DISRUPCIONES DIGITALES Y DATOS: RETOS PARA LA SEGURIDAD EN LA INDUSTRIA EUROPEA

LUIS MARTÍNEZ LÓPEZ

PEDRO NÚÑEZ-CANCHO UTRILLA

ROSA MARIA RODRÍGUEZ DOMÍNGUEZ

Universidad de Jaén

La *autonomía estratégica* en la Unión Europea (UE) surgió en el ámbito de la industria de la defensa y seguridad, y ha evolucionado a otros sectores clave como la economía y la tecnología. La autonomía estratégica es la base para construir un eje geopolítico en la UE, que no la lleve a la irrelevancia en económica. La ciencia, la tecnología, la tecnología digital, el comercio y los datos son elementos claves para alcanzar la autonomía estratégica en la UE. Actualmente, el ámbito digital está siendo dominado por las compañías Big Tech americanas. Por la importancia del sector, se evidencia una grave vulnerabilidad de la UE y es necesario abrir un proceso a medio-largo plazo para que la UE aproveche las nuevas disrupciones tecnológicas, como la Inteligencia Artificial (IA), la computación cuántica, etc., y se conciencie de la necesidad de desarrollar una industria tecnológica líder capaz de competir con las Big Tech y garantizar un futuro confortable y sostenible.

¿Qué lugar ocupa la Unión Europea (UE) en este intrincado panorama? La UE es, con diferencia, el mayor comerciante del mundo, por delante de China y Estados Unidos, y es también el principal socio comercial de 80 países. Al tiempo que persigue una agenda de liberalización comercial, la UE se ha vuelto cada vez más cautelosa sobre la importancia de preservar sus propios intereses económicos y de seguridad: por eso su política exterior -incluido el comercio- se inspira actualmente en la *consigna* de la ***Autonomía Estratégica*** (Helwig and Sinkkonen, 2022), concepto que surgió fundamentalmente en el ámbito de la industria de la defensa y seguridad, y ha evolucionado a otros sectores clave como la economía y la tecnología. La autonomía estratégica es un concepto clave que implica que las cadenas de suministro críticas (ECB, 2019), -aquellas que son cruciales para desarrollar las transiciones verde y digital, deben asegurarse y regionalizarse, partiendo de los intereses de la UE, en lugar de priorizar áreas o regiones específicas como socios comerciales. Y es que, como se ha evidenciado durante y después de la pandemia del COVID-19, existe un carácter asimétrico de la interdependencia y la vulnerabilidad de la UE respecto a otros bloques económicos. Cabe indicar que la UE va a la zaga de China y EE.UU. en cuanto al control de insumos clave (como minerales y materias primas críticas) y está aún más atrasada en otros insumos tecnológicos como por ejemplo la fabricación de semiconductores.

La cuestión de cómo se identifican los productos o sectores esenciales sólo puede responderse teniendo en cuenta consideraciones políticas o económicas, y éstas se están abordando en el curso del debate sobre la *autonomía estratégica abierta* de la UE (1). Todo ello a pesar de que, en los últimos años, el parlamento Europeo ha discutido muchos

aspectos relativos al próximo orden internacional y a los crecientes cambios geopolíticos. También ha analizado el contexto de una *autonomía estratégica de la UE* centrada en los potenciales de deslocalización, en particular para los suministros críticos indicados anteriormente (materias primas, semiconductores, etc.). A dichos insumos, están incorporándose algunos de origen digital basados en tecnologías disruptivas como la Inteligencia Artificial (IA), computación cuántica, etc., que van a ser claves en la competitividad, desarrollo y seguridad de distintas industrias mundiales y de la EU en las próximas décadas. En estas tecnologías, las *Big Tech* americanas (Alphabet, Apple, Meta, Microsoft, X, etc.) y más recientemente las chinas (Alibaba, Huawei, Tecent) son líderes a nivel mundial, creando la posibilidad de importantes fallas de ciberseguridad en las empresas de la UE. Por ello, los responsables políticos deberían considerar *esenciales*, entre otros, a los siguientes ámbitos relacionados con la transición digital: robótica, IA y ciberseguridad.

La autonomía estratégica digital va ligada con el concepto de *Soberanía Tecnológica* (Crespi *et al*. 2021), que se entiende como la capacidad de un Estado o de una federación de Estados de proporcionar las tecnologías que considere esenciales para su bienestar, competitividad y capacidad de acción, y de desarrollarlas o abastecerse de ellas en otras áreas económicas sin una dependencia estructural unilateral (Edler *et al*., 2023). Este concepto se basa en el hecho que ningún país puede confiar únicamente en sus propias capacidades y en el tamaño de su mercado para mantener su soberanía en un mundo globalizado e interconectado. Esto implica que la soberanía no requiere autonomía tecnológica pura y dura, sino que, por el contrario, sugiere la necesidad de que un país desarrolle o preserve, con respecto a las tecnologías clave, su propia autonomía o, alternativamente, tenga el nivel más bajo posible de dependencia estratégica de sus socios internacionales.

En esta contribución se pretende concienciar de la importancia que tiene la transición digital y algunos de sus elementos como los datos o las disrupciones tecnológicas en el devenir económico, social, sostenible y de defensa en la UE. La autonomía estratégica digital debe ser un objetivo claro de la UE. Además, se señalarán los retos que supone la autonomía estratégica digital y las implicaciones políticas que tiene la consecución de esta autonomía. Finalmente, se concluirá la contribución apuntando algunas necesidades y situaciones clave que implica la autonomía estratégica digital en la UE.

DISRUPCIONES TECNOLÓGICAS Y DATOS EN LA UE

La autonomía estratégica, como hemos visto, abarca distintos ámbitos y cada uno de ellos depende de elementos diferenciados. Así, en el campo digital y en ciberseguridad son claves elementos como las disrupciones tecnológicas o la gestión de los datos. A continuación, vamos a ver con brevedad estos conceptos, su implicación en la ciberseguridad y cómo su estado actual en la UE indicará cuales son los retos que debe abordar la Unión y las políticas que se están llevando a cabo actualmente o que se deben afrontar en un futuro cercano.

Disrupciones tecnológicas

Las disrupciones tecnológicas fueron descritas con detalle por (Bower y Christensen, 1995), que definen una tecnología disruptiva como aquella que permite transformar y generar nuevos mercados económicos; tal y como ha ocurrido con Internet desde su aparición en los años 90. Más recientemente situamos la IA, la robótica y en un futuro cercano, si se cumplen las expectativas, la computación cuántica.

A menudo se subestima el potencial de las tecnologías disruptivas, fundamentalmente porque la industria o los agentes económicos, no entienden bien la propia tecnología. La tecnología disruptiva tiene el potencial de revolucionar una industria. Puede hacer que los productos y servicios sean mejores, más rápidos y más asequibles. En algunos casos, puede incluso crear mercados completamente nuevos. La adopción de tecnologías disruptivas permite mantener o alzarse con el liderazgo a las empresas en su actividad económica o industrial, aunque la capacidad de adopción de este tipo de tecnologías ha sido y es siempre compleja; y en muchas ocasiones ni si quiera las empresas líderes son capaces de mantener su liderazgo por su incapacidad para adaptarse a dichas tecnologías disruptivas.

Datos

Las tecnologías disruptivas relacionadas con la transición digital mencionadas anteriormente, IA, computación cuántica, etc., tienen como elemento común clave: *los datos*, que además son el elemento central de la transformación digital de la UE, y que afecta a todos los aspectos de la sociedad y de la economía.

Los datos son el *producto transferible* por excelencia y son necesarios para el desarrollo entre otras de la IA, y para el crecimiento, por ejemplo, en sanidad y tecnologías verdes. Pero moverlos a través de las fronteras requiere que los países tengan políticas coherentes que generen confianza. Por lo que, unos principios globales sobre política de datos pueden ayudar a equiparar normativas internacionales y así abordar la estabilidad y la inclusión financiera, la competencia y la privacidad. Sin dichos principios globales para la gestión de los datos, podríamos enfrentarnos a un agravamiento de la brecha digital entre las naciones, a medida que conjuntos masivos de datos queden cada vez más aislados.

En la UE ya existen grandes cantidades de datos de calidad, sobre todo no personales -industriales, pú-

blicos y comerciales- y aún está por explorar todo su potencial. En los próximos años se generarán muchos más datos. Permitir el flujo de datos entre sectores y países ayudará a las empresas europeas de todos los tamaños a innovar y prosperar en Europa y fuera de ella, y contribuirá a establecer a la UE como líder en la economía de los datos.

Ciberseguridad

Todo lo anterior, junto a la aceleración de la transformación digital de la economía y la sociedad, ha creado oportunidades, pero también grandes retos como la seguridad en general y la ciberseguridad en particular (Garnert, 2022). De aquí, la inclusión del ámbito digital en la consigna de Autonomía Estratégica en la UE.

Dado que cada vez más, nuestras vidas y nuestra actividad diaria dependen de las tecnologías digitales, el coste económico y social de los ciberataques es cada vez mayor y puede causar perjuicios no sólo económicos y sociales, sino también en términos de vidas humanas. Por ello, la ciberseguridad ha adquirido gran importancia y se ha convertido en una prioridad clave de la UE.

En el campo de la defensa, la Agencia Europea de Defensa (AED) ha identificado seis tecnologías especialmente disruptivas:

1. Tecnologías basadas en la computación cuántica (Abd *et al*. 2021)
2. Inteligencia artificial (IA) (Thanh and Zelinka, 2019)
3. Robótica y sistemas de armas autónomos (Singer, 2009)
4. Análisis de grandes volúmenes de datos (Dai and Boroomand, 2021)
5. Sistemas de armas hipersónicas y tecnologías espaciales
6. Nuevos materiales avanzados.

Las cuatro primeras tienen una influencia fundamental no sólo en la defensa y su industria, sino también en el desarrollo de múltiples industrias y servicios (automovilística, aeronáutica, turística, farmacéutica, salud, energía etc.) y en la gestión de la ciberseguridad de sus datos, información y conocimiento.

Los sectores más expuestos a fallas de ciberseguridad por depender en gran medida de las redes de comunicación y los sistemas de información son: el transporte, la energía, la sanidad, las telecomunicaciones y las infraestructuras digitales, los bancos y los mercados financieros, la seguridad, y la defensa.

La UE necesita crear un ciberespacio seguro como base del mercado único digital de la propia Unión construyendo soluciones que permitan liberar todo su potencial, generando confianza a la población hacia los nuevos modelos económicos y sociales creados por la transición digital.

Autonomía Estratégica digital en la UE

El telón de fondo general de la rivalidad geopolítica entre China y EE.UU. que ha llevado a la UE a establecerse como un tercer actor estratégicamente autónomo, adquiere una capa adicional cuando la competencia afecta al ciberespacio y a las tecnologías digitales. En la última década, el ciberespacio se ha geopolitizado por completo. Lucas Kello (2017) ha caracterizado su situación como de *no pacífica*, sin llegar a la guerra, pero sin duda tampoco a la paz. La competencia geopolítica estratégica de bajo nivel se ha convertido en la *nueva normalidad* en el ámbito digital, lo que ha generado en Europa un vacío estratégico (Buchanan 2020; Liebetrau 2022). Además, los Estados miembros tienen problemas para determinar sus propias *normas de circulación en el ciberespacio*, y hay desacuerdos sobre la aplicabilidad y los límites de los principios jurídicos internacionales, como la soberanía, en el ciberespacio (Delerue 2020; Liebetrau 2022). Ante esta situación, no es sorprendente que, bajo la bandera de la autonomía estratégica y la soberanía tecnológica, muchas de las políticas digitales y de ciberseguridad de la UE se encuentren en un proceso de geopolitización.

Hay que recordar que junto con Estados Unidos y el noreste asiático, Europa es el tercer gran productor de innovación técnica y conocimiento. Por lo que, Europa posee grandes conocimientos en ámbitos como la investigación pura y la tecnología industrial aplicada, pero también sufre déficits en campos nuevos y cruciales como la computación cuántica y las aplicaciones basadas en datos, así como muestra también carencias para tener unas condiciones para un rápido crecimiento impulsado por la innovación. Por consiguiente, tanto en la actualidad como en un futuro previsible, la UE no estará en condiciones de alcanzar a China y Estados Unidos en la economía digital. Esto hace que sea aún más importante centrarse en innovación, donde las capacidades digitales son la base para crear una influencia global y reducir dependencias para alcanzar una soberanía tecnológica y autonomía estratégica.

En tecnologías de la información y criptografía, por ejemplo, Europa sólo podrá influir en los procesos de normalización y la utilización de la tecnología si alcanza los conocimientos y la capacidad de investigación y fabricación necesarios. Otros ejemplos relevantes en este ámbito pueden ser, la IA y la robótica/sistemas autónomos.

Vemos pues, que ante la posibilidad de *guerras tecnológicas* (Miller, 2022) y las dependencias tecnológicas que constriñen el crecimiento económico, la UE debe abordar una serie de retos para mejorar su posición actual en el ámbito digital y de cibersegu-

ridad, ya que se encuentra muy por detrás de otras potencias como EE.UU. o China. Para ello, ha de reducir sus dependencias estratégicas (Edler *et al.*, 2023) mediante la generación de más capacidades productivas y tecnológicas que son inherentemente locales, acumulativas y están correlacionadas con la fortaleza de instituciones de conocimiento claves como organismos públicos de I+D, universidades, organizaciones que facilitan la transferencia de tecnología, etc. Estas capacidades son difíciles de crear y acumular, ya que pueden requerir un plazo considerable de tiempo, así como la disponibilidad de activos y competencias complementarios que no siempre están disponibles.

RETOS PARA LA AUTONOMÍA ESTRATÉGICA TECNOLÓGICA EN LA UE

Debido a que la innovación y el progreso tecnológicos han desempeñado un papel crucial desde los inicios del proceso de integración europea (Misa y Schot 2005), las referencias a una *brecha tecnológica europea* -tanto internamente entre los Estados miembros como externamente con respecto a las potencias mundiales- han acompañado el discurso político. Hasta la aparición de la era *digital* como ámbito político específico, la UE no se refirió anteriormente a la innovación tecnológica como una cuestión geopolítica, además de como una cuestión de competitividad económica.

Como hemos visto en las secciones anteriores, la UE está lejos de tener una autonomía estratégica en el campo digital, así como, en la gestión y tratamiento de datos ya que, entre las compañías líderes en estos campos (Big Tech) no hay ninguna perteneciente a la Unión. Ante esta realidad, la UE debe afrontar una serie de retos que reduzcan la dependencia tecnológica con actores externos y generar capacidades propias que le permitan liderar campos tecnológicos impulsados por las actuales innovaciones disruptivas relacionadas con la transformación digital (Broeders, 2023).

¿Cuáles han de ser las prioridades y retos de la UE para definir y proteger más claramente sus propios intereses, y que se integren y/o complementen con sus retos sociales, de crecimiento sostenible entre otros objetivos de la Unión? La respuesta a esta pregunta no es simple ya que implica una serie de intereses, que pueden entrar en conflicto entre sí. Por lo que, aquí simplemente pretendemos focalizar las necesidades más importantes de la UE para mejorar su autonomía estratégica en el ámbito digital, apuntando algunos de los retos más importantes en este campo:

- *Identificar con claridad cuáles son los ámbitos en los que la seguridad digital*, la gestión/tratamiento/análisis de datos y la garantía de la prestación de servicios revisten una importancia crucial para los ciudadanos de la UE.
- Al igual que en el enfoque de autonomía estratégica europea requiere un *modelo de gobernanza centralizado* para alinear los objetivos estratégicos, los recursos y la gestión. Este enfoque debe llevarse también específicamente al ámbito digital. De forma que se aplique un enfoque integral entre las instituciones involucradas para gestionar la autonomía estratégica a lo largo del ciclo de vida de las capacidades críticas, incluida su propiedad y gestión.
- *Establecimiento de normas de referencia mundiales* en materia de regulación y normas digitales acordes con los valores de la UE, especialmente para la economía digital. Esto conlleva crear una normativa jurídica adecuada, que transcienda visión clásica de la UE de crear normativas basadas en la protección tanto de los derechos humanos como de la libertad de mercado, que pueden entrar en contradicción con el nuevo marco del ciberespacio y las tecnologías digitales emergentes siendo a la vez una amenaza y una ventaja para la agenda estratégica de la Unión. Esta normativa es necesaria para reafirmarse como potencia geoestratégica, sin socavar su imagen de potencia reguladora y normativa.
- Desarrollo de capacidades tecnológicas basadas en la UE a través de la innovación y la competitividad industrial. Es decir, construir infraestructuras y servicios críticos de la UE para reforzar el papel de la UE en la cadena mundial de suministro digital y desarrollar una mano de obra europea cualificada (Comisión Europea 2020a, pp. 5-12)
- Reforzar su soberanía en el ámbito digital, reduciendo su exposición a agentes externos tales como, las grandes empresas tecnológicas o los gobiernos.

IMPLICACIONES POLÍTICAS DE LA AUTONOMÍA ESTRATÉGICA DIGITAL

La pugna geopolítica entre los grandes bloques mundiales, EE.UU., China, UE y Rusia, junto a la decadencia cada vez más clara de la globalización y a las últimas crisis sufridas recientemente, han hecho que la UE se plantee la autonomía estratégica como un objetivo prioritario para reducir su dependencia de otros países o gobiernos. En la era de la digitalización, esta necesidad de autonomía estratégica se ha extendido al campo digital en el que la UE tiene un importante retraso con respecto a EE.UU. y China.

Para alcanzar los objetivos de la autonomía estratégica digital, la UE ha tenido que fijar los ámbitos de la seguridad digital y desarrollar a través de su agenda digital distintas directivas y normas digitales acordes con los valores de la UE para reafirmarse como potencia geoestratégica en el ámbito digital.

Igualmente, la agenda digital de la UE ha impulsado el desarrollo de capacidades tecnológicas a través de la innovación y la competitividad industrial. Se ha desarrollado la Estrategia Europea de Datos, una legislación basada en los valores europeos de privacidad y transparencia que permita a los ciudadanos y a las empresas con sede en la UE beneficiarse del potencial de los datos industriales y públicos

La UE está trabajando también para reforzar la ciberseguridad. En noviembre de 2022, el Parlamento aprobó la Directiva sobre la seguridad de las redes y sistemas de información (NIS2), que establece normas exhaustivas para reforzar la resistencia en toda la UE. También en noviembre de 2022, los eurodiputados aprobaron leyes para aumentar la resistencia del sector financiero de la UE a los ciberataques con la ley de resistencia operativa digital (Dora).

La estrategia y el Libro Blanco sobre IA son los primeros pilares de la estrategia digital de la Comisión.

En el ámbito de los datos la iniciativa Gaia-X, que implica el desarrollo de una infraestructura europea de datos, es un ejemplo de gran proyecto destinado a reforzar la soberanía de la UE en materia de datos. Esta preocupación europea por la protección de datos no es nueva. Con el tiempo, la UE se ha ganado una reputación por su legislación activista en este ámbito: se adoptó la Directiva de Protección de Datos ya en 1995 y el Reglamento General de Protección de Datos (GDPR) en 2016. En un testimonio de la enorme influencia reguladora de la UE, muchos terceros países introdujeron posteriormente normas de protección de datos similares en su propia legislación para conservar el acceso a los mercados de la UE.

Para impulsar el intercambio de datos en la UE, el Parlamento y el Consejo adoptaron la Ley de Gobernanza de Datos en 2022 como parte de la estrategia para los datos. Su objetivo es aumentar la disponibilidad de datos y reforzar la confianza en el intercambio de datos y en los intermediarios, y se aplicará a partir de septiembre de 2023. A partir de ahí, en marzo de 2023 el Parlamento adoptó su posición sobre la Ley de Datos, que facilitará a las empresas el acceso a grandes cantidades de datos industriales de alta calidad.

CONCLUSIONES

En los últimos años, la UE ha estado al margen de la competencia tecnológica, debido entre otras cuestiones a la necesidad de generar una autonomía estratégica digital. Por su parte, la UE ha empezado a desempeñar un papel relevante a nivel internacional en la regulación, la normalización y el desarrollo de normas en el ciberespacio. Algunas de estas regulaciones han sido un éxito, y han mostrado cómo la regulación puede convertirse en una importante oportunidad geopolítica para garantizar que las normas se crean teniendo en cuenta los valores humanos y un enfoque centrado en las personas. Estos esfuerzos normativos en ámbitos como la creación de un Espacio Único de Datos en la UE basado en la convergencia, junto a la elaboración de nuevas normas técnicas para las tecnologías disruptivas, etc., pueden ayudar a la UE a reforzar su papel como actor internacional, aunque no son suficientes para alcanzar una autonomía estratégica digital.

Por tanto, la reducción de dependencias internacionales, la creación de capacidades tecnológicas propias de la UE a través de la innovación y la competitividad industrial son elementos que han de ser reforzados en la Agenda digital de la unión para minimizar riesgos de seguridad y eliminar barreras al crecimiento económico que existen actualmente por el retraso existente en la UE en estas tecnologías respecto a otros espacios geopolíticos como EE.UU. o China.

NOTAS

[1] https://ec.europa.eu/commission/presscorner/detail/en/qanda_21_645

REFERENCIAS

A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, «Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in iot-based smart cities,» Information Processing & Management,vol. 58, no. 4, p. 102549, 2021.

Bower, J. L. y Christensen, C. M. (1995). Disruptive technologies: Catching the wave. Harvard Business Review, 73(1), 43-53.

Broeders, D., Cristiano, F. and Kaminska, M. (2023) 'In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of its Geopolitical Ambitions'. JCMS: Journal of Common Market Studies. https://doi.org/10.1111/jcms.13462

Buchanan, B. (2020) The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics (Cambridge (Mass.): Harvard University Press).

Crespi F., Caravella S., Menghini M. and Salvatori C. (2021). European Technological Sovereignty: An emerging framework for policy strategy, Intereconomics 56 (6), 348-354

D. Dai and S. Boroomand, «A review of artificial intelligence to enhance the security of big data systems: state-of-art, methodologies, applications, and challenges,» Archives of Computational Methods in Engineering, pp.1–19, 2021.

Delerue, F. (2020) Cyber Operations and International Law (Cambridge (UK): Cambridge University Press).

ECB, European Central Bank, «The impact of global value chains on the euro area economy», Occasional Paper Series, no. 221, 2019

Edler, J., Blind, K., Kroll, H. and Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means, Research Policy, 52(6), 104765

European Commission. (2020a) The EU's cybersecurity strategy for the digital decade. https://eurlex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN

Gartner, «Top strategic technology trends for 2022: Cybersecurity mesh,» [Online], 2022, last accessed 2022-06-24. https://www.gartner.com/en/doc/756665-cybersecurity-mesh.

Liebetrau, T. (2022) 'Cyber Conflict Short of War: A European Strategic Vacuum'. European Security, Vol. 31, pp. 497–516. https://doi.org/10.1080/09662839.2022.2031991

N. Helwig, V. Sinkkonen, 'Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term', (2022), 27, European Foreign Affairs Review, Issue SI, pp. 1-20, https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/27.2/EERR2022009

Miller, C. (2022). Chip War: The Fight for the World's Most Critical Technology. Simon and Schuster.

Misa, T.J. and Schot, J. (2005) 'Inventing Europe: Technology and the Hidden Integration of Europe. Introduction'. History and Technology, Vol. 21, pp. 1–19.

Singer, P.W. (2009), Wired for War: The Robotics Revolution and Conflict in the 21st Century , Penguin Press, New York, NY.

Thanh C. and Zelinka I., «A survey on artificial intelligence in malware as next-generation threats,» MENDEL, vol. 25, no. 2, pp. 27–34, Dec. 2019.

WTO, World Trade Organization, «Trade growth to slow sharply in 2023 as global economy faces strong headwinds», 2022.