia una estrategia paneuropea

Andrea Renda

Investigador senior y director de Gobernanza global, Regulación, Innovación y Economía Digital (GRID) en el Center for European Studies (CEPS)

En los últimos años, se ha observado el aumento de la relevancia de la IA como prioridad de política pública, especialmente en los países desarrollados. Superpotencias como China y Estados Unidos compiten por dominar este campo, dedicando niveles de inversión sin precedentes y emprendiendo agresivos movimientos estratégicos para fortalecer su posición en el escenario mundial. Académicos y ONGs denuncian los ejemplos extremos de "capitalismo de la vigilancia" en EE.UU. y de vigilancia autoritaria en China. Estas continuas tensiones, que abarcan todo el ámbito de la política digital y que se ejemplifican con la prohibición sobre Huawei adoptada por Estados Unidos, son un importante obstáculo para lograr un sistema aceptado mundialmente de normas y regulaciones sobre la IA. Las iniciativas por parte de varios países (por ejemplo, Francia, Canadá y Japón) para crear un Grupo Intergubernamental sobre Inteligencia Artificial, y más tarde una Asociación Mundial sobre la IA, se ha visto socavada por la falta de confianza y la creciente competencia entre Estados Unidos y China, hasta el punto de que algunos analistas consideran que la perspectiva inminente de una "red fragmentada" o "*splinternet*" es una evolución probable en este ámbito cada vez más estratégico.

En este contexto, la Unión Europea inició su debate sobre la IA en 2017 de manera bastante distópica, con la resolución del Parlamento Europeo sobre las normas de Derecho civil sobre robótica, que preveía el surgimiento de robots autónomos inteligentes y evocaba la necesidad de atribuir derechos y deberes a estas nuevas entidades jurídicas. En la misma resolución también se pidió a la Comisión Europea que considerara la posibilidad de crear un organismo para la IA y estableciera un marco de políticas públicas amplio para mitigar los riesgos de esta potente tecnología de doble uso. Debido a su enfoque casi exclusivo en los riesgos de la IA, la posición del Parlamento provocó una reacción muy crítica de la comunidad científica, pero al menos colocó a la IA en el radar de la política europea: unos meses más tarde, el Consejo Europeo también pidió a la Comisión que tomara medidas para abordar el problema de la IA.

La estrategia sobre la IA de la Comisión se puso en marcha oficialmente con la adopción de una comunicación en abril de 2018. La comunicación, que se publicó paralelamente a las propuestas de la Comisión sobre el establecimiento de un "espacio europeo común de datos", adoptó una postura más positiva hacia la IA en comparación con la resolución inicial del Parlamento Europeo. Sentaba las bases de una estrategia integral sobre IA al aclarar los principales elementos de la futura combinación de políticas de la UE en materia de IA. El principal supuesto que subyace a la estrategia es que Europa "puede liderar el desarrollo y la utilización de la IA para bien y para todos, basándose en sus valores y sus fortalezas". Esos puntos fuertes, según sugirió la Comisión, incluyen investigadores, laboratorios y empresas de reciente creación de prestigio mundial; puntos fuertes en robótica e industrias líderes en el mundo especialmente en el transporte, la salud y la manufactura; el mercado único digital; y una "riqueza de datos industriales, de investigación y del sector público que pueden abrirse para alimentar los sistemas de IA".

"Europa puede liderar": los primeros pasos de la estrategia de la UE sobre IA y la labor del Grupo de Expertos de Alto Nivel

El supuesto principal de que "Europa puede liderar" iba acompañado de tres compromisos separados, pero complementarios: aumentar la inversión hasta un nivel que se corresponda con el peso económico de Europa; no dejar a nadie atrás, en particular en lo que se refiere a la educación y a garantizar una transición fluida hacia la era de la IA en el ámbito del trabajo; y garantizar que las nuevas tecnologías reflejen los "valores" europeos. Con respecto a este último compromiso, la Comisión hizo referencia explícita al Reglamento General de Protección de Datos (RGPD), que en ese momento aún no había entrado en vigor, así como al artículo 2 del Tratado de la Unión Europea, en el que se enumeran los valores fundacionales de la UE como el respeto de "la dignidad humana, la libertad, la democracia, la igualdad, el Estado de derecho y el respeto de los derechos humanos, incluidos los derechos de las personas pertenecientes a minorías" y una "sociedad en la que prevalezcan el pluralismo, la no discriminación, la tolerancia, la justicia, la solidaridad y la igualdad entre mujeres y hombres".

Asesoramiento de expertos: directrices éticas y recomendaciones de inversión

En la comunicación también se anunciaba la adopción de una serie de iniciativas sobre la IA, incluida la creación de un Grupo de expertos de alto nivel sobre la IA (AI HLEG), así como el lanzamiento de una Alianza de la IA, que atrajo rápidamente a miembros de la sociedad civil, la industria y el mundo académico, más de 4.200 a fecha de 15 de mayo de 2020. Se pidió a los 52 expertos del Grupo que elaboraran una serie de directrices éticas, que se publicaron en abril de 2019, y que formularan recomendaciones sobre políticas e inversiones, que se dieron a conocer en junio de 2019.

Las recomendaciones del Grupo de expertos de alto nivel influyeron considerablemente en las instituciones de la Unión Europea. En particular, las directrices éticas introdujeron el concepto de "inteligencia artificial fiable". Esto requería que la IA cumpliera con tres requisitos acumulativos: cumplimiento legal, alineación ética y robustez sociotécnica, por ejemplo, en términos de seguridad, protección y fiabilidad. Las directrices representaron un paso adelante en comparación con los principios éticos adoptados con anterioridad por muchas empresas, gobiernos (como la Declaración de Montreal) y ONGs (como la Declaración de Toronto), redactada por Amnistía Internacional y Access Now, debido, en particular, a sus referencias al cumplimiento de la ley, junto con los posibles medios de verificación y aplicación.

El Grupo destacó que todo enfoque de inteligencia artificial "centrado en el ser humano exige que se respeten los derechos fundamentales, estén o no protegidos explícitamente por los tratados de la Unión Europea, como el Tratado de la Unión Europea o la Carta de Derechos Fundamentales de la Unión Europea. Los expertos sostuvieron, por ejemplo, que esos derechos no consideran a los seres humanos como "objetos para ser separados, clasificados, puntuados, agrupados, condicionados o manipulados". Además, sugirieron que el compromiso de la UE con nociones como "respeto de la igualdad, la no discriminación y la solidaridad" exige que la IA no produzca nuevas desigualdades, especialmente las que puedan afectar negativamente a "los trabajadores, las mujeres, las personas con capacidades distintas discapacidades, las minorías étnicas, los niños, los consumidores u otras personas en riesgo de exclusión".

En las directrices se identificaron cuatro principios fundamentales, definidos como "imperativos" éticos, para una "IA fiable": el respeto de la autonomía humana, la prevención de perjuicios, la equidad y la explicabilidad, es decir, la información utilizada y el proceso seguido por los sistemas de IA para llegar a determinados resultados o decisiones debe ser lo más transparente y auditable posible para los afectados directa e indirectamente. Los cuatro principios clave se tradujeron entonces, a su vez, en siete requisitos que los sistemas de IA deben cumplir para ser definidos como "fiables". Estos principios incluían campos que reflejan las prioridades fundamentales de la política pública de la UE, como la protección de la privacidad y la búsqueda del bienestar social y ambiental, junto con los requisitos que suelen figurar más comúnmente en los debates en torno a la IA ética, entre ellos la intervención humana y la supervisión, la transparencia, la rendición de cuentas, la robustez técnica y la protección de la diversidad y la evitación del sesgo y la discriminación. Sin embargo, tal vez la característica más innovadora de las directrices éticas sea el intento de ayudar a aumentar el cumplimiento de los requisitos mediante la publicación de una lista de evaluación detallada, que se transformó en una herramienta interactiva basada en la Web en junio de 2020.

En las recomendaciones sobre políticas e inversiones del Grupo de expertos de alto nivel se pedía explícitamente que la evaluación de una "IA

fiable" fuera obligatoria para todos los sistemas de IA desplegados por el sector privado que pudieran tener un impacto significativo en las vidas humanas. Entre ellos se incluye, por ejemplo, la IA que interfiere con los derechos fundamentales de un individuo en cualquier etapa del ciclo de vida del sistema, es decir, desde el diseño hasta el desarrollo, la comercialización, la actualización y, finalmente, la eliminación. La evaluación obligatoria se aplicaría también a la IA relacionada con aplicaciones que, si funcionaran mal, plantearían amenazas específicas para la seguridad de las personas, pondrían en peligro equipamientos o propiedades, o generaran un perjuicio ambiental. Parece claro, por lo tanto, que el Grupo no considera que la "AI fiable" sea simplemente una "meta aspiracional", sino más bien el fundamento de un sistema jurídico totalmente nuevo basado en los riesgos, en el que las aplicaciones críticas que puedan afectar a los derechos fundamentales están sujetas a una evaluación obligatoria. El Grupo también pidió a la Comisión Europea que considerara la posibilidad de establecer una "estructura institucional" que pudiera ayudar a reunir y difundir las mejores prácticas de manera más ágil de lo que normalmente pueden hacerlo jueces, reguladores y legisladores.

El Grupo adoptó una postura crítica respecto de varios usos emergentes de la IA, que se considera que crean riesgos importantes para los usuarios y la sociedad. Entre ellos se encuentran la vigilancia masiva y el uso de armas autónomas letales, sobre las que el grupo de expertos pidió una moratoria internacional. El Grupo también recomendó explícitamente a legisladores y reguladores la formulación de normativas o regulaciones para garantizar que los individuos no sean objeto de "un rastreo o identificación personal, físico o mental injustificado, la elaboración de perfiles y la inducción mediante métodos de reconocimiento biométrico basados en IA, como el rastreo emocional, sistemas empáticos, el ADN, el iris y la identificación del comportamiento, el reconocimiento de afectos, es decir, la capacidad de detectar el estado emocional de un individuo, el reconocimiento de la voz y facial y el reconocimiento de micro expresiones. Estos métodos solo deben permitirse en circunstancias excepcionales, por ejemplo, en el caso de amenazas apremiantes a la seguridad nacional e incluso entonces solo si "se basan en pruebas, son necesarios y proporcionados, y respetan los derechos fundamentales".

El Grupo también recomendó medidas específicas para proteger a los niños, incluida una amplia "Estrategia europea para mejorar la protección de los niños". En particular, sugirió que los legisladores de la UE introdujeran una edad legal a la que los niños recibieran un paquete de datos sin mácula (*clean data slate*)", que se aplicaría tanto al sector público como al privado y recomendó que se supervisara la elaboración de sistemas de IA basados en los perfiles de los niños para garantizar su adecuación a los derechos fundamentales, la democracia y el Estado de derecho.

El Libro Blanco sobre la Inteligencia Artificial: del dicho al hecho

La estrategia de la UE sobre IA alcanzó un punto de inflexión con la llegada de la nueva Comisión Europea liderada por Ursula von der Leyen en diciembre de 2019. La Comisión ha establecido las transiciones verde y digital como sus dos prioridades clave y, en los primeros 100 días de su mandato, la nueva presidenta anunció una iniciativa sobre las consecuencias humanas y éticas de la IA. Al mismo tiempo, y especialmente tras el nombramiento de Thierry Breton como comisario para el mercado interior, la Comisión también ha intensificado sus esfuerzos en la estrategia de datos. Esta cuestión está íntimamente relacionada con la política de IA y es crucial en lo que respecta a futuras cooperaciones y alianzas a nivel internacional, debido a las diferencias existentes en el marco jurídico de la protección y la privacidad de datos en los distintos países, y debido al creciente énfasis de Europa en la soberanía tecnológica y de datos.

El 19 de febrero de 2020, la Comisión lanzó un amplio paquete que contenía sus ideas y acciones sobre la transformación digital, incluyendo un Libro Blanco sobre la IA y una estrategia europea para los datos. El paquete, que es a la vez muy firme y completo, marca otro paso adelante en la búsqueda de Europa para liderar una IA "centrada en el ser humano". Se basa en una visión específica del futuro de los datos y de la IA, incluyendo la expectativa de un próximo cambio de paradigma, de un entorno dominado por las *clouds* a unos datos mucho más diseminados. En los años venideros, la Comisión espera que la actual situación 80/20, por la cual el 80% de los datos están almacenados en la *cloud* y 20% en el nivel local, pase a una situación 20/80, con el 80 % de los datos almacenados a nivel local, por ejemplo, en dispositivos, objetos "ciberfísicos" y *edge computing*. Con este cambio, las plataformas como Google y Alibaba pueden llegar a ser menos dominantes. En ese entorno, la Comisión espera que Europa tenga la oportunidad de competir mediante una nueva infraestructura basada en una *cloud* federada, una infraestructura *cloud* que pueda dar cabida a diversos servicios *cloud* heterogéneos bajo un conjunto común de especificaciones de interoperabilidad, posiblemente ampliando las iniciativas nacionales como GAIA-X; repositorios de datos o *data spaces* dedicados en sectores clave (como la industria manufacturera, la salud y la movilidad); y datos abiertos de instituciones públicas y proyectos de investigación. Estas iniciativas serán apoyadas y reforzadas por una nueva cooperación público-privada sobre IA para desarrollar el conocimiento especializado de Europa, especialmente en robótica y la "IA integrada" (IA integrada en sistemas y dispositivos de hardware).

El Libro Blanco establece el doble objetivo de crear un "ecosistema de excelencia" a lo largo de toda la cadena de valor y un "ecosistema de confianza" único, basado principalmente en un enfoque centrado en las personas. Con ello, refleja el enfoque inicial de la Comisión de 2018, basado en una combinación de competitividad ("excelencia") que requiere investigación e innovación, inversión, capacidades y política industrial, y una IA ética de "confianza" lo que se traduce en un enfoque de la regulación basado en el riesgo.

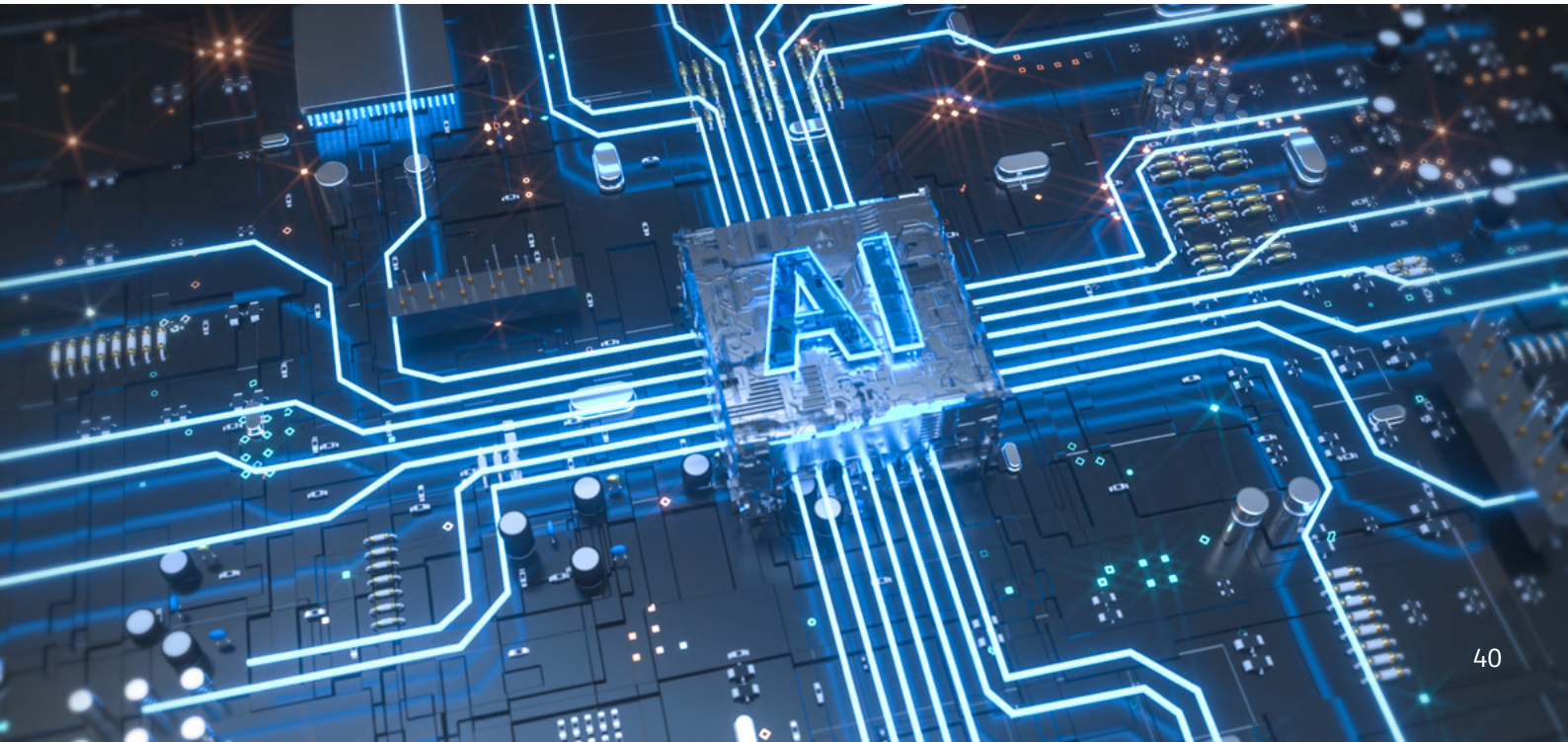
En el lado de la "excelencia", la Comisión anunció la creación de centros de pruebas que pueden combinar inversiones europeas, nacionales y privadas; nuevas medidas de capacitación y apoyo a las pequeñas y medianas empresas; un presupuesto específico para la financiación de capital de inicialmente 100 millones de euros; y, sobre todo, la puesta en marcha de una nueva cooperación público-privada en materia de AI, datos y robótica.

En cuanto al objetivo de la "confianza", junto con los cambios en el régimen de responsabilidad civil por productos, el Libro Blanco refleja la labor del Grupo de expertos. En definitiva, solicita que se adopte un marco regulatorio flexible y ágil limitado a las aplicaciones de "alto riesgo", en sectores como la asistencia sanitaria, el transporte, la policía y el poder judicial, y centrado en las disposiciones relativas a la calidad y la rastreabilidad de los datos, la transparencia y la supervisión humana. Concretamente, la Comisión anuncia que, para las aplicaciones de alto riesgo, las normas podrían referirse a datos de aprendizaje de la IA; el mantenimiento y registro de datos; el suministro de información a los usuarios; y la robustez y precisión del sistema de IA. En esas esferas, también podría haber requisitos de supervisión humana y requisitos específicos para ciertas aplicaciones particulares de la IA, como las utilizadas para la identificación biométrica a distancia. Algunas de las posibles normas ya han suscitado preocupación entre los países no pertenecientes a la UE: por ejemplo, la posibilidad de que los sistemas de IA desarrollados y entrenados fuera de Europa deban recibir un nuevo aprendizaje con datos europeos antes de su comercialización.

En el programa de trabajo de la Comisión se anticipa una iniciativa legislativa sobre la IA para finales de 2020. Prevé dar continuidad al Libro Blanco, enfocada en la seguridad, la responsabilidad, los derechos fundamentales y los datos. Al mismo tiempo, la Comisión está trabajando en una iniciativa legislativa sobre la gobernanza repositorios de datos o *data spaces*, que debería complementar la estrategia de IA creando un enfoque europeo de los datos.

La UE y la gobernanza global de la IA: escenarios futuros

En los últimos dos años, la Comisión ha progresado significativamente en el desarrollo de una estrategia situando a la UE al frente del desarrollo responsable de la IA. Este enfoque de la UE parece estar guiado por la creencia de que si bien Europa puede haberse perdido la primera generación de transformación digital basada en el comercio directo sin intermediarios, la llamada "ola B2C" (*Business to Consumer*), que dio lugar a la aparición de un número reducido de "empresas superestrella" basadas en *clouds*, todavía puede competir en la próxima segunda ola de *edge computing* y almacenamiento de datos más descentralizado y, de hecho, tiene una ventaja en algunas de las tecnologías clave. Aparte del 5G, en el que empresas como Nokia y Ericsson pueden competir con rivales



chinos y surcoreanos, la Comisión ve un mercado favorable para Europa en "sistemas computacionales de baja potencia para el *edge computing* y la próxima generación de computación de alto rendimiento", así como en soluciones neuromórficas, que imitan la arquitectura neurobiológica del cerebro humano y se adaptan bien a la automatización de los procesos industriales y los modos de transporte.

El objetivo de la UE es actuar como un organismo normativo o de desarrollo de estándares globales, tratando de explotar su capacidad reguladora para exportar sus marcos normativos y estándares al resto del mundo. Esto ha sido denominado "poder normativo Europa" o el "efecto Bruselas" por comentaristas y académicos[3]. Tras la experiencia del RGPD, sin duda supondrá la introducción de normas extraterritoriales, que tienen carácter obligatorio para quienes deseen interactuar con el mercado único europeo y sus consumidores, independientemente de la ubicación de la sede de la empresa. Sin embargo, en comparación con el RGPD, el enfoque propuesto por la Comisión contiene algunos elementos nuevos interesantes. En particular, la estrategia de datos y el anuncio de la creación de una federación europea de *cloud* basada en GAIA-X darán lugar a una nueva fase del expansionismo regulatorio de Europa. Esto se basará en el código de software, en lugar de simplemente en la ley. Los grandes operadores de *cloud* de países no pertenecientes a la UE ya han reconocido que ser admitidos en la futura infraestructura de *cloud* federada europea implicará la adhesión a un conjunto de protocolos y normas que incorporan el cumplimiento de normas europeas, empezando por la privacidad, pero también abarcando los próximos requisitos para las aplicaciones de alto riesgo de IA. Del mismo modo, los repositorios de datos anunciados en la estrategia de la UE para la IA incorporarán el *acervo* de la UE, el conjunto de derechos y obligaciones comunes que son vinculantes para todos los países de la UE, como código software.

Es difícil predecir si la estrategia de la UE tendrá éxito a escala internacional. La Comisión parece haber entendido que, sin una amplia alianza internacional para el desarrollo de una IA responsable, los esfuerzos de la UE se verán empequeñecidos por las gigantescas inversiones y los esfuerzos militares de EE.UU. y China. Los avances iniciales, como la propuesta de creación de un Panel Intergubernamental sobre IA y la Cooperación Global sobre AI (Global Partnership on AI), han llevado a un punto muerto debido principalmente a la oposición de las dos superpotencias en pugna. Y aunque la OCDE y el G20 han convergido en gran medida con el enfoque de la UE en sus principios para una IA responsable, estos prometedores avances pueden no dar lugar a un futuro más armonioso y coordinado debido a los aparentemente divergentes intereses del "G2". Las razones no son difíciles de discernir: si bien los principios regulatorios para la IA adoptados por Estados Unidos en enero de 2020 parecen marcar un paso importante hacia la convergencia de los principios ampliamente acordados para una IA responsable, los "Principios de IA de Pekín"(*Beijing* AI Principles)" recientemente adoptados y el respaldo de facto de China al proceso OECD / G20 los hacen menos interesantes desde el punto de vista estratégico para una Casa Blanca que, hasta ahora, se ha centrado más en excluir a China y llegar a un acuerdo con los "países afines".

La profundización de la cooperación internacional también implicaría la adopción de medidas a un nivel más técnico. Actualmente se está llevando a cabo un esfuerzo conjunto de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional para coordinar el desarrollo de estándares de tecnología digital, mientras que la Asociación de Normalización del IEEE, una organización profesional de ingenieros está creando normas de proceso en otros campos, incluyendo la gestión de ingeniería de software y el diseño de sistemas autónomos. En la cooperación internacional también se fomentará la participación de los actores no estatales, que han sido sumamente activos en los últimos años mediante iniciativas de gran alcance de múltiples partes interesadas o multi stakeholder, como los Principios "Asilomar" sobre el uso de la inteligencia artificial y los Principios de la Asociación sobre la IA.

Si estos esfuerzos fracasan, es posible que surjan otros dos escenarios, que no son necesariamente alternativos ni, de hecho, deseables. Por un lado, un grupo de "países afines" podría crear una coalición que excluyera a las grandes potencias como Rusia y China, basándose en las directrices y requisitos de la UE para una "IA confiable" y estableciendo una cooperación en materia de investigación sobre la protección de la privacidad basada en la tecnología. Por otra parte, esta fragmentación del diálogo internacional sobre la IA podría crear una fractura en la gobernanza global de Internet. Esto puede terminar llevando a una división más profunda de la infraestructura de Internet, como la tan evocada "red fragmentada" o "splinternet". Este último escenario sería disruptivo para el mundo digital, y posiblemente conduciría a un orden global muy inestable, más allá del simple ámbito de la IA o de la economía de Internet.

[3] Anu Bradford, The Brussels Effect. How the European Union Rules the World (Oxford: Oxford University Press, 2020). y Richard Whitman (ed), Normative Power Europe. Perspectivas empíricas y teóricas (Basingstoke: Palgrave Macmillan, 2011).

Desinformación: democracia, plataformas y agentes extranjeros

José Ignacio Torreblanca

Director de la oficina de Madrid del European Council on Foreing Relations y Profesor de Ciencias Políticas en la Universidad Nacional de Educación a Distancia (UNED)

En un mundo donde cientos de millones de personas han vivido la pandemia del COVID-19 pendientes de recibir información vital en sus dispositivos móviles, la falta de acceso a información fiable y verificada se ha convertido en un motivo adicional de preocupación para las autoridades sanitarias. El Secretario General de la Organización Mundial de la Salud ha advertido de la existencia de una "infodemia" en referencia a la preocupante propagación de bulos, *fake news* y desinformación relacionada con este virus mortal. El Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad , Josep Borrell, ha sido tajante a la hora de caracterizar la gravedad del problema: "la desinformación", dijo, "mata". Y algunos estudios han concluido que el volumen de información falsa que circula en los medios sociales durante esta crisis es similar al volumen de información legítima[4].

La infodemia que experimentan los ciudadanos durante esta crisis sanitaria mundial no es un fenómeno aislado, sino más bien un elemento estructural de una crisis de información previa que ahora se ha revelado en toda su crudeza. Por esta razón, y aunque sea un cliché decir que toda crisis es también una oportunidad, esta crisis podría crear las condiciones adecuadas para el progreso en la lucha contra la desinformación. Esta lucha es enormemente compleja y requiere de acciones en múltiples frentes. El derecho a una información veraz y, al mismo tiempo, la responsabilidad de las redes sociales y los operadores de plataformas de Internet deben ser, sin duda, los elementos centrales de la carta de derechos digitales por la que abogan en este libro tanto Anthony Giddens como José María Álvarez-Pallete y cuya promulgación, es objeto de un consenso cada vez más amplio.

La crisis de la información

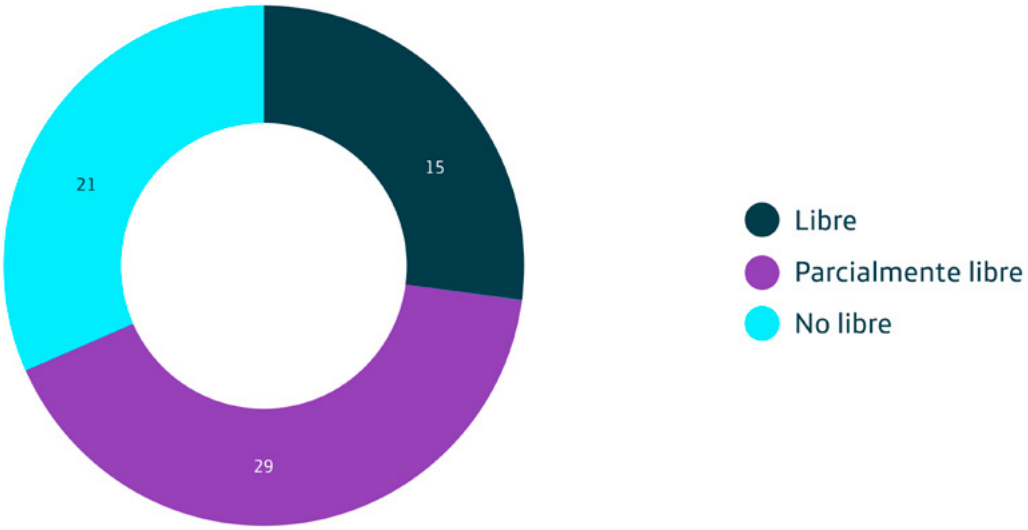
Es sabido que la democracia representativa está atravesando una profunda crisis. Freedom House y otras organizaciones han constatado que hay un retroceso preocupante de la democracia a nivel mundial y un aumento de las fuerzas y movimientos populistas tanto en las democracias como en los estados autoritarios, una tendencia que se manifiesta por su decimotercer año consecutivo.

Este ensayo no trata todas las facetas de la crisis democrática de manera sistemática. Sin embargo, cabe señalar las estrechas conexiones entre la crisis de la democracia representativa y la revolución digital, dado que el cambio tecnológico ha debilitado el papel de los intermediarios democráticos tradicionales: los partidos políticos.

Esta desintermediación dificulta no solo la representación política, sino que erosiona los medios de comunicación tradicionales, cuyo modelo de negocio se ha visto socavado, lo que dificulta mucho más la financiación del periodismo de alta calidad. Esencialmente, esto ocurre debido a la fuga de audiencias y los ingresos por publicidad que la acompañan hacia las plataformas digitales y los medios sociales. Habiendo desintermediado los medios de comunicación tradicionales, los gigantes de la tecnología se han convertido en monopolios cerrados que se aprovechan de su posición dominante para impedir o bloquear el progreso de otras empresas[5]. Debido en gran parte a su naturaleza (aunque también a una

[4] Laura Rosenberger and Philip Howard (2020). "Memo: Disinformation and the Covid Crisis". Global Progress.
[5] Jason Lanier (2018). Diez razones para borrar las redes sociales. Editorial Debate.

Calificación de la libertad en Internet de 65 países



Fuente: Freedom House — ECFR - ecfr.eu

reglamentación inadecuada), estos nuevos intermediarios (plataformas tecnológicas y redes sociales) no proporcionan una nueva intermediación que compense la desintermediación que causan. Por lo tanto, carecen de las cualidades necesarias para generar una esfera pública democrática como alternativa a la que están destruyendo. La prueba de la subsiguiente erosión de la confianza de los ciudadanos puede verse en el hecho de que, según los datos recogidos por el Eurobarómetro en 2018, el 68 % de los europeos dicen estar expuestos al menos una vez por semana a información falsa o que distorsiona la realidad. Resulta revelador que, mientras que el 53 % de los europeos dicen que siguen confiando en la prensa, solo el 24 % afirma confiar en la información que les llega a través de las redes sociales y las aplicaciones de mensajería. La conclusión más alarmante es que el 82 % de los encuestados explican que las *fake news* y la desinformación constituyen un problema para la democracia, una situación que los expertos han descrito como "crisis de la información".

Hackear la democracia

La desinformación y los problemas de representación son anteriores a la era digital. Cada ola de populismo y crisis democrática ha sido asociada con una crisis de información y una tecnología de comunicación. La prensa escrita desempeñó un papel masivo en la movilización de las primeras oleadas de populismo que sacudieron las democracias europeas hacia finales del siglo XIX y la radio ha sido una compañera cercana de todos los regímenes totalitarios, desde los del decenio de 1930 hasta el genocidio de Ruanda. Por lo tanto, mientras que la revolución digital facilita un fenómeno que no es nuevo (la oportunidad de manipular la opinión pública) sí que lo diferencia por su capacidad de hacerlo de forma mucho más rápida y con mayor eficacia y alcance que antes.

Las redes sociales y las plataformas digitales tienen unas características intrínsecamente problemáticas desde el punto de vista de la democracia. La desintermediación mencionada anteriormente, es una de ellas. También lo es un modelo de negocio basado en la llamada "economía de la atención" y en la necesidad de mantener a los usuarios dentro de las aplicaciones el mayor tiempo posible, para exponerlos al máximo número de anuncios y reunir la máxima cantidad de datos sobre su comportamiento. La monetización de la atención requiere la priorización de las emociones y los acontecimientos más llamativos o controvertidos; en términos políticos, esto significa amplificar los mensajes negativos o de confrontación que alimentan la polarización y generan tráfico en las redes.

Otra cuestión es la opacidad de los algoritmos que deciden lo que tiene prioridad y que debe verse primero o con mayor frecuencia por los usuarios de las plataformas y las redes sociales. Un tercer factor es la falta de filtros y controles adecuados, lo que permite que la información falsa se haga pasar por legítima. Al mismo tiempo, los sistemas publicitarios automatizados de las redes permiten y fomentan la creación de sitios web que simulan las páginas auténticas de medios de comunicación, pero que funcionan como

depósitos y recicladores de información fraudulenta. Estos medios de comunicación pretenden ser de naturaleza periodística, pero en realidad son agentes al servicio de una determinada causa de los actores políticos, y su principal objetivo es producir y difundir información falsa[6].

Junto a la transmisión y retransmisión de estos mensajes, verdaderos o falsos, que facilitan las redes sociales a partir de sus algoritmos, existen terceros actores que, mediante el uso de instrumentos avanzados (cuentas falsas o bots), son capaces de crear o amplificar ciertas conversaciones, distorsionando la idea o percepción que tienen otros usuarios de lo que realmente sucede y de lo que se dice en un foro digital. Por ejemplo, como reveló un estudio de Alto Analytics que examinó 25 millones de movimientos en las redes sociales durante la campaña electoral europea de mayo de 2019 en España, el 0,05 % de los usuarios (que mostraron un comportamiento inusual que sugería la automatización de la transmisión y retransmisión de contenidos) fueron responsables de al menos el 10% de los contenidos de carácter político. En otros estudios de la misma empresa se han detectado pautas similares de comportamiento anormal relacionadas con fenómenos como la elección de Jair Bolsonaro como presidente de Brasil, el movimiento de los chalecos amarillos en Francia y los movimientos antivacunas, entre otros.

Las investigaciones sobre el referéndum del Brexit de junio de 2016, junto con las elecciones presidenciales de los Estados Unidos en noviembre de ese año (que llevaron a Donald Trump al poder) han permitido a los analistas comprender mejor cómo ciertos actores sin escrúpulos pudieron explotar algunas de esas características de las redes sociales para manipular el sentimiento de los votantes y, potencialmente, influir en el voto. El Proyecto Lakhta, una granja de "*trolls*" de Internet situada en San Petersburgo y coordinada por la Internet Research Agency, publicó 10 millones de tuits, 116.205 posts falsos en Instagram, 1.107 vídeos en YouTube y 61.483 posts en Facebook, con lo que obtuvo una audiencia combinada de 126 millones de personas en Estados Unidos. Esa enorme actividad digital no solo fue importante en términos cuantitativos, sino que también fue relevante su impacto cualitativo en el sentido de que estaba diseñada y dirigida con pautas muy precisas de segmentación de los mensajes entre las comunidades. Un ejemplo de cómo la campaña llevó a los votantes de derecha a votar fue a través de anuncios falsos en los que organizaciones musulmanas supuestamente auténticas, con apariencia de estar radicadas en EE.UU. pero en realidad creadas en San Petersburgo, apoyaban la campaña presidencial de Hillary Clinton ("Muslims for Hillary").

La campaña Trump se benefició de una convergencia de instrumentos de microsegmentación y desinformación utilizados por el Kremlin. Este esfuerzo fue dirigido por Steve Bannon, financiado por Robert Mercer (quien también apoyó al Brexit), y diseñado por Cambridge Analytica, una empresa dirigida por Alexander Nix que reunió a los principales expertos en técnicas psicométricas diseñadas para entender las emociones de los votantes y experimentar con cómo manipularlas eficazmente.

La facilidad con la que se pudo presentar información distorsionada, manipular las emociones e influir en las intenciones de voto de millones de estadounidenses no solo se debió a la falta de escrúpulos de un puñado de empresas o empresarios y operadores políticos, sino a la sencilla forma en que estas compañías, gracias a su colaboración con Facebook como desarrolladores de aplicaciones comerciales, pudieron apropiarse de los datos personales de 87 millones de ciudadanos estadounidenses y utilizarlos con fines políticos. De esta manera, obtuvieron información valiosa sobre los votantes que otros líderes de campañas políticas y encuestadores no tenían, lo que permitió al equipo de Trump concentrar los recursos y mensajes de la campaña en 13,5 millones de votantes potenciales en 16 estados clave del Medio Oeste. Esto era algo que las campañas convencionales no habían logrado anteriormente, debido a la ausencia de datos precisos sobre los perfiles de estos votantes.

Se ha estimado que el impacto combinado de estas acciones significó que el 25 % de los ciudadanos estadounidenses estuvieron expuestos a algún elemento de noticias falsas durante el pico del período de la campaña (octubre-noviembre de 2016). Pero esta tasa fue más pronunciada entre los votantes conservadores: seis de cada diez visitas a falsos agregadores de noticias se concentraron en el 10 % de los votantes más conservadores. Además, las personas mayores fueron las más susceptibles de estar expuestas a estas estrategias: los estudios posteriores demostraron que los mayores de 65 años fueron cinco veces más propensos a compartir noticias falsas que las personas entre 18 y 25 años.

Aunque empresas como Facebook han negado repetidamente ofrecer a sus clientes productos basados en información sobre los estados emocionales de sus usuarios, hay muchos indicios de que sí que lo habrían hecho. Facebook no solo parece haber reunido información emocional, sino que también puede haber experimentado satisfactoriamente con ella, mediante técnicas diseñadas para impulsar la participación electoral a través de la presión social del grupo de colegas

[6] Kirill Meleshevich and Bret Schafer (2018). "Online information Laundering: The Role of Social Media". Alliance for Securing Democracy, Policy Brief. No. 002.

más cercano al votante. En las elecciones al Congreso de EE.UU. de 2019, movilizó a 340.000 votantes adicionales, a través de un experimento que involucró a 61 millones de usuarios. Facebook también ha estudiado la forma de influir en las opiniones políticas de sus usuarios e incluso en sus votos, cambiando el orden y la secuencia de la información sobre los candidatos y los partidos en su plataforma de acuerdos con teorías sobre el "contagio emocional"[7].

La geopolítica de la desinformación

La interferencia en las elecciones constituye solo una pequeña parte del problema de la desinformación; su alcance y sus repercusiones la han convertido en un problema mundial de máxima importancia. La organización Freedom of the Net identifica a unos 30 gobiernos que actúan como productores y difusores de contenidos destinados a distorsionar la información que circula por Internet, señalando a Rusia, China, Irán y Arabia Saudita como principales responsables.

Como ha quedado acreditado durante la crisis del COVID-19, la información se ha convertido en el nuevo campo de batalla en la competencia geopolítica entre los regímenes autoritarios y las democracias liberales. En el caso de Rusia, se trata cada vez más de una actividad destinada a sembrar la confusión y la desconfianza en los científicos y los políticos. Por su parte, la estrategia de China tiene como objetivo ocultar el perjuicio que el origen y el encubrimiento inicial del virus han causado a su imagen internacional[8].

Que Moscú y Pekín sean los actores que hacen el uso más sistemático de la desinformación no es

[7] Adam Kramer, Jaimie Guillory, and 7. 7. 7Jeffrey Hancock (2014). "Experimental evidence of massive-scale emotional contagion through social networks". Proceedings of the National Academy of Sciences, June 17, Vol. 111. No. 24.
[8] Juan Pablo Cardenal (2020) "Propaganda china para un escenario post Covid-19". Centro para la Apertura y el Desarrollo de América Latina.

una coincidencia. Este fenómeno tampoco se limita a la cuestión del COVID-19; de hecho, lo hacen de forma estratégica. Este es el caso por dos razones. En primer lugar, el control de la información es una necesidad existencial de los regímenes autoritarios; las dictaduras no pueden coexistir con la libertad de información. Por lo tanto, necesitan desarrollar y desplegar estrategias basadas en la propaganda y la desinformación, que luego pueden replicar externamente[9].

En segundo lugar, en un entorno geopolítico hostil, difundir desinformación es esencial, al menos por dos razones. Una, de forma defensiva, en tanto que necesitan bloquear o filtrar el acceso de sus ciudadanos a las noticias verídicas del exterior; otra, de manera proactiva u ofensiva con el objetivo de debilitar o disuadir a los enemigos. Esta última estrategia, que consiste en la difusión de información falsa y maliciosa que socava la confianza del enemigo en sí mismo y, por lo tanto, su voluntad o capacidad de enfrentamiento, ha dominado las relaciones entre Rusia y Occidente durante el último decenio.

Paradójicamente, en el caso de Rusia, la consistencia y la perseverancia en sus estrategias de desinformación están directamente relacionadas con su debilidad. A pesar de tener inmensos recursos naturales y poderosas fuerzas armadas, los líderes de Rusia son conscientes de que el poder occidental es superior en las esferas económica y militar.

Pero mucho más amenazante que el poderío militar de Occidente es el atractivo de su modelo de vida para los ciudadanos rusos. Desde la secesión de Kosovo y las protestas prodemocráticas en Rusia en diciembre de 2010, el régimen ruso ha comprendido que su supervivencia depende de que se debilite el atractivo del modo de vida de Occidente, tanto a los ojos de su propio pueblo como de los propios ciudadanos occidentales. Esto ha impulsado una estrategia que refuerza la naturaleza vertical del poder dentro de Rusia y, paralelamente, una estrategia externa diseñada para aumentar la desconfianza de los occidentales en sus instituciones democráticas. Esta estrategia les lleva a impulsar el apoyo a las fuerzas antisistema que tienen más posibilidades de llevar al poder a los partidos populistas euroescépticos en cada país, desde el *Rassemblement National* de Francia a *Alternative für Deutschland*, pasando por la *Lega* italiana, en la esperanza de que estas fuerzas debilitarán tanto la cohesión intraeuropea como la relación transatlántica[10].

La desinformación debilita las democracias y, simultáneamente, fortalece los regímenes autoritarios. Los medios de comunicación de masas y las herramientas de propaganda totalitaria del pasado han dado paso a medios de vigilancia masiva que se combinan con la tecnología de inteligencia artificial, lo que permite un control más estricto de los ciudadanos mediante la recopilación y explotación de datos para recopilar perfiles políticos de los mismos. A pesar de que Internet nació en medio de sueños utópicos de libertad mundial y conocimiento universal, el 71 % de los 3.800 millones de personas que ahora tienen acceso a la web viven en países donde pueden ser multados o encarcelados por expresar sus opiniones políticas o sus sentimientos religiosos en línea, y el 56 % en estados cuyas autoridades bloquean el contenido por razones ideológicas. De hecho, solo el 20 % de los usuarios de Internet viven en países que se consideran libres e, incluso en los países en que se celebran elecciones, solo el 7% de los usuarios pueden votar sin riesgo de interferencia electoral.

Deber de diligencia

El bien intencionado utopismo que presidió los comienzos de la revolución digital tuvo su traducción en un conjunto de regulaciones sumamente laxas. En 1996 los Estados Unidos aprobaron la Ley de Decencia en las Comunicaciones (*Communications Decency Act*), cuyo artículo 230 establece que "ningún proveedor o usuario de un servicio informático interactivo será tratado como editor o portavoz de ninguna información proporcionada por otro proveedor de contenido informativo". El objetivo era preservar la libertad de expresión y permitir el crecimiento y la innovación en el sector digital, y esto se logró sin duda alguna. Sin embargo, en la práctica, convirtió a las plataformas digitales en "tablones de anuncios" que estaban exentos de toda responsabilidad por su contenido, salvo en un número muy reducido de casos.

La Ley de Decencia en las Comunicaciones ignoró el hecho de que estas empresas eran mucho más que meros depósitos neutrales en los que los usuarios colocaban sus contenidos; de hecho, han sido y son agentes activos que ordenan, secuencian y retransmiten los contenidos para monetizarlos mediante la venta de publicidad, convirtiéndolos efectivamente en editores. Como ocurre con otras plataformas digitales como Uber, la paradoja es que

[9] Sergey Sanovich (2017). "Computation Propaganda in Russia: The Origins of Digital Misinformation". Computational Propaganda Research Project, Working Paper No. 2017.3.
[10] Mira Milosevich (2017). "El poder de la influencia rusa: la desinformación". Análisis del Real Instituto Elcano. 20 January 2017.
[11] William Perrin (2020). "Implementing a duty of care for social media platforms" Renewing Democracy in the Digital Age. Berggruen Institute.

no estaban reguladas inicialmente con respecto al servicio que prestaban ni con arreglo a la legislación del sector al que las empresas decían pertenecer, sino que habitaban una especie de limbo jurídico en el que, en su mayor parte, permanecen hoy en día.

De ese pensamiento utópico bienintencionado en los inicios de las redes sociales ha pasado a una visión mucho más pesimista de la compatibilidad de la democracia con estas redes. Ahora que se ha revelado el funcionamiento comercial de los servicios que prestan estas empresas, por no hablar de su permeabilidad a las potencias y agentes extranjeros, el discurso que rodea al foro mundial, el nacimiento de una conciencia mundial y lo que Mark Zuckerberg ha denominado el "Quinto Estado" han perdido su brillo. Las acciones maliciosas de los estados autoritarios son posibles en gran parte debido a que las democracias han fracasado a lo hora de dotar de una regulación adecuada de las redes sociales. Por eso se necesita un enfoque reglamentario totalmente nuevo del problema, basado en el deber de diligencia por parte de las plataformas[11].

Ese enfoque regulatorio es algo que la UE está bien situada para aplicar, e incluso liderar a nivel mundial. Hasta ahora, la Casa Blanca y el Congreso han mostrado escasa capacidad o interés en hacer frente al sector tecnológico estadounidense, que contribuye de manera sustancial a la influencia mundial y al bienestar económico de los Estados Unidos, así como a la financiación de las campañas electorales. Además, la Primera Enmienda de la Constitución de Estados Unidos de América impone límites mucho más estrictos a la posibilidad de restringir la libertad de expresión que la legislación europea. Por su parte, China trata de crear su propio Silicon Valley a escala local para aprovechar al máximo la capacidad de las nuevas tecnologías en el ejercicio del control social y, de ese modo, sostener el régimen autoritario del Partido Comunista Chino con una capa asfixiante de tecnología digital.

Por el contrario, la Comisión Europea ya ha tenido éxito en el campo de la privacidad con el Reglamento General de Protección de Datos[12]. La introducción del reglamento fue un momento decisivo para las grandes empresas de tecnología, que se vieron obligadas a adoptar normas de privacidad mucho más estrictas en Europa que en Estados Unidos. En ámbitos como el derecho de autor, la inteligencia artificial, la protección de los menores, el derecho al olvido y la desinformación, la UE ha dado muestras claras de que tiene capacidad para convertirse en un regulador y fijador de normas a escala mundial, lo que ha llevado a algunos a describir el bloque como una "superpotencia reguladora"[13].

La Comisión Europea ha decidido tratar la desinformación como una amenaza para la democracia, el orden público, la seguridad de los ciudadanos, la salud pública y el medio ambiente. El enfoque de la Comisión se basa en la idea de que la desinformación no es un subproducto accidental o una consecuencia no deseada de la libertad de expresión en las redes sociales. Ha llegado a la conclusión de que quienes la crean y colaboran en su difusión tienen la misma responsabilidad. Tras intensas negociaciones, se ha logrado que las empresas de tecnología adopten un código de conducta que las obliga a comprobar los perfiles y cuentas falsas así como a informar periódicamente sobre las medidas que han adoptado en este ámbito. Por lo tanto, la Comisión tiene razón cuando afirma que la lucha contra la desinformación requiere un ecosistema digital más transparente y responsable, así como esfuerzos para promover la educación digital y la alfabetización mediática. El enfrentamiento de Twitter con Trump en mayo de 2020, cuando por primera vez, la plataforma invitó a los seguidores del presidente a revisar sus tweets y etiquetó algunos de ellos como una apología de la violencia, marcó un cambio radical que abre nuevas vías (como, por ejemplo, etiquetar los *tweets* de los funcionarios de Rusia o China como también necesitados de verificación).

Además de la Comisión Europea, muchos estados europeos han adoptado o están considerando medidas contra la desinformación. Pero no es una batalla fácil. Como en tantas otras esferas de regulación, señalar lo que hay que prevenir es mucho más fácil que elaborar un catálogo de medidas que resuelvan el problema, especialmente cuando, como se ha mencionado anteriormente, el problema es el propio ecosistema. Por ejemplo, el gobierno alemán ha optado por una estrategia que consiste en multar a las plataformas de Internet que no logren erradicar el contenido que se haya denunciado y verificado como falso o que constituya un delito de incitación al odio. Francia, por otra parte, ha elegido la ruta de establecer un control judicial sobre el contenido de las plataformas[14].

La otrora cómoda existencia de las plataformas tecnológicas, que antes se caracterizaba por un crecimiento continuo de los ingresos y los usuarios, está dominada hoy en día por la preocupación por la sostenibilidad de sus negocios. Como dijo un representante de una de las mayores empresas del sector en uno de los seminarios celebrado por el Consejo Europeo de Relaciones Exteriores parte de este proyecto de investigación, las plataformas

[12]Boletín Oficial del Estado (2016). "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
[13]Anu Bradford (2020). The Brussels Effect: How the European Union Rules the World. Oxford University Press, USA.
[14] Carme Colomina (2019), "La desinformación de nueva generación" (Anuario Internacional CIDOB: páginas. 61-66).

tecnológicas ya no se sienten seguras a la hora de ofrecer garantías de que el contenido publicado en sus sitios cumple con la legislación, incluso si contratan a miles de personas para comprobar lo que publican los usuarios. Y esto es comprensible. Si en un mismo país dos jueces pueden dictar sentencias completamente diferentes sobre el significado de las expresiones mostradas en la red, cuando la red es global el desafío aumenta exponencialmente. Así, lo que un juez de Estados Unidos podría considerar que está protegido por la libertad de expresión podría constituir un delito penal como la incitación al odio en Alemania.

Un problema adicional que plantea la cuestión de la regulación es el de la eficacia. Cualquier paso hacia el control o la prohibición siempre provoca una adaptación por parte del oponente. La regulación y los límites impuestos a los contenidos visibles en Facebook y Twitter ya han tenido la consecuencia involuntaria de incentivar la migración de los contenidos tóxicos a redes como WhatsApp (donde la distribución podría ser igual o incluso más viral, pero la detección y el control es mucho más difícil de lograr) o a otras plataformas cerradas. La tecnología siempre va un paso por delante del regulador, especialmente en lo que respecta a los ámbitos ilícitos, y esto significa que es demasiado fácil para los gobiernos acabar con lo peor de ambos mundos, sacrificando la libertad sin conseguir seguridad.

Por último, es imposible ignorar el hecho de que, junto con los problemas de desinformación del lado de la oferta, también hay problemas en términos de demanda. Estas van desde las predisposiciones psicológicas y cognitivas de las personas a recibir y compartir este tipo de información, hasta otras cuestiones relacionadas con la falta de una cultura política o de noticias que, por lo tanto, requieren iniciativas educativas que son por su propia naturaleza difíciles de llevar a cabo en una democracia[15].

Conclusión

Los dilemas son claros: dar a los gobiernos el poder de censurar el contenido que actualmente está en manos de las empresas tecnológicas es tan mala idea como dejarla en manos de las propias empresas. Al mismo tiempo, la ausencia de límites podría dañar la esfera democrática pública y hacerla permeable a la desinformación tanto de agentes locales como extranjeros; erosionar la confianza de los ciudadanos en las instituciones; y causar un daño significativo a las personas y a los derechos específicos.

Por lo tanto, la UE y sus estados miembros deben actuar de manera diferenciada en varios frentes. En el frente internacional, deberían adoptar medidas firmes contra quienes utilizan la desinformación como arma para debilitar las democracias, al tiempo que lideran una respuesta reguladora mundial basada en los valores y principios universales que sustentan la democracia representativa: los derechos humanos y un orden liberal multilateral basado en normas muy beneficiosas para Europa. En el frente doméstico, si bien los usuarios deben ser protegidos de los peores y más evidentes perjuicios en las redes que violan sus derechos fundamentales, la UE debería adoptar un enfoque constructivo y cauteloso para construir y sostener un espacio público de alta calidad y organizaciones de medios de comunicación que proporcionen hechos precisos para el debate público (en contraposición a la polarización y los ataques a las instituciones democráticas). Esto requiere una triple alianza entre gobiernos, empresas y ciudadanos responsables, una alianza basada en el diálogo y la experimentación.

[15] Jean-Baptiste Jeangène, Alexandre Escorcia, Marine Guillaume, and Janaina Herrera (2018). "Information Manipulation: A Challenge for Our Democracies", report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August.

Banda ancha: el silencioso aliado digital de Europa

Alicia Richart
Fundadora y CEO de DigitalES

El 18 de marzo de 2020, justo en el momento más álgido de la pandemia COVID-19, Thierry Breton, el Comisario europeo responsable del mercado interior, se reunió con Reed Hastings, cofundador y director general de Netflix, para discutir cómo mantener el funcionamiento de Internet sin saturaciones, ya que las medidas de confinamiento aprobadas por los gobiernos de todo el continente dispararon las actividades cotidianas que se realizaban *online*. La reunión se celebró en medio de los temores de que las redes de fibra óptica no pudieran soportar el aumento del tráfico causado por el consumo masivo de ancho de banda tanto para uso profesional como doméstico.

Breton, cuya cartera incluye las estrategias de seguridad cibernética y servicios digitales, reveló las conclusiones de la conversación en un tweet pidiendo a los usuarios su cooperación: "Para asegurar el acceso a Internet para todos, vamos a cambiar a modo estándar (#SwitchToStandard cuando la definición HD no sea necesaria". El Comisario argumentó: "el teletrabajo y la transmisión en directo (streaming) ayudan mucho, pero las infraestructuras pueden verse sometidas a presión". De acuerdo con su petición, Netflix se comprometió a reducir la velocidad de descarga, entendida como el número de bits que se transportan o procesan por unidad de tiempo, de todo su contenido en Europa durante 30 días. "Estimamos que esto reducirá el tráfico de Netflix en las redes europeas en alrededor de un 25%, al tiempo que garantiza un servicio de buena calidad para nuestros miembros", sugirió la empresa. En otras palabras, reduciría la calidad de sus emisiones para no colapsar las redes de banda ancha. La misma petición ("adoptar medidas para garantizar el buen funcionamiento de Internet durante la batalla contra la propagación del virus") fue realizada por el Parlamento Europeo.

Antes de la pandemia, "Preparar a Europa para la era digital" ocupaba el tercer lugar en la lista de prioridades de la Comisión para 2019-2024. Pero esto no era solo otro elemento en la habitual letanía de prioridades. Su nueva presidenta, Ursula von der Leyen, apremió a la Comisión a entregar una estrategia digital en los primeros 100 días de su mandato. En consonancia con este nuevo impulso, el 19 de febrero, poco antes de que la mayor parte de Europa entrara en confinamiento, la Comisión publicó tres documentos importantes: una Declaración sobre el futuro digital de Europa, un Libro blanco sobre la IA y una Estrategia europea sobre datos.

La transformación digital era una prioridad europea mucho antes de la aparición del coronavirus. Sin embargo, no hay duda de que la pandemia ha hecho más por la transformación digital de las sociedades, empresas y gobiernos europeos que cualquier otra política o estrategia. A medida que sociedades y economías enteras entraban en hibernación forzada, los sectores que más rápida y hábilmente digitalizaron la mayoría de sus operaciones, si no todas, se salvaban del colapso económico. Es más, también proporcionaron servicios esenciales a otros sectores y ayudaron a sus países a capear la crisis.

No se puede subestimar el componente digital en la resistencia europea al coronavirus. La mayor parte de esta capacidad depende de que los países tengan redes fiables capaces de sostener no solo operaciones habituales, sino también una incorporación repentina y masiva de nuevas actividades a las redes digitales. Aunque la capacidad de la red era ya una cuestión clave, en la que la Comisión se había centrado antes de la crisis actual, el coronavirus ha puesto de relieve tanto la importancia estratégica de la banda ancha digital como, paralelamente, las vulnerabilidades y asimetrías existentes a las que se enfrentan los Estados miembros de la UE. Después del coronavirus, hay muchas razones para considerar la banda ancha como un elemento clave de la estrategia de Europa para lograr la soberanía digital.

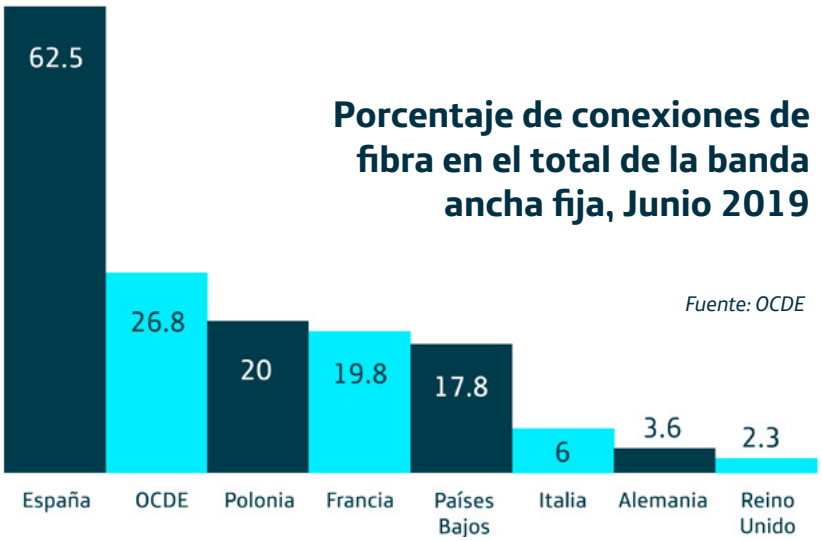
La columna vertebral digital de Europa

Si bien la pandemia de coronavirus ha provocado un rápido aumento de la demanda de banda ancha más rápida en Europa, esta necesidad es previa a la crisis sanitaria. La tecnología de Internet ha comenzado a proporcionar una gama cada vez más amplia de servicios de comunicaciones y acceso a datos y aplicaciones. Estos sostienen enormes volúmenes de tráfico de vídeo y proporcionan conexiones para miles de millones de objetos inteligentes. Esto, a su vez, requiere acceso a banda ancha y, por tanto, una infraestructura de banda ancha robusta.

La Comisión Europea fijó un objetivo ambicioso en su Agenda Digital para Europa de 2014 para garantizar "una cobertura universal de banda ancha con velocidades de al menos 30 Mbps para 2020" y "la adopción de la banda ancha del 50 % de los hogares con velocidades de al menos 100 Mbps para 2020". Esos objetivos reflejaban las marcadas diferencias en cuanto a la infraestructura de banda ancha disponible entre los distintos Estados miembros y entre las zonas urbanas y rurales, incluidas las remotas. La infraestructura de banda ancha es crucial para el desarrollo de la economía digital y puede estimular la innovación, la productividad y el empleo. Así pues, la falta de acceso trae consigo importantes consecuencias para quienes la sufren y crea la llamada brecha digital.

Los objetivos de la UE en materia de banda ancha para 2020 se basaron en la estrategia de la Comisión sobre Conectividad para lograr una sociedad europea del Gigabit en septiembre de 2016. Se estableció el objetivo de garantizar el acceso, para 2025, a un gigabit por segundo (Gbps) a todas las escuelas, centros de transporte, proveedores de servicios digitales y empresas con uso intensivo de tecnología digital; el acceso a velocidades de descarga de un Gbps para todos los hogares europeos; y una cobertura de banda ancha inalámbrica de 5G para todas las zonas urbanas y para los principales ferrocarriles y carreteras. Esto se ha complementado con una serie de iniciativas, entre ellas el nuevo Código Europeo de Comunicaciones Electrónicas, el Plan de Acción del 5G, el Fondo de Banda Ancha para la Conexión de Europa y el Mecanismo 'Conectar Europa'. Se han presupuestado 3.000 millones de euros adicionales en el capítulo digital del marco financiero plurianual 2021-2027 para financiar la infraestructura estratégica de conectividad digital.

El éxito ha sido mixto. Si bien la cobertura de la banda ancha ha mejorado ciertamente en toda la UE, el acceso a la banda ancha rápida es menos uniforme y las zonas rurales siguen siendo importantes puntos débiles. Según el último estudio de la Comisión sobre la cobertura de la banda ancha en Europa, realizado en octubre de 2019, a finales de junio de 2018 casi 223 millones de hogares de la Unión Europea (99.9%) tenían acceso a por lo menos una de las principales tecnologías de acceso a la banda ancha fija o móvil (fibra y 4G,



Porcentaje de conexiones de fibra en el total de la banda ancha fija, Junio 2019

Fuente: OCDE

respectivamente). En el estudio también se constató que el 83,1 % de los hogares de la Unión Europea tenían acceso a la banda ancha más rápida que ofrecen los servicios de acceso de nueva generación. Sin embargo, la cobertura de la banda ancha rural siguió siendo muy inferior a la media nacional en todos los Estados miembros de la UE, y solo el 52,3 % de los hogares rurales de la UE tienen acceso a los servicios de alta velocidad de nueva generación.

Además, la adopción de la tecnología de banda ancha ultrarrápida de fibra hasta el hogar (FTTH) ha sido relativamente lenta en algunos estados miembros. FTTH significa esencialmente que la fibra óptica de la central local se conecta directamente a los hogares a través de enrutadores, lo que permite un servicio de banda ancha ultrarrápido que puede permitir velocidades de 1Gbps. Esto es significativamente más rápido que la línea telefónica de cobre tradicional utilizada por los anteriores servicios de banda ancha. Según el informe de la Comisión, solo el 29.6 % de los hogares de la UE tenían FTTH. La DSL sigue siendo, de lejos, la tecnología de acceso fijo dominante, utilizada por el 92,2% de los hogares, seguida de la VDSL, utilizada por el 56,7 %.

Asimetrías sorprendentes

En la mayoría de las políticas, los Estados miembros se alinean de forma bastante natural según su tamaño o fuerza económica. Pero este no es el caso cuando se trata de la infraestructura de banda ancha. Esta disparidad indica muy claramente que los países miembros de la UE no comparten todavía una visión común sobre la importancia estratégica de la banda ancha o de su importancia como activo vital en tiempos de crisis.

El porcentaje de conexiones de fibra en el total de la banda ancha fija difiere significativamente entre los Estados miembros. Según un informe de junio de 2019, Lituania ocupaba el tercer lugar entre los países de la OCDE, con una tasa de utilización del 74.6 %, en comparación con Bélgica, con un 0.98 %, y Grecia, con un 0.16 %. De los países de la UE, Lituania está seguida por Suecia (68.95 %), Letonia (68.54 %) y España (62.53 %), que ocupa el sexto lugar entre los países de la OCDE y el cuarto lugar en Europa.

Lo que resulta chocante de este cuadro es que Alemania y Francia, que no solo son las dos mayores economías de la UE sino, al menos a primera vista, líderes digitales con estrategias industriales digitales bien concebidas, ocupan el trigésimo tercer y el vigésimo cuarto lugar respectivamente. El hecho de que Alemania vaya después de México y Colombia en las conexiones de fibra indica una enorme falta de inversión por parte de sus autoridades en los últimos años. Sin embargo, lo más importante es que muestra que los Estados miembros de la UE deben considerar la expansión de las conexiones de fibra como una prioridad estratégica. La Comisión también debe asegurarse de que se establezcan objetivos adecuados y se financien con la ayuda de los nuevos instrumentos presupuestarios disponibles en el marco financiero plurianual revisado.

Sin embargo, cabe señalar también que el crecimiento anual de la aceptación de fibra completa es alentador. Varios Estados miembros parecen estar en vías de cumplir el objetivo de 2025 de disponer de una conexión de banda ancha predominantemente con capacidad de gigabit para todos los hogares. En Alemania, parece que la banda ancha ultrarrápida finalmente se está incrementando. Esto es especialmente gracias a las acciones de ciertas ciudades y empresas como Deutsche Glasfaser. El proyecto nacional "Gigabit para Alemania" también es digno de mención a este respecto. En el Reino Unido, que también se ha quedado atrás debido a la decisión de confiar en las soluciones de cobre de VDSL antes de pasar a la fibra, varios actores están aprovechando la oportunidad de construir su negocio aprovechando el vacío existente en el mercado. Francia está claramente en un punto intermedio y todavía tiene objetivos muy ambiciosos que cumplir. Italia, que durante un tiempo disfrutó de una sólida ventaja gracias a las inversiones pioneras de la empresa FastWeb, planea recuperar el terreno perdido. Esto es evidente en el éxito del plan de Fibra Abierta de la compañía nacional de energía, Enel, que había instalado más de 2,5 millones de puntos para los hogares en enero de 2018.

Lecciones aprendidas de España

Como se ha mencionado anteriormente, el informe de la OCDE revela que el 62,53 % de las líneas de banda ancha en España están conectadas por fibra óptica, lo que significa que ocupa el sexto lugar entre 38 países. Su red ultrarrápida es ahora la más grande de Europa, y la más grande en términos del número de hogares que están conectados. A finales de 2019, ascendía a más de 23 millones de hogares. Además, todas las ciudades de más de 10.000 habitantes ya disponen de una red de fibra para utilizarla en cualquier tipo de actividad, incluidas las de empresa a empresa y las de empresa a consumidor.

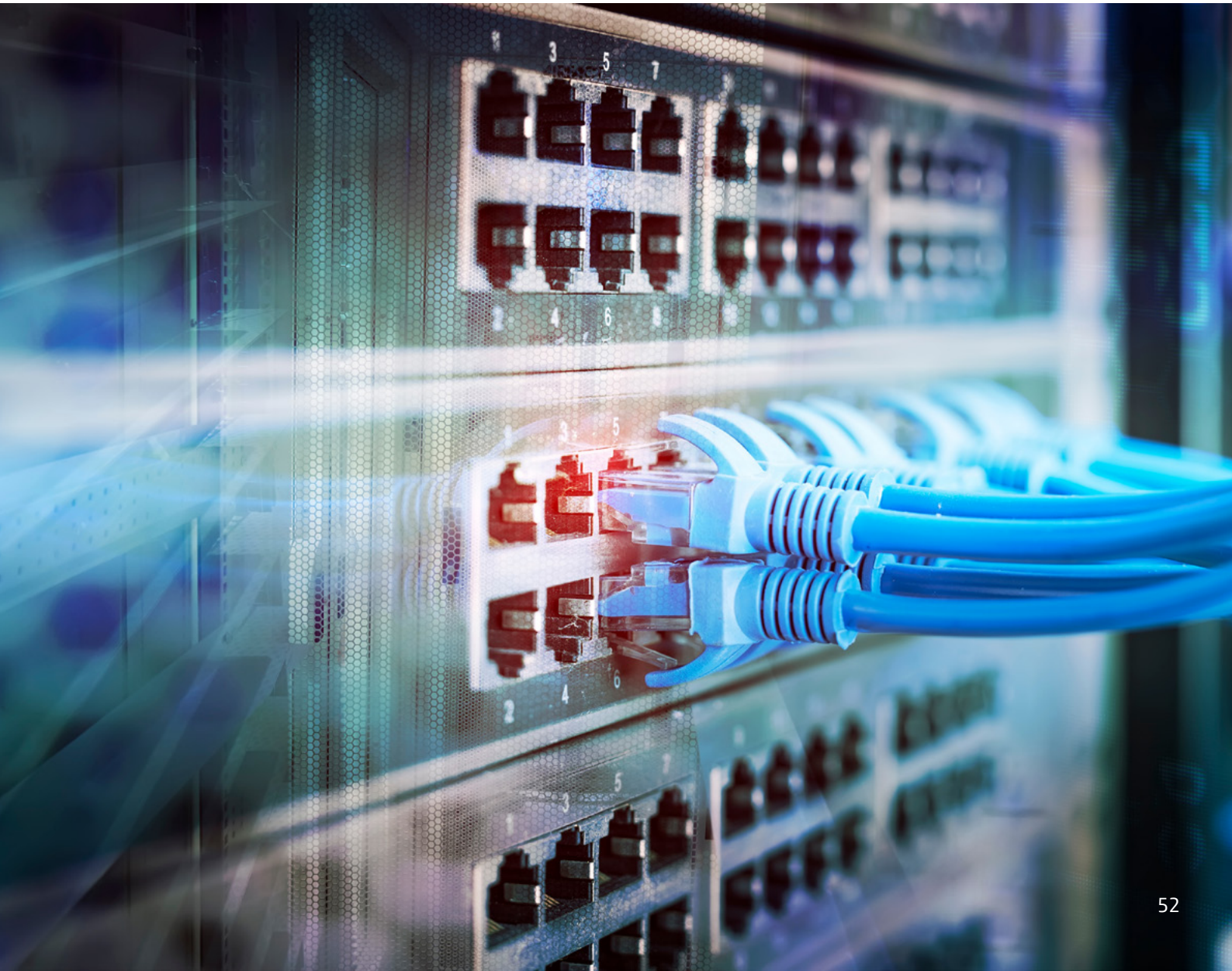
La red de fibra óptica desplegada en España es la más amplia de Europa, con más de 33,3 millones de puntos de acceso, alcanzando a del 75 % de la población, con una cobertura 4G superior al 95 %. El hecho de que España sea el líder europeo en conexiones de fibra y el tercero del mundo le permite soportar el pico de tráfico que experimentan las redes en situaciones de alta

demanda como la planteadas por el coronavirus. Esta resiliencia se debe también a los esfuerzos de los operadores de telecomunicaciones por asegurar la eficiencia, capacidad y flexibilidad de la red.

Lo que el gobierno español y los operadores suelen denominar el "milagro de la fibra española" ha supuesto un esfuerzo inversor sin precedentes en un contexto de contracción del mercado para los operadores desde la última recesión. Desde su liberalización entre 1998 y 2016, el sector de las telecomunicaciones en España ha experimentado una enorme inversión total de 126.600 millones de euros en un período de tiempo relativamente corto. Los operadores de telecomunicaciones del país han instalado cables de fibra óptica que llegan a 31 millones de destinos, más que Francia, Alemania, el Reino Unido e Italia juntos. Según la OCDE, solo Corea del Sur y Japón superan esta cifra.

En términos de banda ultrarrápida, España supera los 10.2 millones de conexiones, de las cuales el 42.6 % son operadas por Telefónica, con 4.3 millones de líneas. Orange tiene 3.1 millones, Vodafone 1.2 millones y MasMovil 1.1 millones, según datos del tercer trimestre de 2019. A finales del año pasado, Vodafone describió el despliegue de 2.9 millones de líneas FTTH y MasMovil 1,3 millones. Además, tanto Vodafone como Orange, empresas británicas y francesas respectivamente, tienen mejores redes en España que en sus países de origen. España es el país con mayor número de líneas de fibra óptica, así como con las de mejor calidad técnica. De hecho, las conexiones españolas llegan a la casa (FTTH), mientras que en otros países solo se conectan con el edificio (FTTB). Por ejemplo, Alemania tiene una penetración de fibras del 2,3 %, de las cuales más de dos tercios solo llegan al exterior del edificio. En España, el 97.2 % de la población tiene acceso a la fibra 4G y la penetración de la fibra es del 74 % de los hogares, en comparación con el 26 % en toda Europa y el 15 % en los Estados Unidos.

Esta capacidad fue puesta a prueba el lunes 16 de marzo, la primera vez que la red fue seriamente desafiada por el uso masivo simultáneo para el entretenimiento y el teletrabajo. En los primeros días posteriores a la declaración del estado de



emergencia, el tráfico de voz móvil, teléfono móvil, aumentó en un 40 % y el de datos fijos en un 70 %. Según datos facilitados por José María Álvarez-Pallete, presidente de Telefónica, en una entrevista, el uso de WhatsApp se multiplicó por seis, Netflix por cuatro y el uso de herramientas de videoconferencia, como Google Hangouts, Zoom, Webex y Facetime, por factores de entre seis y ocho. Telefónica registró un crecimiento del 35 % en el tráfico de Internet en su red fija en el primer mes tras el inicio de la crisis. Esta cifra equivale al crecimiento que normalmente se produce en todo un año. Y la red de telecomunicaciones de Telefónica y el resto de los operadores resistió la prueba.

La experiencia española muestra la importancia de la cooperación pública y privada, el pensamiento estratégico y un marco regulador estable. Ese marco se actualizó en 2014 con la nueva Ley General de Telecomunicaciones y la Agenda Digital Española. Varias decisiones tomadas en medio de una recesión fueron claves en ese momento, y fueron adoptadas tanto por los operadores como por el propio gobierno. Entre ellas cabe citar la priorización y simplificación de las inversiones; la especialización y el reciclaje de los equipos técnicos para desarrollar actividades de planificación y diseño de redes ópticas; la labor de colaboración de las empresas; el lanzamiento de productos convergentes de alta calidad; y un sistema de regulación que facilitara el acceso de los operadores a los conductos, haciendo que la instalación sea más barata y rápida.

La tecnología en la era COVID-19

Los argumentos a favor de una sólida infraestructura de Internet en toda la UE nunca han sido más convincentes que en el contexto de la pandemia del coronavirus. Ha sostenido las florecientes iniciativas tecnológicas que intentan hacer frente a la enfermedad, ya sea deteniendo su propagación, tratando a los pacientes o ayudando a desarrollar vacunas.

En un reciente informe del Parlamento Europeo se han identificado diez tecnologías para ayudar a combatir el coronavirus, que van desde la Inteligencia Artificial (IA) para rastrear la enfermedad; las nanotecnologías para probar las futuras vacunas y tratamientos; la impresión en 3D de equipamiento médico, como ventiladores y mascarillas; y las aplicaciones Blockchain para mantener las cadenas de suministro médico. Como se indica en el informe: "A diferencia de anteriores crisis de salud pública, ésta parece estar transformando a los ciudadanos de objetos de vigilancia y análisis epidemiológico en sujetos de generación de datos mediante el auto-seguimiento, el intercambio de datos y los flujos de datos digitales". De esta manera, las tecnologías han sido capaces de proporcionar soluciones a los problemas clave que presenta la pandemia y, como tales, han desempeñado un papel fundamental en nuestra respuesta de emergencia. De hecho, la capacidad de la UE para responder a las crisis sanitarias y económicas depende en gran medida de su capacidad para aprovechar estas tecnologías.

Sin embargo, cabe señalar el alto costo que está pagando Europa por su atraso digital en comparación con los países asiáticos que han demostrado diligencia y eficacia, especialmente en lo que respecta a los datos de la rastreabilidad y el control digital de las infecciones han sido esenciales para superar y erradicar las epidemias del COVID-19 en China, Singapur, Taiwán y Corea del Sur.

Cada uno de esos países confió en su sólido sector tecnológico y, concretamente, en la ciencia de los datos y otras tecnologías para rastrear y combatir la pandemia, mientras que las principales empresas de tecnología aceleraron sus iniciativas relacionadas con la salud. Así, el desarrollo de la IA y el *big data* hizo que la identificación, el seguimiento y el pronóstico de los brotes fueran más inmediatos. Esto se logró, por ejemplo, a través del análisis de nuevos informes, de plataformas de redes sociales y documentos gubernamentales. Además, la utilización de la capacidad de predicción permitió formular propuestas más eficaces en relación con las drogas existentes que podrían ser útiles. El uso de recursos de computación en el *Cloud* y las supercomputadoras de varias empresas tecnológicas también están acelerando el desarrollo de una cura o vacuna contra el virus. La velocidad con la que estos sistemas pueden ejecutar cálculos y soluciones de modelos es mucho más rápida que el procesamiento informático estándar.

El precio del subdesarrollo digital de Europa y la necesidad de cambios y reformas urgentes en la educación, la legislación, el espíritu empresarial y sus débiles ecosistemas cooperantes es innegable. Además, está también la cuestión de la ineficiencia de los gobiernos para hacer frente a esos desafíos mundiales, que solo ahora comienzan a acordar compromisos ambiciosos en IA, entre otras iniciativas.

Como hemos visto, la tecnología y el análisis de datos son, y seguirán siendo, fundamentales. Debemos apoyar la tecnología y las enormes oportunidades que nos ofrece para anticiparnos a futuras amenazas y tomar las decisiones correctas

para afrontarlas. Debemos compartir la información y hacerlo de una manera ágil y efectiva, y esto ya está a nuestro alcance. Debemos sentar las bases de un sistema *big data* mundial que nos permita enfrentarnos a virus como el COVID-19 con una perspectiva diferente, compartiendo el conocimiento como una sola humanidad.

En este sentido, deberían impulsarse y, de ser posible, desarrollarse más proyectos como GAIA-X, la zona europea de datos, o como las iniciativas de salud *big data*. Lanzado a principios de junio de 2020, GAIA-X es un proyecto de colaboración entre Alemania y Francia que cuenta, con la cooperación de la Comisión Europea y unas 100 empresas y organizaciones para desarrollar un concepto de nube europea. El proyecto está motivado por la noción de "soberanía de los datos" o, más precisamente, de "gobernanza de los datos", y tiene por objeto someter los flujos y el almacenamiento de datos a un mayor control europeo. Refleja el hecho de que no solo se ejecutarán cada vez más procesos de negocio básicos en servicios basados en el *cloud*, sino que todos los principales proveedores de *cloud* son empresas con sede en Estados Unidos y, por lo tanto, están sujetos a la jurisdicción estadounidense. Esto hace que Europa sea vulnerable porque no puede determinar la forma en que se gestionan y regulan los datos.

Aun así, el desarrollo de estos proyectos no estará exento de dificultades: el calendario, los detalles técnicos precisos, la financiación e incluso la gobernanza aún no están claramente definidos. Además, los espacios de datos actualmente disponibles han tenido años de desarrollo a sus espaldas y tienen especificaciones técnicas muy desarrolladas. No obstante, el objetivo final es contar con un ecosistema viable de servicios digitales interconectados que funcionen a la perfección y sean capaces de ofrecer a la industria y a otros sectores de la economía europea una alternativa real y competitiva a los proveedores dominantes de hoy en día.

El increíble salto en el uso de la tecnología en los últimos meses no se detendrá aquí. Como ha sugerido el historiador Yuval Noah Harari, la situación actual la llevará aún más lejos: procesos que antes habrían llevado años o décadas ahora tienen lugar en cuestión de días. Nadie hubiera imaginado hace dos meses que la gran mayoría de los españoles podían pasar a trabajar desde casa de la noche a la mañana. Lo que más importa ahora es que este impulso definitivo, que ha hecho que veamos el sector digital como un pilar de nuestra sociedad y un servicio esencial, vaya acompañado de una estrategia que garantice e impulse los procesos de recuperación en Europa.

Si la digitalización y la innovación fueron cruciales en lo que podríamos denominar la era pre-COVID-19, apoyarlas a través, por ejemplo, la promoción de la formación continua y el desarrollo de las habilidades digitales- es ahora aún más urgente. Las medidas adoptadas y el apoyo prestado por los gobiernos en la actualidad permitirán que el sector tecnológico se consolide como un pilar esencial de la actividad económica, que también será una fuente, directa e indirecta, de ocupación. La tecnología es un aliado silencioso, como se ha demostrado durante la pandemia, y un aliado fundamental en la era post-COVID-19.

Francia y Alemania... ¿en qué están de acuerdo sobre la IA?

Ulrike Franke

Miembro de European Council on Foreign Relations y del proyecto de IA en el Future of Humanity Institute de la Universidad de Oxford.

Cuando se trata de conocer el punto de vista de Europa sobre la IA y tener una idea de hacia dónde se dirige Europa en términos de políticas y capacidades en esta tecnología, una se ve impulsada casi automáticamente a mirar a la Unión Europea. La UE es el lugar de estudio adecuado: publica sus informes en inglés, cuenta con traducciones en muchos otros idiomas, y todos los documentos son fácilmente accesibles. También hay otras buenas razones para mirar hacia la UE cuando se trata de IA ya que la ha situado entre una de sus prioridades, especialmente con la llegada la nueva Comisión Europea bajo el liderazgo de Ursula von der Leyen.

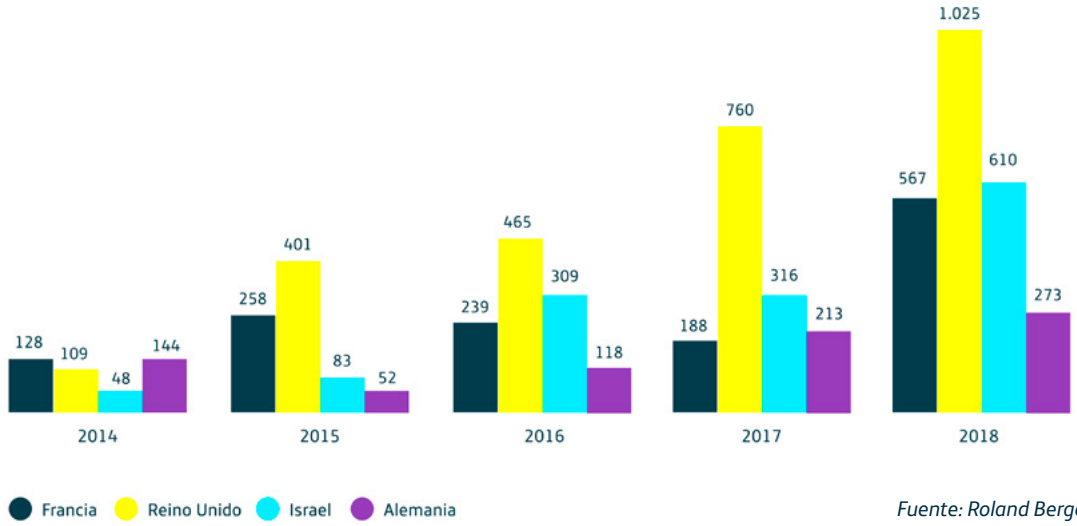
Desde 2018, la UE ha publicado una serie de textos relevantes en el ámbito de las políticas públicas como es el caso de la Declaración sobre la Cooperación en materia de IA, la Comunicación sobre IA y, en especialmente, el Plan Coordinado sobre Inteligencia Artificial de diciembre de 2018 que se presentó como una estrategia inicial de la IA para la UE.

En 2019, el Grupo de Expertos de Alto Nivel de la Unión Europea sobre IA, compuesto por 52 expertos del mundo académico, la sociedad civil y la industria, publicó sus Directrices Éticas para una IA fiable, así como recomendaciones sobre políticas e inversiones. Más recientemente, la Comisión publicó su Libro Blanco sobre IA, llamado "Un enfoque europeo para la excelencia y la confianza". La UE no se queda en las palabras, sino que ha puesto a disposición dinero real para sustentar sus planes de acción. La Comisión tiene como objetivo aumentar la inversión en IA (pública y privada) alcanzando los 20.000 millones de euros al año durante la próxima década, y en 2021 tiene previsto lanzar "Europa digital", un programa centrado en la creación de capacidades digitales estratégicas de la UE, que también incluye miles de millones para la IA y supercomputadoras.

Dada la prioridad que la UE da a este asunto, sumado a la relevancia de la regulación y las cuestiones comerciales, así como sus propias pretensiones de representar "el enfoque europeo", parece lógico centrarse en la UE como un actor principal para conocer la postura de Europa sobre la IA y sus planes futuros. Sin embargo, cualquier análisis o reflexión sobre IA debe complementarse con el parecer de los Estados miembros.

Hay varias razones por las que no podemos limitarnos a un enfoque único desde la UE. En primer lugar, porque la UE cuenta con competencias exclusivas solo en ámbitos contados, como es el caso del comercio. En otros, por el contrario, solo puede actuar cuando los Estados miembros delegan capacidad de actuación o cuando acuerdan las orientaciones políticas. En segundo lugar, hay campos en los que, hasta ahora, la UE no juega un papel directo. Este es el caso de la IA en el ámbito militar. Aunque en los últimos años, y tras la partida del Reino Unido, la UE ha comenzado a reforzar su papel en el sector de la defensa, por ejemplo, mediante la creación de la Cooperación Permanente Estructurada (PESCO) y el Fondo Europeo de Defensa, los Estados miembros siguen siendo, de lejos, los actores más importantes en materia de

Recaudación de fondos dedicados a la IA (millones de dólares)



Fuente: Roland Berger

defensa. Además, incluso en los campos en los que la UE tiene competencias claras, los puntos de vista de los Estados miembros siguen siendo importantes ya que influyen en las políticas de la UE. Por último, incluso para los que se focalizan exclusivamente en los planes y acciones de la UE, es importante tener en cuenta las políticas llevadas a cabo por los Estados miembros.

Actualmente a escala global, tanto los gobiernos como los expertos están tratando de entender las implicaciones tecnológicas, (geo)políticas, económicas y sociales de la IA. Esto significa que estamos en una fase de constante evolución, sujeta al desarrollo de ideas, que se discuten y se rechazan o modifican. Lo mismo ocurre con la UE y sus Estados miembros, cuyas ideas, planes y estrategias probablemente se ajusten y cambien con el tiempo y, lo que es más importante, su desarrollo está sujeto a la interacción con los demás.

La UE es consciente de sus limitaciones y de la necesidad de interactuar con los Estados miembros, por lo que en el Plan Coordinado se ha pedido a todos ellos que pongan en marcha estrategias nacionales de IA. En mayo de 2020, al menos 18 de los 27 estados miembros de la UE han seguido este consejo y han publicado estrategias nacionales, proyectos de programas o documentos similares, a saber, Alemania, Austria, Bélgica, Dinamarca, España, Estonia, Francia, Finlandia, Italia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, República Checa, Suecia y el Reino Unido. Además, hay programas y planes regionales, como la Declaración sobre la IA en la región nórdica y báltica, y las ideas del Grupo de Visegrad sobre la IA. Otros han creado grupos de expertos y están redactando sus estrategias nacionales.

¿Existe la voluntad de trabajar juntos en un enfoque común europeo sobre la IA?

Si la UE quiere desempeñar un papel de coordinación y, en última instancia, aglutinar los planes de sus Estados miembros sobre la IA de manera consolidada, es necesario que haya un acuerdo sobre el hecho de que, en lugar de perseguir prioridades nacionales por separado, la cooperación en esta materia es beneficiosa para todos. En este sentido, la Declaración de Cooperación en materia de IA de abril de 2018 fue un buen comienzo. Con este documento, los Estados miembros de la UE se comprometieron a colaborar entre sí para abordar las cuestiones sociales, económicas, jurídicas y éticas relacionadas con la IA, así como para garantizar que la UE sea competitiva en esta materia. El Plan Coordinado de la UE, que tenía por objeto establecer la UE como entidad coordinadora, también fue útil ya que alentó a los Estados miembros a elaborar sus propias estrategias de IA. Por otro lado, el hecho de que algunos ya hubieran publicado sus estrategias nacionales para cuando se publicó el Plan Coordinado de la UE ha podido limitar su impacto.

Observando las decisiones de los "dos grandes" países europeos, Francia y Alemania, se constata que no es un asunto sencillo decidir cuándo ir por cuenta propia, cuándo colaborar con socios seleccionados y cuándo delegar el poder a la UE. En sus estrategias nacionales de IA, los dos países apoyan la cooperación bilateral o multilateral y

la adopción simultánea de objetivos nacionales y europeos. Sus motivaciones declaradas para hacerlo, sin embargo, difieren. En el caso alemán, el enfoque en la cooperación europea, específicamente franco-alemana, parece ser un objetivo en sí mismo, o la idea por defecto. La estrategia francesa, en cambio, adopta un enfoque más pragmático, apoyando la cooperación europea solo en los ámbitos en que los autores de la estrategia la consideran útil.

El subtítulo de la estrategia francesa es "Hacia una estrategia francesa y europea" incluye ya el ángulo europeo desde su propio enunciado. El prólogo de la estrategia señala además que "no podemos concebir la IA en un marco puramente nacional". Aquí hay razón específica que tiene que ver con el interés de Francia en la UE en tanto que actor relevante: las preocupaciones geopolíticas en torno a la IA. El documento señala que "Francia y Europa deben asegurarse de que sus voces sean escuchadas y deben hacer todo lo posible por permanecer independientes. Pero hay mucha competencia: Estados Unidos y China están a la vanguardia de esta tecnología y sus inversiones superan con creces las realizadas en Europa". A los autores de la estrategia les preocupa que "Francia y Europa ya pueden ser consideradas como 'cibercolonias' en muchos aspectos". Sobre la base de esta perspectiva geopolítica Francia impulsa un enfoque europeo en lugar de una exclusivamente nacional. Sin embargo, si bien el enfoque francés considera útil la cooperación europea en materia de IA, se centra en la colaboración bilateral franco-alemana.

La estrategia francesa aborda la cooperación europea de manera práctica, identificando los ámbitos que considera "especialmente adecuados para la integración en un esquema europeo", como el transporte y la movilidad. La estrategia añade, sin embargo, que "los demás sectores prioritarios (salud, defensa y medio ambiente) no se prestan tan fácilmente a un tratamiento directo a escala europea, aunque sería útil que Alemania se involucrara". A su vez considera a Alemania el socio principal de Francia en repetidas ocasiones. Por ejemplo, afirma que, "para comenzar el desarrollo de una política industrial europea en IA, nuestra misión recomienda que, inicialmente, se trabaje dentro de un eje franco-alemán". Posteriormente incluye a otro gran jugador europeo, diciendo a continuación: "Italia (el norte en

particular) también debe ser visto como un posible socio serio, sobre todo por sus avances en el campo de la robótica", un campo en el que llega a hablar de un "tríptico franco-alemán-italiano".

El subtítulo de la estrategia alemana es "IA made in Germany", pero esto no se traduce en un enfoque nacionalista. De hecho, la estrategia alemana tiene un claro enfoque europeo, particularmente franco-alemán. Los términos "europeo", "UE" y "Europa" se mencionan alrededor de 90 veces, y el objetivo declarado es hacer que Alemania y Europa sean líderes mundiales en la IA. Reflejando el enfoque de Francia en el eje franco-alemán, la estrategia alemana menciona a Francia más a menudo que a cualquier otro país. Tiene previsto construir un "centro virtual" de institutos de investigación e innovación con Francia. Alemania también quiere trabajar en IA con el Consejo Francés de Innovación. Mientras que la motivación francesa para colaborar a escala europea se basa claramente en las preocupaciones sobre el poder geopolítico de Europa y su capacidad para hacer frente a otros actores, en particular EE.UU. y China, este enfoque está en gran medida ausente en el pensamiento alemán sobre la IA. De hecho, para Alemania, trabajar con socios europeos en IA parece estar más impulsado por una convicción general de que es lo correcto, más que por una consideración específica. Curiosamente, el punto de vista geopolítico tan prominente en el pensamiento francés está ausente en la visión alemana.

Francia y Alemania, ¿cuánto están de acuerdo?

Dado el papel crucial que Francia y Alemania desempeñan en la política europea, y dado el poder económico de los Estados, así como la experiencia y el talento en IA y campos relacionados, vale la pena examinar los enfoques de ambos países sobre la IA. Aunque hay que ser cauteloso a la hora de hacer declaraciones definitivas debido a la mencionada naturaleza provisional de las políticas y el pensamiento sobre la IA en este momento, también hay que señalar que hay diferencias significativas en cuanto a la forma en que Francia y Alemania se acercan a la IA. Si estas diferencias persisten o se profundizan, esto podría causar problemas para un enfoque común europeo.

Francia ha mostrado mucho interés en la IA desde el principio. La IA se convirtió en una prioridad de primer nivel, y el presidente Emmanuel Macron debatió ampliamente del tema en una entrevista online a principios de 2018, justo cuando Francia estaba lanzando su estrategia sobre la cuestión. El ecosistema de IA de Francia es muy dinámico; un estudio realizado por Roland Berger identificó Francia estaba a la cabeza en inversión (extranjera) dentro de la UE. Alemania, de acuerdo con el mismo estudio, iba justo detrás. En cuanto a las políticas públicas, sin embargo, Alemania, pese a ser inicialmente lenta en abordar los problemas de la IA, posteriormente aceleró sus propuestas a partir del segundo semestre de 2018. Se creó una comisión de investigación y en noviembre de 2018 publicó la estrategia nacional sobre la materia, que se complementó con audiencias públicas y de expertos y otros eventos.

La primera diferencia importante entre los enfoques francés y alemán es la lente a través de la cual los países ven la IA. Mientras que Francia, como se mencionó anteriormente, considera la IA un elemento importante de la geopolítica, y está preocupada por la posición de Francia y Europa en el mundo debido a los desarrollos de la IA, la estrategia alemana adopta una lente económica. Dado que la estrategia alemana se redactó bajo la dirección de los ministerios de educación e investigación, economía y energía, y trabajo y asuntos sociales, se centra principalmente en la investigación, la economía y la sociedad. Se concentra en la preservación de la fuerza de la industria alemana, en particular de las pequeñas y medianas empresas, el famoso *Mittelstand* alemán, buscando asegurar que la IA no permita que otros países superen económicamente a Alemania. La esperanza del gobierno es que la IA ayude al *Mittelstand* a seguir fabricando productos líderes en el mundo. Así pues, el enfoque alemán sobre la IA está marcado por el temor a perder oportunidades económicas, lo que hace que adopte un tono defensivo. Una encuesta realizada en 2018 reveló que el 69 % de los alemanes cree que, debido a la IA, se perderá un "número masivo de puestos de trabajo" (creencia que prevalece especialmente entre los jóvenes de 16 a 24 años), mientras que al 74 % le preocupa que "cuando las máquinas decidan, se perderá el elemento humano".

El contraste de tono es otra diferencia interesante entre los dos países. Cuando la estrategia alemana expresa la preocupación de que la IA pueda llevar a una pérdida de poder económico, la estrategia francesa adopta un tono más optimista, describiendo la inteligencia artificial como "uno de los esfuerzos científicos más fascinantes de nuestro tiempo". Cedric Villani, el matemático francés que dirigió el grupo que redactó la estrategia, expresa en su prólogo la convicción de que "Francia y Europa, en su conjunto, deben actuar de forma sinérgica, con confianza y determinación, para formar parte de la emergente revolución de la IA". Este enfoque parece estar de acuerdo con las creencias de los ciudadanos franceses: una reciente encuesta de la IFOP reveló que el 73 % de ellos tienen una opinión positiva o muy positiva de la IA.

Un último campo en el que las diferencias franco-alemanas parecen actualmente más pronunciadas, es en el papel que la IA podría desempeñar en el

ámbito militar y de defensa. Francia considera que el ámbito militar es un elemento importante de sus esfuerzos de desarrollo de la IA. La estrategia francesa designa la defensa y la seguridad como uno de sus cuatro sectores de IA prioritarios para la política industrial (uno de los autores de la estrategia es un ingeniero de la agencia francesa de adquisición de defensa). El Ministerio de Defensa francés también anunció inversiones en la investigación de IA. En particular, Francia, en septiembre de 2019, se convirtió en el primer país europeo en publicar una estrategia militar de IA, un informe escrito por un equipo del Ministerio de Defensa, con expertos externos. El documento esboza el enfoque de Francia sobre la IA en el ejército, proporciona ejemplos de aplicaciones militares habilitadas por la IA y anuncia la creación de varios organismos que ayudarán a los militares franceses a adoptar la IA. La estrategia militar de la IA sigue las ideas de la estrategia nacional de la IA de Francia, adoptando un enfoque geopolítico similar. Describe a los EE.UU. y China como "superpotencias" de la IA, y a Europa como "una potencia intermedia en ciernes". Francia, junto con Alemania, Canadá, Israel, Japón, Singapur, Corea del Sur y el Reino Unido, forman parte del "segundo círculo", en IA. El documento expresa repetidamente la preocupación por la dependencia de otros países (en particular de las empresas privadas de otros Estados) y adopta la "preservación de un corazón de soberanía" como uno de sus principios rectores.

Los elementos militares, de seguridad y geopolíticos de la IA están notablemente ausentes de la estrategia nacional alemana. De hecho, la estrategia solo incluye una frase sobre seguridad y defensa, lo que traslada la responsabilidad de esta área al Ministerio de Defensa. La estrategia dice: "En lo que respecta a los nuevos escenarios de amenaza para la seguridad interna y externa, además de la investigación sobre la seguridad civil, el Gobierno Federal promoverá la investigación para detectar el contenido manipulado o generado automáticamente en el contexto de la seguridad cibernética. La investigación sobre las aplicaciones de la IA, en particular para la protección de la seguridad exterior y con fines militares, se llevará a cabo en el ámbito de las responsabilidades del ministerio". Lamentablemente, parece poco probable que el Ministerio de Defensa de Alemania siga el ejemplo de Francia y publique una estrategia militar dedicada a la IA, en la que se esbozan sus opiniones sobre esta tecnología en el ámbito militar. Más bien, la estrategia nacional parece representativa del enfoque generalmente cauteloso de Alemania respecto a la vertiente militar. Un informe para la asamblea parlamentaria de la OTAN sostiene que, dado el valor potencial de la IA para las fuerzas armadas, los líderes de la OTAN en ciencia y tecnología, como Francia, Alemania, el Reino Unido y los Estados Unidos, deben invertir en investigación y desarrollo de la IA relacionada con la defensa. Pero el informe señala a Alemania como rezagada en este campo, comentando: "es alentador ver que todos ellos están invirtiendo recursos sustanciales en la IA relacionada con la defensa, con la posible excepción de Alemania". Hasta ahora, el debate público y político sobre la IA en el ejército en Alemania se centra principalmente en los sistemas de armas autónomas y en los esfuerzos para controlarlas. El Ministerio de Relaciones Exteriores organizó una conferencia internacional sobre el tema en marzo de 2019 y ha celebrado una serie de reuniones de seguimiento.

La referencia de la estrategia nacional sobre la IA a las "responsabilidades ministeriales" podría interpretarse como un mandato para que el Ministerio de Defensa alemán desarrolle su propia estrategia sobre las aplicaciones militares de la IA. Sin embargo, dado el historial del Ministerio de Defensa de publicar raramente, o nunca, documentos doctrinales, es poco probable que el ministerio lo haga públicamente. Dicho esto, en octubre de 2019, la unidad del ejército encargada de desarrollar nuevos conceptos e ideas para las fuerzas terrestres sorprendió a la mayoría de los expertos al publicar un documento de posición titulado "Inteligencia artificial en las fuerzas terrestres". Sin embargo, el documento está algo desconectado de otras publicaciones alemanas, y no tiene un impacto directo en las acciones del gobierno alemán o del Ministerio de Defensa. En efecto, y como dijo uno de los autores del documento en una conversación privada, el Ministerio de Defensa no estaba particularmente satisfecho con su publicación. No está claro qué será de los conceptos desarrollados en el documento de posición.

Por lo tanto, mientras que Francia considera las aplicaciones militares un elemento importante de la IA, Alemania, por el momento, rehúye el tema. Es probable que esto dificulte la coordinación futura sobre el tema. Esto es particularmente digno de mención y preocupante dados los dos proyectos militares de gran envergadura que Francia y Alemania están desarrollando conjuntamente: el Futuro Sistema Aéreo de Combate (FCAS), y el Sistema Principal de Combate Terrestre.

IA ética: ¿el camino a seguir para Europa?

Si bien hay diferencias notables en la forma en que Francia y Alemania abordan la cuestión de la IA, como se ha señalado anteriormente, también hay muchos campos en los que ambos países (y otros de Europa) están de acuerdo. Este es el caso más notable con respecto a la "IA ética". La UE ha expresado su ambición de convertirse en "la región líder en el mundo en el desarrollo y despliegue

de tecnologías de vanguardia, IA ética y segura". La UE persigue dos objetivos centrándose en la ética. En primer lugar, sigue el análisis de muchos expertos que han señalado la importancia de incluir consideraciones éticas en el desarrollo y la aplicación de la IA. La UE espera no solo establecer normas para sus propios ciudadanos y empresas, sino también, a través de su alcance normativo mundial (denominado "efecto Bruselas"), influir en los actores extranjeros para que sigan el ejemplo europeo. En segundo lugar, y algo más rebatido, la Comisión Europea espera que este enfoque en la IA ética pueda a largo plazo dar a las empresas europeas una ventaja. El Plan Coordinado establece que, para la UE, "encabezar la agenda de la ética, a la vez que se fomenta la innovación, tiene el potencial de convertirse en una ventaja competitiva para las empresas europeas en el mercado mundial". La idea es que a medida que más consumidores se den cuenta de la importancia de la privacidad de los datos, y de la conducta ética, las empresas europeas que siguen las normas de la IA ética estarán en ventaja.

Tanto para Francia como para Alemania, la idea de una IA ética y digna de confianza tiene mucho atractivo. El gobierno alemán ve los "requisitos éticos y legales" como una parte integral y una futura "marca", de la IA made in Germany. La estrategia establece tres objetivos principales, el tercero de los cuales es "integrar la IA en la sociedad en términos éticos, jurídicos, culturales e institucionales en el contexto de un amplio diálogo social y de medidas políticas activas". La estrategia menciona específicamente la cooperación europea en este punto: "Una mayor cooperación dentro de Europa, pero también a nivel internacional, es esencial para muchos desafíos para [...] un uso de la IA centrado en el ser humano, especialmente cuando se trata de normas uniformes y éticamente exigentes para el uso de las tecnologías de la IA en Europa". La ética es también el ámbito de debate con respecto a la IA militar con el que Alemania se siente más cómoda, lo que puede suponer una apertura para las deliberaciones europeas sobre la IA militar. La estrategia francesa también tiene una sección sobre la ética de la IA, en la que se recomienda "aplicar la ética por diseño", es decir, durante el proceso de desarrollo, ya que "no puede integrarse a posteriori". La estrategia señala la importancia de la transparencia, la inclusión y la diversidad. Relacionada con la ética está la importancia de la privacidad de los datos, que desempeña igualmente un papel crucial tanto para Francia como para Alemania. Además, en cuanto a la ética, Europa también puede considerar la posibilidad de colaborar con el Reino Unido, que ha mostrado mucho interés en la IA ética.

Como las políticas de IA en todo el mundo se están elaborando y están en proceso de cambio, y dado que Europa está compuesta por 27 Estados miembros de la UE, por las propias instituciones de la organización regional y muchos otros países europeos no pertenecientes a la UE, es imposible definir "el enfoque europeo de la Sin embargo, este análisis del pensamiento actual de la UE, Francia y Alemania demuestra que existen diferencias interesantes y notables en la forma en que los actores se acercan a la IA. Se necesita una mayor coordinación, tanto bilateral como a nivel europeo, para suavizar, en lugar de profundizar, estas diferencias.

Nota del proyecto: En busca de la soberanía digital de Europa

Carla Hobbs

Coordinadora del Proyecto Europes's Digital Power, ECFR.

En los últimos cinco años, Europa se ha convertido en un pionero mundial en la formulación de políticas digitales, para la admiración y la exasperación de muchos. Abandonando su anterior actitud de laissez-faire respecto de la regulación tecnológica en favor de un enfoque asertivo, la Unión Europea ha intervenido activamente para elevar las normas de privacidad, imponer a las empresas tecnológicas multas antimonopolio y configurar el debate sobre cuestiones como los perjuicios en línea y la inteligencia artificial ética. Y por lo que parece, solo está empezando.

Este cambio tuvo lugar bajo la comisión Juncker en medio de la creciente toma de conciencia de que Europa tenía que proteger sus valores, intereses y ciudadanos en un espacio digital que se estaba convirtiendo gradualmente en un campo de batalla geopolítico y geoeconómico. Al carecer de las credenciales tecnológicas para competir con China y los Estados Unidos como actor digital, la UE comenzó en cambio a dar forma al ecosistema digital ejerciendo su poder de regulación para introducir normas extraterritoriales que obligaran a todos aquellos que deseen interactuar con su mercado único y sus consumidores. Como dijo el Comisario del Mercado Interior de la UE, Thierry Breton, "no somos nosotros los que tenemos que adaptarnos a las plataformas actuales. Son las plataformas las que necesitan adaptarse a Europa".

El resultado es que hoy en día la UE es la principal potencia reguladora digital del mundo. Pero ¿es el poder regulador suficiente para proteger los intereses y la visión de Europa sobre Internet y las tecnologías digitales? Si es así, ¿qué viene después del hito del Reglamento General de Protección de Datos de 2016? ¿Cómo podemos asegurarnos de que la regulación no perjudique la esencia y los valores fundacionales de Internet, o la haga menos atractiva, rentable o útil? ¿Debe la UE seguir trabajando unilateralmente en cuestiones digitales o hay posibilidades de alianzas transatlánticas o de otro tipo?

Con estas preguntas en mente ECFR lanzó el proyecto "Europes's Digital Power" en colaboración con Telefónica en 2019. Esta colección de ensayos forma una parte importante de ese proyecto. El equipo se puso en marcha, viajando a Londres en mayo de 2019, a Berlín en septiembre, a Washington, DC en octubre y virtualmente a Bruselas en junio de 2020 para presentarlo a más de cien responsables políticos, reguladores, representantes de los gigantes de la tecnología, académicos y otros actores relevantes en una serie de talleres.

De estos debates surgieron varios mensajes y recomendaciones clave. En cuanto a la cuestión de la regulación propiamente dicha, si bien hubo una importante divergencia de opiniones sobre la escala y los métodos que debían emplearse, la mayoría de los participantes coincidieron en que era necesario que los gobiernos intervinieran para mitigar los efectos perjudiciales de Internet. La regulación debe ser ágil y flexible, desarrollada a través de un proceso iterativo que refleje el dinamismo de la industria que se pretende configurar. La regulación también debe ser proporcional y matizada, con el fin de crear un sistema más seguro en general, en el que la libertad de expresión y la innovación todavía puedan florecer.

Para lograrlo, Europa necesitará responsables políticos y jueces informados y con recursos suficientes que puedan hacer frente a la escala, la complejidad y los problemas jurisdiccionales que plantea la regulación de Internet. Aquí, la comunidad tecnológica tiene un

importante papel que desempeñar para educarlos y compartir datos esenciales para reducir las asimetrías de información. Esto se relaciona con la cuestión de la co-gobernabilidad de Internet entre los sectores público y privado, que los interlocutores acordaron que será esencial para avanzar, dado que las empresas que poseen gran parte de la infraestructura digital del mundo están en mejores condiciones de hacer cumplir las normas, mientras que los reguladores pueden decidir mejor cuáles deben ser esas normas y límites. Así pues, de los debates de los talleres surgió una preferencia constante por el enfoque "*multistakeholder*" en la regulación de Internet. Sin embargo, también se reconoció que el modelo necesita mejoras significativas si se quiere que sea un instrumento eficaz de formulación y aplicación de políticas, habida cuenta de su funcionamiento lento y difuso y de la falta de incentivos para la rendición de cuentas.

En cuanto al panorama geopolítico más amplio, los participantes estadounidenses instaron a sus homólogos europeos a que se resistieran a considerar a los Estados Unidos y la Unión Europea como puntos equidistantes en un triángulo con China. En cambio, sostienen, se trata de dos aliados que comparten más similitudes que diferencias, como el apoyo a los valores de la sociedad abierta online. Esto podría proporcionar un terreno fértil sobre el que desarrollar una posición transatlántica común. Esta posición común tendría entonces una influencia significativa en la definición de las normas que rigen el ecosistema digital y la dirección que pueden tomar los actores fundamentales, como la India.

Por último, hubo un consenso abrumador sobre un punto: Europa debe pasar de ser una superpotencia reguladora a una superpotencia tecnológica si espera salvaguardar verdaderamente sus valores e intereses en el espacio digital, cosechar los beneficios económicos de las tecnologías digitales emergentes y mantener a los europeos a salvo de la desinformación y los ataques cibernéticos. Hasta ahora, Europa ha estado más preocupada por escribir las reglas del juego que por jugarlo, y el bloque sigue a la zaga de China y Estados Unidos en el desarrollo de soluciones y compañías tecnológicas líderes. Pero como un participante señaló, "los árbitros no ganan". La UE debe complementar su peso regulador con inversiones en infraestructura digital, habilidades e industria para convertirse en un actor digital por derecho propio.

Si quedaban dudas sobre este último punto, el inicio de la pandemia del coronavirus en Europa las ha resuelto, dando el salto hacia un nuevo nivel de conciencia en las sociedades, los gobiernos y las empresas acerca de la importancia crítica de las tecnologías digitales para la resiliencia económica y sanitaria de Europa. La completa dependencia de los europeos de la tecnología no solo para sostener la economía, ya que millones de personas trabajaban desde sus casas durante el confinamiento, sino también para combatir el propio virus, hizo que de la noche a la mañana la transformación digital de Europa se convirtiera en una cuestión de importancia existencial. El aumento de las tensiones y la disociación digital entre China y los Estados Unidos durante la pandemia añadieron un elemento adicional de urgencia, ya que Europa ya no puede simplemente esperar, sino que se ve obligada a elegir un carril o definir el suyo propio. Esto no quiere decir que la transformación digital de Europa no fuera una prioridad antes de la pandemia. De hecho, "Preparar a Europa para la era digital" ocupaba el tercer lugar en la lista de objetivos de la Comisión Europea para 2019-2024, una prioridad que se puso de manifiesto en una serie de iniciativas legislativas sobre la inteligencia artificial, datos y otros campos, todos ellos publicadas apenas un mes antes de que se iniciaran los confinamientos en Europa. De hecho, los funcionarios de la UE se apresuraron a señalar durante el taller de Bruselas que la experiencia de la pandemia había validado la agenda de política digital de la UE y que fortalecería el argumento a favor de un aumento de los recursos financieros para respaldarla.

Sin embargo, mientras que el motivo, el dinero y la mentalidad pueden estar ahí, eso deja el método, que no es de ninguna manera la parte fácil. Los participantes en el debate de Bruselas sostuvieron que Europa podría haberse perdido la primera generación de transformación digital, pero podría posicionarse para competir en la próxima ola de tecnología, como el Edge Computing, en el que las empresas europeas tienen varias ventajas competitivas. La UE también puede seguir configurando el entorno digital ejerciendo su poder regulador mediante, por ejemplo, la creación de una federación europea de nubes que exija a quienes soliciten la admisión que se adhieran a las normas de la UE. Por último, también puede exportar su modelo a democracias afines de todo el mundo y construir una alianza con ellas para aumentar el apoyo a la misma.

Es innegable que los retos son muchos, desde la desunión de los Estados miembros en cuestiones de tecnología hasta el infeliz matrimonio entre el enfoque de "las reglas primero" de Europa y su apuesta por impulsar las soluciones tecnológicas y la innovación de cosecha propia. Pero lo que se había hecho evidente al final del proyecto era que Europa estaba decidida a superar estos desafíos, su resistencia digital y su soberanía ya no era una cuestión de "si" y "cuándo" sino de "cómo" y "ahora".

Fue en este contexto que nació esta colección de ensayos. ECFR invitó a determinados interesados que habían participado en los cuatro cursos prácticos a que compartieran sus ideas sobre la forma en que la UE puede mejorar su soberanía digital en un contexto posterior a la aparición del coronavirus en campos que van desde el 5G hasta la banda ancha, y desde la computación en nube hasta la desinformación.

Espero que las recomendaciones resulten útiles para los lectores y que el mensaje central de la colección inspire a los encargados de la formulación de políticas, las empresas y la sociedad civil por igual. Europa tiene una oportunidad única de impulsar su transformación digital y lograr una mayor independencia y resistencia tecnológica. No puede permitirse el lujo de perdérsela.

Sobre los autores

Esta colección de ensayos forma parte del proyecto “Europe's Digital Power”. Se publicó originalmente en julio de 2020 como resultado de la colaboración entre el European Council on Foreign Relations (ECFR) y Telefónica que comenzó con la celebración de una serie de talleres en Londres, Berlín, Washington, Bruselas y Madrid. Cada taller reunió a expertos y destacados profesionales del sector privado y público, la academia, empresas tecnológicas y la sociedad civil para compartir sus puntos de vista sobre cómo Europa puede convertirse en un actor relevante en el ámbito digital y salvaguardar sus valores e intereses en este espacio. Estos debates fueron el origen de la presente publicación que reúne a investigadores y personalidades relevantes en el debate que nos ocupa.

José María Álvarez-Pallete

es el Presidente Ejecutivo de Telefónica S.A., cargo que ocupa desde 2016. Se incorporó al Grupo Telefónica en 1999 y pasó a ocupar varios puestos como Director General Financiero de Telefónica Internacional, y más tarde ese mismo año se convirtió en Director Financiero de Telefónica S.A. En 2002 fue nombrado Presidente Ejecutivo de Telefónica Internacional. Entre 2006 y 2011 fue Director General de Telefónica Latinoamérica. Fue nombrado Presidente Ejecutivo de Telefónica Europa en 2011, y fue nombrado Director de Operaciones de Telefónica, S.A. en 2012. Es licenciado en Ciencias Económicas por la Universidad Complutense de Madrid, estudió Ciencias Económicas en la Universidad Libre de Bruselas, y posee un Programa de Gestión Internacional del IPADE.

Anthony Giddens

es miembro vitalicio del King's College de Cambridge y profesor emérito de la London School of Economics. Fue Director de la LSE de 1997 a 2003 y fue nombrado miembro de la Cámara de los Lores en 2004. Lord Giddens tiene títulos honoríficos o premios comparables de más de 20 universidades. Cofundó la editorial Polity Press, que hoy en día produce 150 títulos al año. Giddens es un miembro del Consejo de la ECFR.

Jeremy Shapiro

es el Director de Investigación del European Council on Foreign Relations. Anteriormente, fue miembro de Brookings Institute en Washington, DC. Antes de Brookings, fue Miembro de la Unidad de Planificación de Políticas del Departamento de Estado de EE.UU. y asesor principal del Subsecretario de Asuntos Europeos y Euroasiáticos en Estados Unidos.

Andrew Puddephatt OBE

es el Presidente Ejecutivo de la Junta Consultiva de Global Partners Digital, una empresa que promueve la democracia y los derechos humanos online, y Presidente de Internet Watch Foundation, una organización ánimo de lucro que protege a los niños online. También preside el International Media Support, con sede en Dinamarca, y es Vicepresidente del Sigrid Rausing Trust. Anteriormente, Puddephatt fue el Director Ejecutivo del ARTÍCULO 19 entre otros cargos. Ha sido miembro experto del Consejo de Europa y de los grupos de trabajo de expertos del Commonwealth sobre libertad de información y libertad de expresión, y es asesor de la UNESCO sobre políticas de medios de comunicación e Internet. Es miembro del Consejo de la ECFR.

Janka Oertel

es la Directora del Programa de Asia del European Council on Foreign Relations. Anteriormente trabajó como becaria superior en el programa para Asia del Fondo Marshall Alemán de la oficina de Berlín de los Estados Unidos, donde se centró en la política transatlántica de China, incluidas las tecnologías emergentes, la política exterior china y la seguridad en Asia oriental. Antes de unirse a la GMF, fue Directora de Programas en la oficina de Berlín de la Fundación Korber. Tiene un doctorado de la Universidad de Jena.

Andrés Ortega Klein

es investigador principal del Real Instituto Elcano, consultor independiente y Director del Observatorio de las Ideas. Fue Director del Departamento de Análisis y Estudios de la Presidencia del Consejo de Ministros de España en dos ocasiones y también trabajó como asesor en el Ministerio de Asuntos Exteriores y Cooperación. Ha desarrollado una extensa carrera en el periodismo como corresponsal en Londres y Bruselas, y como columnista y redactor de El País. Ortega Klein es licenciado en Ciencias Políticas por la Universidad Complutense de Madrid y tiene una Maestría en Ciencias Económicas en Relaciones Internacionales en la Escuela de Economía de Londres. Es miembro del Consejo de la ECFR.

Frances G Burwell

es una miembro distinguida del Atlantic Council y Directora principal de McLarty Associates. Hasta enero de 2017, fue vicepresidenta de la Unión Europea e Iniciativas Especiales en el Consejo. Ha sido Directora del Programa de Relaciones Transatlánticas del Consejo Atlántico y Directora interina del Programa de Economía y Negocios Globales, y actualmente dirige la Iniciativa del Mercado Digital Transatlántico. Su trabajo se centra en la Unión Europea y en las relaciones entre los Estados Unidos y la UE, así como en otras materias de carácter económico, político y de defensa transatlánticas.

Andrea Renda

es investigador y Director de gobernanza mundial, regulación, innovación y economía digital (GRID) del Center for European Studies (CEPS). En la actualidad es investigador principal no residente en el Instituto de Ética de la Universidad de Duke, y fue profesor adjunto de Derecho y Economía en la Facultad de Derecho de Duke (Estados Unidos) durante el año académico 2016/2017. Desde septiembre de 2017, ocupa la “Cátedra Google” de Innovación Digital en el Colegio de Europa en Brujas (Bélgica). Es miembro del Grupo de Expertos de Alto Nivel de la UE sobre la Inteligencia Artificial.

José Ignacio Torreblanca

es un investigar en políticas públicas y Director de la oficina de Madrid del European Council on Foreign Relations y Profesor de Ciencias Políticas en la Universidad Nacional de Educación a Distancia (UNED). También es columnista semanal en EL MUNDO como autor del blog "Café Steiner" y colaborador de RNE. Anteriormente, fue Jefe de Opinión del diario EL PAÍS (2016-2018) y antes de eso, fue el primer director de la Oficina de Madrid de la ECFR (2007-2016) tras el lanzamiento de la ECFR en toda Europa. Torreblanca es Doctor en Ciencias Políticas por la Universidad Complutense de Madrid (UCM).

Alicia Richart

es la fundadora y Directora General de DigitalES, una asociación sin ánimo de lucro, que tiene como objetivo promover la transformación digital de España. Antes de esto, Richart trabajó en el gabinete del Ministro de Industria, Energía y Turismo de España como asesora donde dirigió el programa Industria 4.0 y la actualización de la Ley General de Telecomunicaciones (2014). De 2012 a 2014, Richart fue la Campeona Digital Española, nombrada por la Comisión Europea. Es ingeniera industrial, graduada en el Instituto Químico de Sarrià (1999), y tiene un MBA de la Escuela de Negocios ESADE (2005).

Ulrike Franke

es experta investigadora del European Council on Foreign Relations y miembro del proyecto Gobernanza de la IA del Instituto del Futuro de la Humanidad de la Universidad de Oxford. Tiene un doctorado en Relaciones Internacionales de la Universidad de Oxford, una licenciatura de Sciences Po Paris y una doble licenciatura summa cum laude de Sciences Po Paris (Affaires internationales/ Securité internationale) y de la Universidad de St. Gallen (Asuntos Internacionales y Gobernanza). Sus áreas de interés incluyen la seguridad y la defensa alemana y europea, el futuro de la guerra y el impacto de las nuevas tecnologías como los drones y la Inteligencia Artificial.

Carla Hobbs

es editora de "La soberanía digital de Europa: De regulador a superpotencia en la era de la rivalidad entre EE.UU. y China". Es la coordinadora del proyecto "El Poder Digital de Europa" y coordinadora del programa de Madrid en el European Council on Foreign Relations. Anteriormente trabajó en el Servicio Europeo de Acción Exterior en la Delegación de la Unión Europea en Chile. Hobbs tiene un máster en historia por la Universidad de Edimburgo y un máster en periodismo internacional de la City University de Londres.

Agradecimientos

Queremos agradecer a Telefónica todo su apoyo en la celebración de los talleres y seminarios, así como en esta publicación. También estamos agradecidos a todos los participantes en los talleres del proyecto que compartieron con nosotros su experiencia y conocimientos sobre asuntos digitales y a los que se asociaron con nosotros en los eventos del proyecto, como la Embajada de España en Washington, DC, la Carnegie Endowment for International Peace y el Center for European Policy Studies. También nos gustaría agradecer a todos los miembros de ECFR su inestimable aportación y participación en el proyecto.

Telefónica DIGITAL POLICY LAB

This text was originally published by ECFR as a part of an ongoing research project with Telefonica