EUROPA: EL AVANCE EN LO DIGITAL A EXPENSAS DE ASIA Y EEUU

ANDREA G. RODRÍGUEZ
Investigadora y coordinadora de proyectos, CIDOB

En los últimos años, un debate que gana presencia en los pasillos de Bruselas, así como entre los académicos y los miembros de los *think tanks*, es hasta qué punto Europa puede devenir soberana en el campo digital. La creciente centralidad de dicho debate responde a la identificación de este tema como estratégico por parte de los estados miembros debido a la constatación de tres sucesos que, en el plano internacional, han favorecido esta relevancia y que responden a tres fenómenos concurrentes: primero, la vulnerabilidad que genera la concentración, en manos extranjeras, de datos sensibles; segundo, el modelo salvaje de explotación de datos de Silicon Valley; y tercero, el auge de China y, en particular, de sus técnicas de gestión de información, que otrora fueran el talón de Aquiles de los países autoritarios.

Empecemos por este último factor: el impulso digital de China y su liderazgo –por lo menos aparente– en el campo de la Inteligencia Artificial y de otras tecnologías emergentes han obligado a Occidente a replantearse sus relaciones con el país asiático. El tecnonacionalismo chino ha conseguido ser, de puertas para dentro, una manera de compensar la falta de libre circulación de información que permite a los gobiernos democráticos –en contacto continuo con la ciudadanía– identificar las demandas de la sociedad civil, y a las empresas, emprender la senda de la innovación. La vigilancia masiva y la Inteligencia Artificial pretenden solventar esta carencia –la de detectar las aspiraciones reales de la ciudadanía– sin tener que prescindir de la censura. De puertas para afuera, el centralismo chino se postula como una alternativa viable al sistema liberal y democrático cada vez más atacado en Europa.

En cuanto a Silicon Valley, su enfoque encaja más con el denominado *capitalismo de vigilancia*; un concepto popularizado por el libro superventas *La era del capitalismo de la vigilancia* de 2019 de la profesora estadounidense Shoshana Zuboff, que atinó en su descripción del modelo de extracción, procesamiento, explotación, comercialización, y reutilización de datos de las tecnológicas de Silicon Valley, en detrimento de los derechos y libertades del individuo, y de la seguridad de los estados. La concentración masiva de poder en unas pocas manos en Mountain View (Palo Alto) –y de manera creciente en Shenzhen– reavivó el debate regulatorio en Europa, cuyo resultado fue la promulgación del Reglamento General de Protección de Datos (2016) y, más tarde, de paquetes legislativos cruciales, como el *Digital Services Package* (2020).

Existe la creciente percepción de que el no poder controlar el ciclo de los datos es un riesgo para la seguridad nacional. La permeabilidad de las empresas chinas en el mercado europeo –en particular en el sector de las telecomunicaciones– así como los oligopolios digitales de los estadounidenses –en servicios de almacenamiento en la nube– son potenciales agujeros por los que puede escapar información sensible. Y lo cierto es que Europa, que aún carece de grandes empresas tecnológicas que puedan servir de alternativa, depende de ellos.

Solo a través de la consecución de esta posición intermedia y autónoma, capaz de mediar entre los modelos hipercentralizado (de China) y descentralizado (de EEUU), Europa podrá consolidar su posición como potencia media digital

El principio de autonomía estratégica defiende que Europa tenga suficiente rango de acción y capacidades esenciales –sin tener que recurrir a terceras partes– para el desarrollo normal de la vida política, económica y social, liberada de dependencias que limiten su agencia. Dichas capacidades rigen en cuatro áreas: en sus instituciones, en su infraestructura, en la sociedad, y en el desarrollo de nuevas tecnologías. Solo a través de la consecución de esta posición intermedia y autónoma, capaz de mediar entre los modelos hipercentralizado (de China) y descentralizado (de EEUU), Europa podrá consolidar su posición como potencia media digital y conseguir la libertad de acción que necesita para proteger su seguridad y su modo de vida.

Dentro de la Unión, la acción europea se ha centrado en la protección de los derechos *on line* de los ciudadanos frente a las amenazas exteriores, sean estos estados, personas, sistemas autónomos, o empresas. Las diferentes iniciativas contra la desinformación, o la recién publicada *Artificial Intelligence Act* (2021) son buena prueba de ello. La UE también ha tenido éxito en la coordinación avanzada de sus estados miembros para progresar en la ciberresiliencia de las instituciones, empresas, e infraestructuras europeas, como ha demostrado el éxito de la Directiva de Seguridad de las Redes y de la Información (NIS), recientemente actualizada (NIS2), así como los di-

ferentes documentos relativos a la ciberseguridad de la Unión, como el último paquete legislativo publicado en diciembre de 2020, entre cuyos documentos se incluye una nueva estrategia común.

Sin embargo, a pesar de los esfuerzos en estas dos líneas de acción, la Unión Europea necesita aún reforzar sus capacidades tecnológicas. Ha habido intentos, eso sí. La propuesta de la "nube federada europea", Gaia-X, es un proyecto prometedor. Sin embargo, a pesar de su carácter europeo, es una iniciativa que parte con dos grandes defectos. El primero es de nacimiento: es una iniciativa franco-alemana, no una iniciativa nativa paneuropea. Aunque esto pueda ser resoluble, condiciona el futuro de Gaia-X, ya que evidencia que existen países dispuestos a avanzar en su idea de autonomía –aunque sea por medios propios, y otros no. Y rebela también que la UE necesita ser más proactiva y más rápida en la activación de proyectos en materia digital.

Europa debe seguir reforzando su capacidad para corregir los fallos del mercado digital y legislar *ex ante* para guiar el desarrollo tecnológico

El segundo defecto atañe a su composición, subrayando la importancia de la capacitación digital. Gaia-X contará con la aportación de grandes empresas estadounidenses como Amazon o Google. Esto no debería ser del todo malo: es una nueva oportunidad de seguir aprovechando el "efecto Bruselas" y conseguir avanzar en los derechos digitales más allá de las fronteras europeas, ayudando a transformar internamente el operativo de estas empresas.

Otro ejemplo que justifica la necesidad de empuje es el *Quantum Flagship*. Este "buque insignia", inaugurado en 2016 con un manifiesto, reconoce que en la próxima década habrá un salto cualitativo en las tecnologías base digitales: aquello sobre lo que construir productos, servicios, o desarrollar otras tecnologías. Lo cuántico, sin prescindir de los riesgos que conlleva, será clave para seguir avanzando en otras tecnologías "columna", como la Inteligencia Artificial o la cadena de bloques (*blockchain*) de las cuales dependerán las innovaciones que incorporaremos –y que ya estamos incorporando, en nuestra vida diaria.

El *Flagship* ha nacido con una dotación extra de 1.000 millones de euros asignados como complemento a los gestionados en el marco de los proyectos de investigación Horizonte 2020. Salvo sorpresas, Europa no será vanguardia tampoco en *quantum*. En el momento de escribir estas líneas, abril de 2021, China y Estados Unidos son los firmes candidatos en liza por liderar la computación y las comunicaciones del citado proyecto. Todo apunta, es más, a que los nuevos estándares de criptografía que protegerán la información europea en las siguientes décadas vendrán del Instituto Nacional de Estándares y Tecnología estadounidense (NIST), y no de Europa. En este momento en que esta tecnología aún está en gestación, la conclusión parece clara: hay que aunar talento, estrategia, y capacidades nacionales. La movilización de recursos no lo es todo. Para el desarrollo de estas tecnologías emergentes, sean de base o de columna, debería sumarse al reconocimiento del interés estratégico la necesidad de que los estados miembros promuevan una estrategia común, más debate, y que, seguidamente, movilicen los recursos necesarios para cubrir las carencias identificadas, priorizando aquellas áreas clave para la ciberresiliencia europea.

En definitiva, en el plano institucional, Europa debe seguir reforzando su capacidad para corregir los fallos del mercado digital y legislar *ex ante* para guiar el desarrollo tecnológico. En el plano infraestructural, Europa deberá proteger sus sistemas y redes de información, especialmente los críticos, y conseguir alternativas *made in Europe* en los sectores digitales clave, lo cual será imposible sin la construcción y el desarrollo de las capacidades tecnológicas europeas. Para garantizar un futuro humanocéntrico y digital, y garantizar la protección de los derechos y libertades de sus ciudadanos, Europa debe mirar a las siguientes revoluciones tecnológicas para evitar caer en un círculo vicioso en el que simplemente va encajando lo que otros ya han hecho a su manera.