Capítulo segundo

Poder, geopolítica, soberanía y tecnología

José Ignacio Torreblanca

Resumen

Este texto analiza el retorno de la tecnología como variable estructural del poder internacional. Sostiene que, igual que en revoluciones anteriores —agrícola, industrial y digital—, las innovaciones tecnológicas contemporáneas están reconfigurando la economía, la organización estatal y el orden global. Sin embargo, muestra que la actual revolución tecnológica presenta rasgos distintivos: una difusión acelerada y global, la consolidación de la esfera digital como dominio de conflicto y la emergencia de empresas privadas como proveedoras de infraestructuras esenciales para la soberanía y la seguridad. El texto argumenta que la competencia entre EE. UU. y China está impulsando dinámicas de securitización, desacoplamiento selectivo y fragmentación en bloques tecnológicos, con consecuencias directas sobre los estándares, los datos, las cadenas de suministro y las alianzas. El texto examina, finalmente, la posición vulnerable de la UE: fuerte en capacidad regulatoria, pero dependiente y vulnerable ante EE. UU. y China para el acceso a tecnologías críticas. A partir de este diagnóstico, plantea la construcción de una soberanía digital europea como condición para preservar su autonomía

estratégica, su modelo democrático y de valores y su capacidad de decisión política y estratégica.

Palabras clave

Soberanía digital, Geopolítica de la tecnología, Coacción tecnológica, Inteligencia artificial, Regulación digital europea.

Power, geopolitics, sovereignty, and technology

Abstract

This text examines the return of technology as a structural variable of international power. It argues that, as in previous revolutions—the agricultural, industrial, and digital ones—contemporary technological innovations are reshaping the economy, state organization, and the global order. However, it shows that the current technological revolution has distinctive features: rapid and global diffusion, the consolidation of the digital sphere as a domain of conflict, and the emergence of private companies as providers of infrastructures that are essential to sovereignty and security.

The competition between the United States and China, the text argues, is driving dynamics of securitization, selective decoupling, and fragmentation into technological blocs, with direct consequences for standards, data, supply chains, and alliances. Finally, the text examines the European Union's vulnerable position: strong in regulatory capacity, yet dependent on and exposed to the United States and China for access to critical technologies. On the basis of this diagnosis, it calls for the construction of European digital sovereignty as a prerequisite for preserving the EU's strategic autonomy, its democratic and values-based model, and its capacity for political and strategic decision-making.

Key words

Digital sovereignty, Geopolitics of technology, Technological coercion, Artificial intelligence, European digital regulation.

Introducción

Este texto analiza el retorno de la tecnología como variable estructural del poder internacional. Sostiene que, igual que en revoluciones anteriores —agrícola, industrial y digital—, las innovaciones tecnológicas contemporáneas están reconfigurando la economía, la organización estatal y el orden global. Sin embargo, muestra que la actual revolución tecnológica presenta rasgos distintivos: una difusión acelerada y global, la consolidación de la esfera digital como dominio de conflicto, y la emergencia de empresas privadas como proveedoras de infraestructuras esenciales para la soberanía y la seguridad. El texto argumenta que la competencia entre EE. UU. y China está impulsando dinámicas de securitización, desacoplamiento selectivo y fragmentación en bloques tecnológicos, con consecuencias directas sobre los estándares, los datos, las cadenas de suministro y las alianzas. El texto examina, finalmente, la posición vulnerable de la UE: fuerte en capacidad regulatoria, pero dependiente y vulnerable ante EE. UU. y China para el acceso a tecnologías críticas. A partir de este diagnóstico, plantea la construcción de una soberanía digital europea como condición para preservar su autonomía estratégica, su modelo democrático y de valores y su capacidad de decisión política y estratégica.

1 El retorno de la historia

Hoy en día, las grandes potencias, plenamente conscientes de que el acceso, control y dominio de las tecnologías críticas, es un requisito indispensable para su supervivencia estratégica, han entrado en una competencia cada vez más intensa por asegurar su soberanía digital y tecnológica. Esta rivalidad no se limita al ámbito económico, sino que abarca dimensiones militares, políticas, culturales y normativas. La tecnología se ha convertido, así, en un factor estructural del poder y de la rivalidad internacional, al mismo nivel que el territorio, la población o los recursos naturales.

Este fenómeno no es nuevo. A lo largo de la historia, las grandes revoluciones tecnológicas han actuado como precursoras de grandes cambios sistémicos, desencadenando profundas transformaciones económicas, sociales y políticas tanto dentro de las sociedades como en la configuración del sistema internacional y las relaciones entre sus unidades. Esos cambios han

desencadenado, a menudo, importantes conflictos, tanto dentro como entre los estados.

Hace aproximadamente siete mil años, la transición desde economías de subsistencia hacia formas de agricultura intensiva, asociadas a la domesticación de especies como el trigo y al desarrollo de tecnologías de irrigación, produjo un cambio radical en la organización social. La generación de excedentes agrícolas permitió la especialización del trabajo y sentó las bases para la aparición de las primeras instituciones políticas permanentes: burocracias administrativas, sistemas fiscales, ejércitos profesionales y jerarquías religiosas.

Estos avances impulsaron la codificación del derecho, la organización formal del conocimiento y la expansión del comercio a larga distancia. A su vez, las necesidades de gestión de grandes poblaciones y territorios favorecieron una concentración del poder político en determinados núcleos geográficos, dando lugar a estructuras estatales complejas. Surgieron así los denominados «imperios hidráulicos», cuyo poder descansaba en el control de los recursos hídricos y agrícolas, así como en la capacidad de financiar y armar ejércitos de gran tamaño. Estas entidades proyectaron su influencia más allá de sus fronteras, entrando en conflicto con entidades políticas similares.

Más cercana a nuestros días, la Primera Revolución Industrial (1760-1840), impulsada por la máquina de vapor, la mecanización textil y el uso intensivo del carbón, también tuvo profundas consecuencias políticas y geopolíticas. Por un lado, marcó el paso decisivo de una economía agraria a una economía industrial. Por otro, erosionó las estructuras políticas, sociales y económicas del Antiguo Régimen, facilitando la transición hacia el liberalismo económico y político. La industrialización aceleró la urbanización y dio lugar a nuevas clases sociales —la burguesía industrial y el proletariado urbano— cuyas demandas transformaron profundamente las estructuras de representación política.

Estos cambios desencadenaron revoluciones políticas —la americana (1776-1789) y la francesa (1789-1808), que cristalizaron en nuevas formas de organización estatal que cuestionaron el orden monárquico tradicional europeo y modificaron profundamente el orden internacional vigente en aquel momento. El choque entre estos nuevos regímenes y las monarquías absolutas desencadenó una prolongada etapa de conflictos armados que

culminó en el Congreso de Viena (1814) y en la creación de un nuevo equilibrio de poder continental.

En sentido parecido, la Segunda Revolución Industrial (1860-1930), basada en la electricidad, el ferrocarril, el telégrafo y los barcos de vapor, amplificó de forma extraordinaria la capacidad de los Estados para proyectar poder, tanto en el ámbito interno como en el internacional. Estas tecnologías redujeron drásticamente los costes de transporte y comunicación, integrando mercados nacionales y expandiendo el comercio mundial a una escala sin precedentes.

El impacto geopolítico de la superioridad tecnológica occidental fue un factor decisivo, ya que permitió la dominación de vastos territorios a un coste relativamente bajo. De manera similar a como la expansión española en América se había apoyado en avances en navegación, metalurgia y el uso del caballo, la conquista de África en el siglo XIX y la gran etapa de colonialismo que siguió habría sido impensable sin el tridente tecnológico formado por el barco de vapor, la ametralladora y la quinina (Headrick, 1979). La tecnología no solo otorgó ventajas militares, sino que dio lugar a un sistema de relaciones internacionales basado en la creación de grandes imperios coloniales y las rivalidades entre ellos. Aunque los imperios europeos lograron dominar Asia y África —y EE. UU. a la luz de la doctrina Monroe revivida hoy, el continente americano— el choque entre los imperios europeos dio lugar a la Primera Guerra Mundial y el comienzo de un largo proceso de declive europeo.

En Asia, los casos de China y Japón ilustran de forma clara las consecuencias del retraso tecnológico. Durante el siglo XIX, la incapacidad del Imperio Qing para adoptar las tecnologías clave de la Revolución Industrial condujo a una serie de derrotas militares frente a potencias occidentales, materializadas en las guerras del opio y el denominado «siglo de la humillación». Esta experiencia histórica ha dejado una huella duradera en la cultura estratégica china. La centralidad que los líderes chinos conceden hoy a la tecnología como garante de la soberanía nacional y del estatus internacional no puede entenderse sin este trasfondo histórico. Su apuesta decidida por no quedar rezagados en ámbitos como la inteligencia artificial, la computación avanzada o los semiconductores responde tanto a cálculos económicos como a una lógica geopolítica y de supervivencia.

En sentido parecido, Japón, que durante el periodo Tokugawa había mantenido una política de aislamiento internacional, sufrió

un gran *shock* tecnológico de profundas consecuencias políticas, económicas y culturales en 1853 tras la aparición de los «barcos negros» estadounidenses —como se denominó a los barcos de vapor del comodoro Perry— viéndose obligada también a firmar una serie de tratados completamente asimétricos que le forzaban a abrirse al comercio internacional.

La Tercera Revolución Industrial (1970-2000), articulada en torno a las tecnologías de la información y la comunicación (TIC), también ha transformado de manera estructural las economías y los Estados. A finales del siglo pasado, la digitalización, la automatización y la liberalización financiera, facilitaron una nueva ola de globalización, caracterizada por cadenas de valor transnacionales, flujos masivos de capital y una integración sin precedentes de los mercados. Estas dinámicas favorecieron la emergencia de nuevos actores internacionales de gran peso, especialmente China, pero también otros países del sur global, un fenómeno que se vio acelerado por el fin de la Guerra Fría y la incorporación de China, India y otras economías asiáticas a las dinámicas de globalización.

El resultado de la difusión del progreso y la innovación tecnológica desde Occidente hasta el resto del mundo ha sido la progresiva erosión del predominio exclusivo de Occidente y la transición hacia un orden internacional multipolar en el que el poder económico y tecnológico se distribuye de forma más difusa. Dentro de esa dinámica, el auge de China ha supuesto la emergencia de una potencia con capacidad de medirse económica, tecnológica y militarmente con EE. UU. Eso ha llevado a los analistas a preguntarse acerca de la posibilidad de un conflicto entre ambas potencias de acuerdo con los parámetros clásicos detectados a lo largo de la historia entre potencias establecidas y potencias emergentes y referidos en términos de «Trampa de Tucídides» por autores como Allison (2017), que han cuantificado dieciséis grandes transiciones de poder a lo largo de la historia, concluyendo que solo cuatro de ellas no desembocaron en un conflicto bélico.

La cuarta revolución industrial, iniciada en torno a 2010 con avances en robótica, conectividad global e inteligencia artificial, está profundizando estas transformaciones de forma aún más singular. El centro de gravedad del poder empresarial se ha desplazado desde sectores tradicionales —como la energía o las finanzas— hacia el sector tecnológico, que abarca desde el *software* en la nube y los semiconductores hasta las infraestructuras digitales críticas y las plataformas y redes sociales.

Este desplazamiento ha provocado una creciente intervención del Estado en ámbitos que con anterioridad se consideraban predominantemente privados. Las grandes potencias compiten ahora por controlar los puntos estratégicos de la economía digital: datos, algoritmos, infraestructuras de conectividad y capacidad de computación. En este contexto, la inteligencia artificial se ha convertido en un campo central de rivalidad geopolítica, especialmente entre EE. UU. y China, con implicaciones directas sobre alianzas, normas internacionales y equilibrios de poder. La IA no solo está transformando las relaciones productivas y laborales dentro de los Estados, sino que está reconfigurando la arquitectura del poder global, al introducir nuevas asimetrías y dependencias tecnológicas. Al igual que en revoluciones tecnológicas anteriores, quienes logren dominar estas capacidades definirán, en gran medida, las reglas del orden internacional del siglo XXI y la jerarquía de poder dentro de ese orden.

Si en los años ochenta del siglo pasado las compañías más grandes del mundo en capitalización bursátil eran las grandes empresas petroleras o bancarias, en la actualidad, esa posición está ocupada por las grandes tecnológicas estadounidenses como Nvidia, Google, Amazon, Apple y Meta, siguiéndoles muy a la zaga las tecnológicas chinas y sin una presencia relevante de empresas europeas entre las veinte más grandes del mundo. Ese mapa empresarial dibuja hoy la distribución de poder económico y tecnológico global, pero también una nueva geopolítica marcada de manera tan profunda por la conversión de las interdependencias en vulnerabilidades (Leonard, 2021), las asimetrías en las capacidades tecnológicas y las guerras de conectividad como lo fue la segunda mitad del siglo XX por las asimetrías en torno al acceso al petróleo y el gas.

Las consecuencias internacionales de esta reconfiguración del mundo en torno a las tecnologías digitales son claras. Al igual que la economía basada en la explotación de combustibles fósiles generó un orden internacional y una serie de alianzas vinculada al acceso y control de los centros de producción en Oriente Próximo y el golfo Pérsico, la actual economía, basada en la explotación de datos, está generando su propio sistema de relaciones internacionales, basado en el acceso a materias primas críticas para alimentar ese desarrollo tecnológico y las cadenas de suministro y centros y redes de producción y distribución de las tecnologías digitales —en especial, Taiwán—. Para Europa, la nueva geopolítica de la tecnología implica transitar desde las dependencias y

vulnerabilidades asociadas al petróleo y el gas de Oriente Próximo y Rusia hasta quedar atrapada en una nueva dependencia de los modelos de inteligencia artificial, los centros de datos, los semiconductores y otras tecnologías en disputa entre EE. UU. y China.

2 La nueva geopolítica de la tecnología

Como se ha puesto de manifiesto en la sección anterior, las innovaciones tecnológicas han generado de manera recurrente transformaciones profundas tanto en el interior de los Estados como en el sistema internacional, alterando las relaciones de poder, las formas de organización política y las dinámicas de conflicto y cooperación. No obstante, y pese a las claras continuidades entre la actual revolución tecnológica y procesos históricos anteriores, es posible identificar una serie de elementos cualitativamente novedosos que distinguen a la transformación tecnológica contemporánea de las revoluciones precedentes.

En primer lugar, hay que señalar la velocidad, alcance y profundidad de los cambios tecnológicos actuales, especialmente en lo relativo a la conectividad global y la difusión de innovaciones. Mientras que tecnologías clave del siglo xx, como el teléfono, necesitaron cerca de medio siglo para alcanzar el millón de usuarios y un siglo para alcanzar los cien millones, las herramientas contemporáneas basadas en inteligencia artificial generativa, como ChatGPT, lograron el millón de usuarios en cinco días y los cien millones en cinco meses (Hu, 2023). Este fenómeno no es excepcional, sino representativo de una dinámica más amplia: la difusión de nuevas tecnologías ya no sigue patrones graduales, sino procesos acelerados y simultáneos a escala global.

Una transformación similar puede observarse en el ámbito económico. Históricamente, la expansión del comercio internacional estuvo condicionada por barreras físicas, tecnológicas y regulatorias, avanzando de forma progresiva y en oleadas asociadas a mejoras en el transporte y las comunicaciones. Por el contrario, el comercio de servicios digitales carece de estas limitaciones materiales, lo que ha permitido a las empresas tecnológicas escalar sus modelos de negocio de forma extremadamente rápida y operar de forma simultánea en múltiples mercados nacionales. Este rasgo refuerza la concentración de poder económico y tecnológico en un número limitado de actores —especialmente estadounidenses— capaces de explotar economías de escala globales.

Un segundo elemento novedoso se refiere a la transformación del concepto de seguridad inducido por el desarrollo tecnológico. Junto con los dominios tradicionales de la guerra —tierra, mar, aire y espacio— ha emergido un quinto dominio operativo: el ciberespacio, que incluye no solo los ataques a infraestructuras críticas, con un potencial creciente debido al incremento de la conectividad de múltiples dispositivos (*Internet of Things*), sino también la manipulación del espacio informativo o cognitivo.

En este ámbito, se desarrollan tanto operaciones defensivas como ofensivas capaces de afectar gravemente a la capacidad de actuación de los Estados. Estas acciones pueden tener un impacto material directo, al degradar o inutilizar sistemas militares, infraestructuras críticas o redes de mando y control, pero también un impacto psicológico y social, mediante campañas de desinformación, manipulación informativa y operaciones de influencia dirigidas a erosionar la cohesión social y la voluntad de resistencia de los gobernantes y de la población civil de un Estado, a menudo valiéndose de agentes de influencia o fuerzas políticas locales que amplifican dichos contenidos.

Los regímenes autoritarios, especialmente Rusia y China, han encontrado en la apertura y falta de regulación de las plataformas de redes sociales en Occidente un instrumento muy eficaz para afianzar su poder, tanto hacia dentro como hacia fuera. Como señaló la directora de los medios estatales rusos, Margarita Simonyan, *Russia Today*, *Sputnik* y la red global de medios rusos existen por la misma razón que existe el Ministerio de Defensa ruso: para librar la guerra informativa contra Occidente, creando y cautivando audiencias que, como evidenció de forma inmediatamente anterior a la invasión de Ucrania, puedan ser movilizadas en coyunturas críticas (Torreblanca, 2020).

La experiencia de EE. UU. durante las elecciones presidenciales de 2016 ilustra de forma clara el potencial desestabilizador de la combinación de operaciones que combinan los ciberataques y la desinformación. El asalto a los servidores del Partido Demócrata, sumado a la exposición masiva de la población —se calcula que hasta 136 millones de personas— a noticias falsas amplificaron la polarización política y las divisiones sociales internas (Taylor, Ewing y Johnson, 2018).

De manera similar, en el contexto europeo, a partir de 2014, con motivo de la primera invasión de Ucrania, Rusia se valió de la apertura de las redes sociales, de la debilidad de los medios de

comunicación tradicionales y de la vulnerabilidad de la opinión pública a la recepción de información falsa o sesgada para desencadenar campañas masivas de desinformación con el ánimo de debilitar y dividir a las democracias europeas.

Dichas injerencias fueron particularmente visibles durante procesos como el referéndum de 2016 sobre la permanencia del Reino Unido en la UE (Brexit), pero también en España. En nuestro país, los acontecimientos relacionados con el intento ilegal de secesión en Cataluña en 2017 pusieron de relieve cómo la amenaza exterior más grave a la soberanía nacional experimentada por España en su etapa democrática reciente no adoptó una forma militar convencional, sino que se materializó a través de una amplia operación de desinformación e influencia extranjera atribuida a Rusia. Con el objetivo de debilitar a la UE y a la OTAN alentando dentro de España un fenómeno similar a las revoluciones de colores y a las movilizaciones dentro de Rusia en favor de la democracia, que consideraba que Occidente había impulsado, Moscú creó un ecosistema completo de desinformación compuesto por medios oficiales, alianzas estratégicas con los independentistas, manipulación de las redes sociales y movilización de *proxies* con influencia tanto en la extrema derecha como izquierda (Alandete, 2017; Fernández, 2024; Schwirtz y Bautista, 2021 y Washington Post, 2017).

Los fenómenos de desinformación, que se acentuaron durante la pandemia, llevando a la OMS a hablar de una «infodemia», evidencian de qué manera la manipulación del espacio informativo puede tener consecuencias estratégicas comparables a las de los instrumentos militares tradicionales y cómo determinados actores pueden explotar estos instrumentos a su favor.

Un tercer elemento distintivo de la revolución tecnológica actual es el papel central de las empresas privadas de tecnología como proveedoras de servicios esenciales para la soberanía nacional. Si bien en etapas históricas anteriores sectores estratégicos como la banca, los seguros, el transporte ferroviario o la industria automovilística estuvieron frecuentemente en manos privadas, estos podían ser, al menos en teoría, replicados o nacionalizados por el Estado en situaciones de emergencia.

Durante la Segunda Guerra Mundial, por ejemplo, las capacidades industriales civiles fueron reconvertidas con relativa rapidez para fines militares, como ocurrió con la industria del automóvil y la aviación. En la actualidad, sin embargo, una parte sustancial

de las infraestructuras críticas que sustentan el funcionamiento de las economías avanzadas se encuentra en manos de empresas privadas, sin que el Estado disponga de la capacidad técnica, financiera o temporal para sustituirlas. Este es el caso de los servicios de computación en la nube, la fabricación avanzada de semiconductores, el despliegue y mantenimiento de cables submarinos de comunicaciones o las redes de satélites de órbita baja. Estas infraestructuras resultan cruciales tanto para la actividad económica como para las capacidades militares y de inteligencia, pero exceden ampliamente las capacidades productivas directas del sector público (Sánchez y Torreblanca, 2023).

El conflicto en Ucrania ha puesto de manifiesto esta nueva realidad. Empresas tecnológicas occidentales, particularmente estadounidenses, como Microsoft, Amazon o Starlink, han desempeñado un papel clave en el aseguramiento de las infraestructuras digitales críticas ucranianas, la provisión de servicios clave a sus Fuerzas Armadas, especialmente en lo relativo a la adquisición y procesamiento de datos, y en la mitigación de los ciberataques rusos. La fusión creciente entre el Pentágono estadounidense y determinadas empresas de *software* y servicios digitales especializados en el ámbito militar como es el caso de Anduril o Palantir, dibujan un escenario sumamente preocupante. Al igual que Eisenhower había alertado en 1953 sobre el poder de lo que denominó «complejo militar-industrial», esta preocupación por el poder estructural de las empresas privadas y su vinculación con la soberanía nacional llevó al presidente Biden a formular una advertencia similar en su despedida sobre el «complejo tecnológico-industrial» y las consecuencias para la democracia en EE. UU. y en el mundo de la enorme concentración de poder en manos de un reducido número de empresas tecnológicas (Biden, 2025; Bria, 2025).

Como se demostraría desde la toma de posesión del presidente Trump en enero de 2025 y en los meses siguientes, las grandes tecnológicas estadounidenses lograrían sin esfuerzo alguno que la Casa Blanca asumiera como propias sus agravios y demandas, de carácter histórico, contra la legislación europea en materia de servicios y mercados digitales, dando paso a un ataque frontal y una serie de coacciones abiertas contra la UE —también, por cierto, y de forma igualmente profunda, contra el Reino Unido—.

Todas estas transformaciones tienen implicaciones profundas para la seguridad internacional. Tradicionalmente, la evolución tecnológica y la doctrina militar tendían a avanzar de manera

más o menos sincronizada, lo que concedía a los Estados y a sus fuerzas armadas un margen temporal suficiente para adaptar sus estructuras organizativas, sus estrategias y sus industrias de defensa. En el contexto actual, sin embargo, el ritmo de innovación tecnológica supera con creces los ciclos de planificación, adquisición y despliegue de capacidades militares, cuyos horizontes temporales son necesariamente más largos. Como resultado, la aceleración tecnológica introduce niveles elevados de incertidumbre estratégica, dificultando la anticipación de amenazas y la formulación de doctrinas estables (Frías, 2024).

Henry Kissinger llamó la atención sobre esta problemática en una de sus últimas obras (Kissinger, Schmidt y Huttenlocher, 2021). El orden internacional posterior a la Segunda Guerra Mundial se vio estabilizado por la existencia del arma nuclear, que no solo estableció una jerarquía de poder clara y ampliamente reconocida, sino que permitió el desarrollo de una teoría de la disuasión racional, explícita y compartida; independientemente de las diferencias ideológicas entre los actores. La posesión de armas nucleares, medible y verificable, facilitó la previsibilidad estratégica.

En el caso de la inteligencia artificial, sin embargo, Kissinger advertía de que el intento de convertir esta tecnología en un vector de poder militar se enfrenta a un desafío fundamental: la dificultad de construir una teoría de la disuasión efectiva basada en una tecnología cuyos límites, capacidades y efectos permanecen en gran medida inciertos. A diferencia del arma nuclear, cuyo uso en la Segunda Guerra Mundial permitió la consolidación de una teoría y práctica de la disuasión e, incluso, el establecimiento de acuerdos de limitación y no proliferación, la inteligencia artificial podría resultar estratégicamente más eficaz como capacidad encubierta, susceptible de ser empleada de forma unilateral y sorpresiva para lanzar ataques preventivos. Esta característica incrementa la incertidumbre y eleva el riesgo de inestabilidad sistémica.

Si la inteligencia artificial constituye, como sugería Kissinger, el equivalente contemporáneo de un nuevo Proyecto Manhattan, el desafío central no reside únicamente en su desarrollo tecnológico, sino en la elaboración de un marco de disuasión y gobernanza internacional capaz de estabilizar su uso y evitar dinámicas de escalada incontrolada. Sin una teoría de la disuasión adaptada a esta nueva realidad tecnológica, el riesgo no es la ausencia de equilibrio, sino la generación de un orden internacional estructuralmente más inestable.

En una trayectoria histórica marcada por las interacciones entre tecnología y orden internacional, la inteligencia artificial, aunque está reconfigurando progresivamente las relaciones de poder y jerarquía entre los estados y el propio orden internacional en torno a una competición bipolar entre EE. UU. y China, que sin duda pueden ser calificados como «digitales» (Bradford, 2023), todavía no ha provocado una ruptura decisiva que permita definir de forma concluyente las nuevas características del poder global ni sus elementos de estabilidad o inestabilidad.

3 Desacoplamiento, guerra fría y esferas de influencia tecnológicas

El impulso geopolítico dominante en la actualidad se caracteriza por una securitización creciente de la tecnología. Los Estados ya no conciben la innovación tecnológica primordialmente como un factor de eficiencia económica o bienestar social, sino como un recurso estratégico de poder. En consecuencia, cada avance tecnológico es evaluado en función de dos criterios centrales: el poder relativo que puede conferir a terceros y el grado de vulnerabilidad estratégica que puede generar para el propio Estado (Torreblanca, 2021).

Esta lógica responde a un escenario en el que los Estados priorizan ganancias relativas sobre ganancias absolutas. La experiencia histórica demuestra que, cuando se impone esta lógica, los Estados están dispuestos a sacrificar crecimiento económico propio si ello contribuye a frenar, contener o ralentizar el desarrollo tecnológico y, por extensión, militar de sus rivales estratégicos. De forma paralela, buscan reducir los niveles de interdependencia considerados excesivos o peligrosos mediante estrategias de desacoplamiento selectivo, especialmente en sectores tecnológicos críticos.

Este marco analítico permite explicar tres dinámicas contemporáneas estrechamente vinculadas: uno, las restricciones impuestas por EE. UU. a la exportación de tecnologías avanzadas hacia China: dos; la aceleración de la estrategia china de autonomía tecnológica, y, tres, la insistencia de la UE en alcanzar la denominada soberanía digital.

El paralelismo histórico más inmediato se encuentra en la década de 1980, cuando la administración Reagan trató de impedir que la Unión Soviética accediera a tecnologías digitales de doble uso

con el objetivo de ralentizar su desarrollo económico y militar. Nos adentramos, pues, en una nueva guerra fría tecnológica con características propias, en la que el control, el acceso y la negación de mercados, datos y tecnologías críticas ocupan un lugar central en el debate político y estratégico.

La instrumentalización geopolítica de la tecnología y de la interconectividad digital ha generado disputas crecientes en torno a múltiples ámbitos estratégicos: infraestructuras digitales críticas (como las redes 5G y los cables submarinos), materias primas esenciales (incluidas las tierras raras), industrias clave (inteligencia artificial, computación en la nube, semiconductores), el control de los flujos y el almacenamiento de datos, así como la definición de estándares técnicos que condicionarán el desarrollo futuro de las tecnologías emergentes.

En este contexto, numerosos Estados han comenzado a levantar fronteras digitales, adoptando políticas de localización de datos, controles a la exportación de tecnologías sensibles y restricciones a la movilidad del talento científico (Ferracane, Marel y Lee-Makiyama, 2018). De forma simultánea, buscan construir esferas de influencia tecnológica con países considerados políticamente afines, con el objetivo de expandir y consolidar tanto su poder estructural como sus modelos regulatorios y tecnológicos.

Históricamente, las tecnologías asociadas a las grandes revoluciones —agrícola, industrial o de la información— tendieron a difundirse de forma relativamente generalizada una vez superada su fase inicial de desarrollo (Ding, 2024). Ningún Estado logró negar de manera sostenida a otros el acceso a tecnologías como el barco de vapor, la electricidad o, de manera más reciente, la energía nuclear para uso civil o, incluso, militar. Aun los intentos contemporáneos de limitar la proliferación nuclear de carácter militar han tenido un éxito parcial y limitado en el tiempo.

Durante la Guerra Fría, aunque el bloque occidental trató de restringir el acceso del bloque soviético a determinadas tecnologías, el ecosistema tecnológico global permaneció esencialmente unificado. Las principales potencias desarrollaron tecnologías militares comparables, con amplios procesos de copia, espionaje y adaptación. En contraste, el momento actual se caracteriza por una tendencia inédita hacia la fragmentación del sistema tecnológico internacional en al menos dos grandes bloques diferenciados e incompatibles entre sí: uno liderado por EE. UU. y otro encabezado por China.

EE. UU. ha sido pionero en el desarrollo de un ecosistema tecnológico integrado, capaz de cubrir prácticamente todas las capas críticas: desde infraestructuras espaciales y satelitales hasta cables submarinos, plataformas digitales, servicios en la nube y capacidades avanzadas de inteligencia artificial. Para alcanzar una autonomía tecnológica plena, Washington depende todavía de algunos cuellos de botella estratégicos, como la litografía avanzada para la fabricación de semiconductores —dominada por la empresa neerlandesa ASML— o la extracción y refinado de tierras raras, esenciales para las industrias tecnológica y de defensa, que China domina desde hace décadas.

China, por su parte, ha desplegado una estrategia deliberada y de largo plazo orientada a la autosuficiencia tecnológica. A través de la identificación temprana de sectores críticos y de inversiones masivas coordinadas por el Estado, a las que ha sumado una estrategia muy eficaz de espionaje industrial, Pekín ha logrado posicionarse por delante de EE. UU. en determinadas tecnologías estratégicas y reducir de forma significativa su dependencia externa. Aunque la fabricación de semiconductores avanzados sigue siendo su principal área de vulnerabilidad, China se encuentra en una trayectoria clara de convergencia tecnológica en este ámbito.

Como resultado, tanto EE. UU. como China están hoy en condiciones de ofrecer a sus socios y aliados soluciones tecnológicas integrales que excluyen, total o parcialmente, al bloque rival. De manera análoga a la construcción de una «gran muralla digital» en el mercado interno chino —mediante la exclusión de las principales empresas tecnológicas estadounidenses—, Pekín ha buscado ampliar su poder estructural creando su propia esfera de influencia tecnológica a escala internacional.

Estas dinámicas evocan el denominado «Gran Juego» del siglo XIX entre el Imperio británico y el Imperio ruso, en el que la competencia por áreas de influencia combinaba intereses estratégicos, económicos y tecnológicos. En el contexto actual, las alianzas tecnológicas permiten a las grandes potencias acceder a nuevos mercados, materias primas y flujos de datos, al tiempo que pugnan por imponer sus estándares técnicos y normativos a nivel global (Hobbs, Puddepath y Torreblanca, 2016, Financial Times, 2022).

Según los datos disponibles, China ha exportado tecnologías de vigilancia a más de sesenta países, entre ellos Irán, Myanmar,

Venezuela o Zimbabue, muchos de ellos con graves déficits en materia de derechos humanos (Feldstein, 2019). 36 de estos países forman parte de la Iniciativa de la Franja y la Ruta, lo que les facilita el acceso a financiación concesional para adquirir tecnologías de empresas chinas como Huawei, Hikvision, Dahua o ZTE. En otros ámbitos emergentes, como el *blockchain*, Pekín ha promovido iniciativas como la Blockchain-Based Service Network (BSN) con el objetivo de reconfigurar la arquitectura digital global y crear infraestructuras basadas en estándares definidos por China. A la vez que China exporta tecnología, importa materias primas críticas para asegurar su desarrollo tecnológico, dando lugar a una serie de relaciones extractivistas y de reprimarización económica que dibujan un nuevo colonialismo digital.

Las democracias liberales tampoco han permanecido al margen de estas dinámicas. Además de emplear y exportar tecnologías de vigilancia, han impulsado alianzas digitales orientadas a limitar la expansión del poder tecnológico chino. Un ejemplo significativo fue la *Clean Network Initiative*, promovida durante la primera administración Trump por el entonces secretario de Estado, Mike Pompeo, que buscaba incentivar a los aliados de EE. UU. a restringir el uso de tecnologías chinas y adoptar lo que se denominó infraestructuras «limpias» en ámbitos como redes, aplicaciones, nubes, cables y rutas de datos (BBC News, 2020).

Este grupo incluyó a los estados miembros de la UE, junto con aliados asiáticos como Japón, Israel, Australia, Canadá, India o Nueva Zelanda y latinoamericanos, y evocó explícitamente estrategias de contención propias de la Guerra Fría. De forma progresiva, tanto en Europa como en América Latina y otras regiones, numerosos países han comenzado a alejarse de proveedores chinos, considerados de «alto riesgo», mientras que China ha intensificado sus esfuerzos por sustituir tecnologías occidentales por soluciones domésticas en su propio mercado.

La competencia tecnológica también se manifiesta en el recurso creciente a operaciones de influencia extranjera, desinformación y ciberataques, que se han convertido en instrumentos centrales de la guerra híbrida contemporánea. Estas prácticas han incentivado a muchos Estados a reducir su nivel de interconexión digital e incluso a fragmentar Internet y sus bases industriales tecnológicas con el fin de limitar dependencias estratégicas.

En consecuencia, aunque la revolución tecnológica continuará avanzando, su trayectoria ya no estará guiada exclusivamente

por la lógica del mercado, los actores económicos privados o las instituciones multilaterales. Por el contrario, los Gobiernos han pasado a desempeñar un papel central, orientando el desarrollo tecnológico bajo criterios de seguridad nacional, competencia geopolítica y control estratégico, configurando un sistema internacional crecientemente fragmentado y competitivo. De la aspiración de una interconexión global se ha pasado, por tanto, a la realidad de la balcanización tecnológica, el desacoplamiento y la reducción de interdependencias y vulnerabilidades.

4 La UE: de superpotencia regulatoria a colonia digital

El papel de la UE en un sistema internacional crecientemente dominado por rivalidades tecnológicas resulta problemático en profundidad. Por su propia naturaleza como poder civil y normativo, la UE ha tendido históricamente a concebir la tecnología como un instrumento de prosperidad económica, cohesión social y ampliación de derechos, y no como un vector de poder geopolítico. Esta aproximación se ha traducido, sobre todo durante la última década, en una apuesta decidida por una gobernanza regulatoria de la tecnología centrada en la protección de derechos fundamentales, la competencia leal y la limitación de abusos de poder por parte de actores privados.

Esta estrategia ha otorgado a la Unión el calificativo de «superpotencia regulatoria», alimentando la expectativa de que pudiera consolidarse como un tercer polo tecnológico normativo, alternativo a los modelos estadounidense y chino. En esta visión, Europa aspira a convertirse en un espacio atractivo para aquellos Estados y sociedades que defienden un orden internacional basado en reglas, con un acceso relativamente abierto a la tecnología, donde esta no fuera una fuente de coerción estratégica o dependencia estructural, sino un multiplicador de desarrollo, inclusión y autonomía individual (Hobbs y Torreblanca, 2020).

Mediante el denominado «efecto Bruselas», la UE ha demostrado una notable capacidad para exportar sus normas regulatorias, especialmente en ámbitos como la privacidad y la protección de datos. Reglamentos europeos como el GDPR, que regula la privacidad de datos, llegaron a ser considerados el «patrón oro» de la regulación digital a escala global. El tamaño y el atractivo del mercado europeo permitieron que, incluso en ausencia de grandes plataformas digitales propias, las principales empresas tecnológicas estadounidenses operaran en Europa bajo estándares

significativamente más estrictos que los vigentes en EE. UU., donde la ausencia de una legislación federal integral en materia de privacidad ha generado un marco mucho más laxo y fragmentado (Bradford, 2020).

Sin embargo, la hipótesis implícita de que Europa podría beneficiarse de servicios digitales avanzados sin desarrollar capacidades industriales propias equivalentes se ha ido erosionando progresivamente a medida que la competencia geopolítica por la tecnología entre EE. UU. y China se ha intensificado.

En una primera fase, EE. UU. presionó con éxito a la UE para que se desacoplara tecnológicamente de China, de manera particular en sectores como las redes 5G, privando a los Estados miembros de alternativas tecnológicas relevantes. En una segunda, Washington comenzó a instrumentalizar la dependencia europea de la tecnología estadounidense para cuestionar las regulaciones europeas y tratar de obtener exenciones o reinterpretaciones favorables para sus empresas. Finalmente, a medida que la rivalidad sinoestadounidense se ha agudizado, Washington ha intensificado la presión sobre Bruselas para que alineara sus estándares regulatorios con los estadounidenses, calificando las normativas europeas de extraterritoriales, discriminatorias e incluso extorsionadoras.

Esta dinámica ha situado a la UE en una posición de vulnerabilidad estructural, al carecer de la capacidad material necesaria para evadir de forma creíble las coacciones tanto estadounidenses como chinas. La estrategia europea de desarrollar alternativas tecnológicas autóctonas en ámbitos como los semiconductores, la nube o la inteligencia artificial constituye una respuesta racional, pero extremadamente costosa en términos de tiempo, recursos financieros y coordinación política. En consecuencia, esta vía no permite garantizar una soberanía digital europea a corto plazo, obligando a la UE a operar durante un periodo prolongado bajo condiciones de dependencia estratégica.

Las presiones estadounidenses para que Europa rechazara la tecnología china se iniciaron durante la primera administración Trump, pero no solo continuaron, sino que se intensificaron durante la administración Biden, especialmente a través de la proliferación de controles a la exportación de tecnologías críticas hacia China. Según la caracterización del entonces consejero de Seguridad Nacional Jake Sullivan, EE. UU. construiría un «jardín pequeño con vallas altas» en el ámbito tecnológico

(The White House, 2023). Sin embargo, la inclusión en estas restricciones de las tres tecnologías más estratégicas del presente —inteligencia artificial, semiconductores y computación cuántica— evidenciaba que dicho «jardín» distaba mucho de ser reducido. Al contrario, significaba el lanzamiento de un desafío frontal a China.

Otro episodio revelador de la vulnerabilidad europea frente a EE. UU. ha tenido lugar con la decisión del Gobierno neerlandés, en respuesta directa a presiones estadounidenses, de obligar a la empresa ASML a cesar la exportación de máquinas de litografía ultravioleta extrema, indispensables para la fabricación de semiconductores avanzados Este caso ha puesto de manifiesto hasta qué punto incluso las escasas ventajas tecnológicas críticas europeas podían ser neutralizadas por decisiones políticas externas (Quin, 2024).

La dependencia europea de empresas tecnológicas privadas estadounidenses ha quedado aún más expuesta durante la guerra de Ucrania. En septiembre de 2022, Elon Musk ordenó restringir el acceso ucraniano al sistema de satélites de baja órbita Starlink, crucial para las comunicaciones militares ucranianas (Roulette, Bryan-Low y Balmforth, 2025). Musk justificó su decisión alegando el temor a una escalada nuclear. Este episodio evidenció los riesgos inherentes a que capacidades tecnológicas esenciales para la seguridad colectiva estén controladas por actores privados, capaces de influir de forma directa en dinámicas estratégicas de primer orden.

El caso Starlink supuso un punto de inflexión para la UE, al revelar de forma tangible las consecuencias de haber externalizado infraestructuras críticas a empresas privadas extranjeras. A este episodio se han sumado las crecientes invectivas de Musk contra la UE durante el ciclo electoral estadounidense, alineadas con las posiciones del entonces presidente Donald Trump y del movimiento MAGA. Estas posiciones fueron reforzadas por declaraciones del entonces senador J. D. Vance, quien llegó a cuestionar el compromiso estadounidense con Europa alegando una supuesta degradación de la calidad democrática europea debido a sus regulaciones digitales.

Tras su designación como vicepresidente de EE. UU., Vance elevó esta crítica a eje central de la política estadounidense hacia Europa en un controvertido discurso pronunciado en la Conferencia de Seguridad de Múnich de febrero de 2025, en el que sostuvo que la

principal amenaza para Europa no provenía de Rusia, sino de las restricciones internas a la libertad de expresión (Vance, 2025).

Ese mismo mes, el presidente Trump instruyó a sus secretarios de Comercio y del Tesoro a responder a lo que calificó como «extorsiones regulatorias» europeas, en referencia directa a la legislación sobre servicios y mercados digitales (The White House, 2025a). Se activaba así de forma explícita la alianza entre la Casa Blanca y las grandes empresas tecnológicas estadounidenses, visibilizada ya en la ceremonia de investidura de Trump, a la que asistieron los principales directivos de Silicon Valley. Figuras como Mark Zuckerberg han equiparado la regulación europea con sistemas de censura institucionalizados, comparables —según él— a los de China. Tanto Zuckerberg como Musk han desafiado abiertamente a la Unión, negándose a cumplir determinadas obligaciones relativas a la lucha contra la desinformación y los daños en línea en plataformas como X.

La interferencia directa de Musk en procesos políticos europeos, como su apoyo explícito a fuerzas antisistema como Alternativa para Alemania (AfD) durante las elecciones legislativas alemanas en febrero de 2025, ha generado un notable impacto político. No solo por respaldar a una fuerza extremista, sino por normalizar discursos que relativizaban el pasado histórico alemán, lo que ha sido percibido como una injerencia sin precedentes por parte de un actor privado extranjero.

Una nueva fuente de alarma ha emergido con la decisión de la administración Trump de imponer sanciones al Tribunal Penal Internacional tras la emisión de órdenes de detención contra el primer ministro israelí Benjamín Netanyahu, EE. UU. forzó a Microsoft a retirar servicios de correo electrónico al fiscal responsable del caso. La empresa cumplió la orden, evidenciando que, bajo la legislación estadounidense, las compañías deben acatar primero y litigar después, incluso cuando ello afecta a instituciones internacionales asentadas en Europa (Satariano y Smialek, 2025).

Este episodio ha puesto de relieve de forma inequívoca el riesgo sistémico derivado de la dependencia europea de servicios de computación en la nube estadounidenses. Aunque ha reforzado el interés por desarrollar infraestructuras de nube soberana europeas, también ha confirmado que dichas alternativas no estarían disponibles en el corto plazo, prolongando así la exposición europea a posibles coacciones políticas.

Por último, la publicación de la doctrina de seguridad nacional estadounidense en diciembre de 2025 ha confirmado los peores temores europeos, al legitimar abiertamente la instrumentalización de la superioridad tecnológica estadounidense con fines de transformación política en Europa. La estrategia estadounidense describe a Europa como víctima de una deriva ideológica antidemocrática y defiende la necesidad de promover el acceso al poder de fuerzas políticas alineadas con el trumpismo. El temor, desde la perspectiva europea, es que EE. UU. replique —mediante plataformas digitales privadas— tácticas de influencia similares a las empleadas previamente por Rusia, provocando un choque frontal transatlántico en materia de servicios digitales, soberanía regulatoria y democracia (The White House, 2025b).

En conjunto, estos episodios revelan que la UE se enfrenta no solo a un déficit de capacidades tecnológicas, sino a un desafío existencial en términos de soberanía y democracia, en un contexto en el que la tecnología ha dejado de ser un bien neutral para convertirse en un instrumento central de coerción geopolítica.

5 La construcción de la soberanía digital europea

La UE ha reconocido de forma explícita que la tecnología constituye una dimensión central de su seguridad y de su autonomía política (European Commission, 2023). La Comisión Europea surgida de las elecciones de junio de 2024 materializa este reconocimiento mediante la creación, por primera vez, de una vicepresidencia ejecutiva dedicada a la Soberanía Tecnológica, lo que marca un punto de inflexión en la concepción europea del poder en el siglo XXI.

Aunque el concepto de soberanía tecnológica no es unívoco —y resulta especialmente complejo en un contexto global caracterizado por interdependencias profundas y vulnerabilidades cruzadas—, las instituciones europeas lo utilizan para referirse a una idea concreta: la capacidad de la Unión para tomar decisiones digitales y tecnológicas de acuerdo con sus propios intereses y valores, sin estar sujeta a coacciones externas derivadas de dependencias críticas.

Desde esta perspectiva, garantizar la seguridad tecnológica europea exige actuar simultáneamente en tres planos complementarios: capacidades propias, resiliencia frente a la coacción y defensa del espacio democrático.

El primer pilar —inevitable, pero de largo plazo— consiste en desarrollar una base tecnológica e industrial europea en aquellos ámbitos donde la dependencia externa genera riesgos económicos o de seguridad. La carta de misión remitida por la presidenta de la Comisión, Úrsula von der Leyen, a la responsable de la nueva cartera identifica con claridad estos sectores: supercomputación, semiconductores, computación en la nube, inteligencia artificial, computación cuántica, tecnologías espaciales, Internet de las cosas y genómica (European Commission, 2024).

Sin capacidades propias en estos ámbitos, la UE carece de margen de maniobra real. La seguridad tecnológica no puede sostenerse exclusivamente sobre regulación si no existe una infraestructura material que permita ofrecer alternativas creíbles. No obstante, esta estrategia exige inversiones masivas, coordinación entre Estados miembros y una aceptación política explícita de que la política industrial constituye una necesidad insoslayable de seguridad nacional.

Dado que el desarrollo de estas capacidades llevará años, la UE necesita instrumentos de protección y disuasión a corto y medio plazo frente a la coacción tecnológica ejercida por terceros, incluidos sus aliados. La experiencia reciente demuestra que la dependencia europea de tecnologías y servicios digitales estadounidenses puede ser utilizada como palanca de presión política, regulatoria o incluso ideológica.

Para mitigar esta vulnerabilidad, la Unión debería adoptar una estrategia que, primero, utilizara estratégicamente la política comercial, recordando que EE. UU. mantiene un superávit estructural con la UE en servicios digitales; segundo, reforzara la política de competencia, reduciendo el poder de mercado —y por extensión político— de las grandes plataformas tecnológicas; tercero, avanzara en instrumentos fiscales comunes, indispensables para financiar inversiones tecnológicas estratégicas y evitar la captura regulatoria, y cuarto, explorara herramientas de seguridad nacional, incluidas cláusulas de preferencia europea o restricciones selectivas en sectores considerados críticos.

Estos instrumentos ya se han aplicado respecto a China, en particular para reducir la dependencia de las empresas de ese país sujetas a marcos legales que las obligan a cooperar con sus servicios de inteligencia. Dado que EE. UU. dispone de legislación con efectos extraterritoriales comparables, la UE debe comenzar a evaluar también el riesgo para su seguridad de su exposición

a empresas estadounidenses, especialmente en ámbitos como la nube, las plataformas digitales o las infraestructuras de datos.

Un tercer elemento de la seguridad tecnológica europea es la defensa de los procesos democráticos frente a la interferencia digital. La UE ha avanzado significativamente en este ámbito mediante la Ley de Servicios Digitales y la Ley de Mercados Digitales, así como con la aprobación del denominado «escudo democrático», que reconoce explícitamente los procesos electorales como infraestructuras críticas equiparables a las energéticas o de transporte

Esta aproximación es esencial en un contexto en el que plataformas digitales —ya sean estadounidenses o chinas— pueden ser utilizadas como vehículos de desinformación, manipulación informativa o apoyo indirecto a fuerzas políticas hostiles a la democracia. Garantizar la seguridad tecnológica implica, por tanto, garantizar la integridad del debate público, incluso frente a actores privados con capacidad de influencia sistémica.

Pese a su vulnerabilidad en otros ámbitos, la UE ha demostrado que no debe renunciar a su poder regulatorio. La aplicación efectiva de la legislación digital europea a las grandes empresas tecnológicas, incluidas las sanciones por incumplimiento, constituye uno de los pocos instrumentos de poder estructural de los que dispone la UE. Ceder en este terreno no reduciría la presión externa, sino que la aumentaría, al confirmar que la dependencia tecnológica puede traducirse en subordinación política. La firmeza regulatoria no es incompatible con la cooperación transatlántica, es, de hecho, una condición para que esta se base en relaciones más simétricas (Torreblanca, 2025).

En un mundo en el que solo existen dos grandes polos tecnológicos —EE. UU. y China—, la UE se enfrenta al riesgo de convertirse en una colonia digital si no actúa de forma decidida. Paradójicamente, su vulnerabilidad es hoy mayor frente a EE. UU. que frente a China, justo por la profundidad de la interdependencia existente. Garantizar la seguridad tecnológica europea exige, por tanto, una combinación de política industrial ambiciosa, instrumentos de defensa frente a la coacción, protección del espacio democrático y voluntad política sostenida. La soberanía tecnológica no es un fin en sí mismo, sino la condición necesaria para preservar el modelo político, económico y social europeo en un entorno internacional crecientemente competitivo y coercitivo.

Conclusión

La tecnología se ha convertido en un factor central del poder internacional, comparable al territorio, la población o los recursos estratégicos. La revolución tecnológica actual, caracterizada por su rapidez, su alcance global y el papel estructural de actores privados, está acelerando la securitización de la innovación y empujando al sistema internacional hacia una lógica de rivalidad, fragmentación y competencia entre bloques tecnológicos liderados por EE. UU. y China.

En este contexto, la UE ocupa una posición ambivalente. Su fortaleza como potencia regulatoria le ha permitido influir en la gobernanza digital global, pero la falta de capacidades industriales propias en tecnologías críticas la expone a dependencias que se traducen ya hoy en una extrema vulnerabilidad ante coacciones externas.

La regulación, por sí sola, no es suficiente para defender la soberanía europea en un entorno geopolítico crecientemente hostil. Garantizar la seguridad tecnológica europea exige, por tanto, una estrategia integrada que combine política industrial a largo plazo, instrumentos de resiliencia y disuasión frente a la coacción tecnológica y una protección reforzada del espacio democrático frente a injerencias digitales. La soberanía tecnológica es la condición necesaria para preservar la capacidad de decisión, el modelo democrático y la autonomía estratégica de la UE en el orden internacional del siglo XXI.

Bibliografía

Alandete, D. (2017). La trama rusa empleó redes de chavistas para ganar influencia en Cataluña [en línea]. *El País*. [Consulta: 15 enero 2026]. Disponible en: https://elpais.com/politica/2017/11/10/actualidad/1510341089_316043.html

Allison, G. (2017). *Destined for War: Can America and China Escape Thucydides's Trap?* Houghton Mifflin Harcourt.

BBC News. (2020). Huawei ban: UK to impose early end to use of new 5G kit [en línea]. BBC News. [Consulta: 15 enero 2026]. Disponible en: https://www.bbc.com/news/business-55124236

Biden, J. (2025). President Biden's Farewell Address. The White House, 15 January [en línea]. The White House. [Consulta:

15 enero 2026]. Disponible en: https://www.presidency.ucsb.edu/documents/farewell-address-the-nation-4

Bria, F. (2025). El golpe de Estado de los tecnoautoritarios: de la América postdemocrática a la Europa que viene [en línea]. *La Vanguardia*. [Consulta: 15 enero 2026]. Disponible en: https://www.lavanguardia.com/internacional/20251102/11220880/golpe-tecnoautoritarios-america-postdemocratica-europa-viene.html

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

—. (2023). *Digital empires: The battle for global tech dominance*. Nueva York, Oxford University Press.

Ding, J. (2024). *Technology and the Rise of Great Powers: How Diffusion Shapes Economic Competition*. Princeton University Press.

European Commission. (2023). Joint Communication to the European Parliament, the European Counciland and the Council on "European Economic Security Strategy" (JOIN/2023/20 final) [en línea]. European Commission. [Consulta: 15 enero 2026]. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0020

—. (2024). Mission Letter from Ursula Von der Leyen, President of the European Commission, to Henna Virkkunen, Executive Vice-President-designate for Technological Sovereignty, Security and Democracy [en línea]. European Commission. [Consulta: 15 enero 2026]. Disponible en: https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf

Feldstein, S. (2019). *The Global Expansion of AI Surveillance* [en línea]. CEIP. [Consulta: 15 enero 2026]. Disponible en: https://carnegieendowment.org/research/2019/09/the-global-expansion-of-ai-surveillance?lang=en

Fernández, J. J. (2024). El ejército identifica un ecosistema de influencia rusa en España con 179 altavoces. *El Periódico*. [Consulta: 15 enero 2026]. Disponible en: https://www.elperiodico.com/es/politica/20240718/ejercito-ecosistema-desinformacion-ruso-espana-altavoces-105779287

Ferracane, M. F., Marel, Erik van der y Lee-Makiyama, H. (2018). *Digital Trade Restrictiveness Index* [en línea]. Bruselas, European Centre for International Political Economy (ECIPE).

[Consulta: 15 enero 2026]. Disponible en: https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf

Financial Times. (2022). US hits China with sweeping tech export controls [en línea]. *Financial Times*. [Consulta: 15 enero 2026]. Disponible en: https://www.ft.com/content/6825bee4-52a7-4c86-b1aa-31c100708c3e

Frías, C. (2024). "Rusia, Ucrania y el campo de batalla 'transparente'". Documento de Opinión 18/2024 del Instituto Español de Estudios Estratégicos (IEEE). Disponible en: https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO18_2024_CARFRI_Rusia.pdf [Consulta: 15 de enero de 2026].

Headrick, D. R. (1979). *Los instrumentos del imperio: tecnología y colonialismo europeo en el siglo XIX*. Madrid, Alianza**.**

Hobbs, C., Puddephat, A. y Torreblanca J. I. (2016). The Geoeconomics of the Digital. En: Leonard, M. (ed.). *Connectivity Wars: Why Migration, Finance and Trade and the Geo-Economic Battlegrounds of the Future* [en línea]. European Council on Foreign Relations. [Consulta: 15 enero 2026]. Disponible en: https://ecfr.eu/archive/page/-/Connectivity_Wars.pdf

Hobbs, C. y Torreblanca, J. I. (2020). *La soberanía digital de Europa*. Madrid, Catarata.

Hu, K. (2023). ChatGPT sets record for fastest-growing user base in history [en línea]. *Reuters*. [Consulta: 15 enero 2026]. Disponible en: https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/

Kissinger, H. A., Schmidt, E. y Huttenlocher, D. (2021). *The Age of AI: And Our Human Future*. Little, Brown and Company.

Leonard, M. (2021). *The Age of Unpeace: How Connectivity Causes Conflict*. Bantam Press.

Qin, S. (2024). ASML Cancels Some Shipments to China at Biden Administration's Request [en línea]. *The Wall Street Journal*. [Consulta: 15 enero 2026]. Disponible en: https://www.wsj.com/tech/netherlands-blocks-asml-exports-of-some-chip-making-equipment-to-china-2fe4a162

Roulette, J., Bryan-Low, C. y Balmforth, T. (2025). Musk ordered shutdown of Starlink satellite service as Ukraine retook territory from Russia [en línea]. *Reuters*. [Consulta: 15 enero 2026]. Disponible en: https://www.reuters.com/

investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/

Sánchez, I. y Torreblanca, J. I. (2023). Ukraine one year on: When tech companies go to war [en línea]. European Council on Foreign Relations. [Consulta: 15 enero 2026]. Disponible en: https://ecfr.eu/article/ukraine-one-year-on-when-tech-companies-go-to-war/

Satariano, A. y Smialek, J. (2025). Europe's Growing Fear: How Trump Might Use U.S. Tech Companies Against Europe [en línea]. *New York Times*. [Consulta: 15 enero 2026]. Disponible en: https://www.nytimes.com/2025/06/20/technology/us-tech-europe-microsoft-trump-icc.html

Schwirtz, M. y Bautista, J. (2021). Married Kremlin Spies, a Shadowy Mission to Moscow and Catalonia [en línea]. *New York Times*. [Consulta: 15 enero 2026]. Disponible en: https://www.nytimes.com/2021/09/03/world/europe/spain-catalonia-russia.html

Taylor, J, Ewing, P. y Johnson, C. (2018). Grand Jury Indicts Russians Linked To Interference In 2016 Election [en línea]. *National Public Radio*. [Consulta: 15 enero 2026]. Disponible en: https://www.npr.org/2018/02/16/586500591/grand-jury-indicts-russians-linked-to-interference-in-2016-election

Torreblanca, J. I. (2020). Democracia y redes sociales. En: Lapuente, V. y Costas, E. (eds.). *Cómo salvar las democracias liberales* [en línea]. Madrid, Círculo de Empresarios, pp. 131-150. [Consulta: 15 enero 2026]. Disponible en: https://circulodeempresarios.org/app/uploads/2020/06/Libro-Democracias-Liberales-OK-paginas.pdf

—. (2021). Technology. En: Leonard, M. y Krastev, I. (eds.). *The Power Atlas: Seven Battlegrounds of a network world* [en línea]. European Council on Foreign Relations. [Consulta: 15 enero 2026]. Disponible en: https://ecfr.eu/wp-content/uploads/power-atlas.pdf

—. (2025). Big tech, Donald Trump, and techno-imperialism: How Europe can avoid becoming a digital colony [en línea]. European Council on Foreign Relations. [Consulta: 15 enero 2026]. Disponible en: https://ecfr.eu/article/big-tech-donald-trump-and-techno-imperialism-how-can-europe-avoid-becoming-a-digital-colony

Vance, J. D. (2025). Speech by J.D. Vance. J.D. Vance (Vice President, United States of America) talking about "The U.S. in the World"

[en línea]. Munich Security Conference. [Consulta: 15 enero 2026]. Disponible en: https://securityconference.org/en/medialibrary/asset/the-speech-of-jd-vance-20250214-1817/

Washington Post. (2017). Catalonia held a referendum. Russia won. October 2, 2017. Disponible en: https://www.washingtonpost.com/opinions/global-opinions/catalonia-held-a-referendum-russia-won/2017/10/02/f618cd7c-a798-11e7-92d1-58c702d2d975_story.html

The White House. (2023). Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership at the Brookings Institution [en línea]. The White House. [Consulta: 15 enero 2026]. Disponible en: https://www.presidency.ucsb.edu/documents/remarks-national-security-advisor-jake-sullivan-renewing-american-economic-leadership-the

—. (2025a). Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties [en línea]. The White House. [Consulta: 15 enero 2026]. Disponible en: https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/

—. (2025b). *National Security Strategy of the United States of America* [en línea]. Washington, DC, The White House. [Consulta: 15 enero 2026]. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf