MONOGRAFÍAS
DE LA
REAL ACADEMIA DE DOCTORES DE ESPAÑA

ANÁLISIS DE LA AUTONOMÍA ESTRATÉGICA ABIERTA DIGITAL DE LA UE. RETOS TECNOLÓGICOS Y GEOPOLÍTICOS EN UN MUNDO CONVULSO

Dr. D. Gonzalo León Serrano

Vol. 1 • Número 1• 1ª Etapa • 2024 • Paginas 1-206

REAL ACADEMIA DE DOCTORES DE ESPAÑA
San Bernardo, 49. 28015 Madrid 915319522
www.rade.es secretaria@rade.es publicaciones@rade.es

MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

Editor:
Real Academia de Doctores de España
San Bernardo, 49. 28015 Madrid
www.rade.es secretaria@rade.es publicaciones@rade.es

ISSN Monografías de la RADE (Internet): 3020-6421
ISSN Monografías de la RADE (Ed. Impresa): 3020-6413

ISBN: 978-84-124810-4-4
Depósito Legal: M-4574-2024

Madrid, 6 de marzo de 2024

Obra producida en el ámbito de la subvención concedida a la Real Academia de Doctores de España por el Ministerio de Ciencia, Innovación y Universidades

ÍNDICE

PRÓLOGO

JOSÉ RAMÓN CASAR CORREDERA

Académico de Número y Presidente de la Sección de Ingeniería de la Real Academia de Doctores de España

Tiene el lector ante sus ojos una monografía rigurosa y evocadora, salida de la reflexión intensa del profesor Gonzalo León Serrano, Académico de nuestra Real Academia de Doctores de España, cuyos conocimientos sobre la Unión Europea (UE) en el contexto mundial, y sobre la tecnología, adquiridos durante muchos años de dedicación universitaria y en las Administraciones, no podían plasmarse de mejor manera.

Aborda el profesor León Serrano el concepto de autonomía estratégica desde la perspectiva de la Europa actual en el panorama mundial, en el que las relaciones de influencia de los viejos y emergentes actores cambian el escenario geopolítico por momentos. Lejos de proponer una autarquía imposible, propone, como la Comisión Europea, una autonomía abierta, en la que la soberanía propia debe hacerse compatible con la colaboración con otros socios fiables.

Desde la reflexión de que Europa es un gigante regulatorio con escasa soberanía industrial, militar y energética, desgrana la teoría, sobre la que hemos tenido ocasión de debatir en al menos dos sesiones en nuestra Real Academia (el 30 noviembre 2022 y el 29 de noviembre de 2023), de que son las tecnologías las que pueden dotar a la UE (y a otros actores) de unas deseables autonomía, independencia y seguridad. Es el paradigma de soberanía tecnológica, que esta Monografía hace pivotar principalmente (que no exclusivamente) alrededor de las tecnologías "digitales", especialmente de la Microelectrónica y la Inteligencia Artificial.

En el capítulo 2, dedicado principalmente a aspectos de la autonomía tecnológica digital, revisa, a modo de ejemplo, algunos ejemplos clave con impacto geopolítico demostrable, como son: la capacidad de acceder a "tierras raras" para fabricar productos electrónicos, las nuevas tecnologías de comunicaciones 5G (y 6G), el desarrollo y protección de los cables de datos submarinos (y los sistemas de satélites), los sistemas de supercomputa-

ción y de tratamiento masivo de datos, las plataformas para el acceso a servicios digitales y la ciberseguridad.

En el capítulo 3, la Monografía aborda algunas de las facetas que componen el diseño de una estrategia factible para la UE y propone un modelo multinivel genérico para considerar las posibles prioridades de intervención política, potencialmente en función del grado de autosuficiencia tecnológica. Los diversos niveles se agrupan en tres, a saber: nivel 1: Recursos naturales e infraestructuras de procesamiento y transporte, nivel 2: Investigación, innovación, educación y fabricación, y nivel 3: Marco regulatorio, mercado y principios y valores compartidos. Luego el capítulo se centra en la relevancia de las Tecnologías de Semiconductores y de Inteligencia Artificial en la Unión Europea, incluyendo sus aspectos geopolíticos. Finalmente, el capítulo incluye una revisión (comparada) y una reflexión sobre la Gobernanza y la Regulación, especialmente en el campo, ya más que emergente, de la Inteligencia Artificial. En ese ámbito, estamos de acuerdo, creo, el profesor León y yo mismo en que entre la Autorregulación y la Regulación Defensiva, se debiera encontrar un punto de justo equilibrio regulatorio, que preservara los derechos de los ciudadanos, pero también que permitiera progresar en las oportunidades para esos mismos ciudadanos, desde la afirmación de la autonomía estratégica de Europa frente a otros actores globales.

El capítulo 4 aborda el problema de la digitalización de la Defensa, sus recursos y escenarios, como parte integral de los objetivos de autonomía estratégica y soberanía de nuestro actual y futuro modelo organizativo. El contexto OTAN, los exiguos presupuestos, los nuevos recientes conflictos en la frontera este de Europa, los intereses industriales nacionales, y el siempre presente debate entre nacionalización y globalización (incluso a nivel europeo) son factores que condicionan la "reafirmación de la autonomía estratégica digital abierta".

Finalmente, en el Capítulo 5, la Monografía recoge una colección de grandes propuestas, que van desde lo tecnológico a lo regulatorio y desde las posibles y deseables alianzas con otros actores a la reformulación de las cadenas de suministro, especialmente de materiales y servicios críticos. Y ello en la UE, pero también en España. Creo saber que más que formular soluciones definitivas, el objetivo del profesor León Serrano con estas propuestas o recomendaciones es el de propiciar una reflexión colectiva sobre los posibles ámbitos de actuación y las posibles iniciativas, algunas de ellas urgentes, sin duda.

En cualquier caso, lo nuclear de esta Monografía europeísta está en la insistente reflexión sobre el valor estratégico de la tecnología en la consecución de la autonomía ciudadana y en la preservación del bienestar y de

determinados valores y principios. Este objetivo está muy lejos de coincidir o incluso de alinearse con un objetivo regulatorio puro, al que son tan proclives nuestras instituciones. Como dice Roderick Parkes, director del Instituto de Investigación del DGAP, "producir normas no compensa no producir cosas".

Termino esta ya larga presentación, agradeciendo al profesor León el esfuerzo intelectual y personal invertido en producir esta Monografía y felicitándole por el resultado y valor impagable que tienen sus reflexiones y propuestas, que, generosamente, pone a disposición de todos nosotros.

PREFACIO

No hay duda de que vivimos en un **tiempo convulso** en el que la sociedad se enfrenta a múltiples problemas para los que no existe una solución sencilla. Un tiempo al que se le puede calificar simultáneamente de "*volátil, incierto, complejo y ambiguo*" (denominado conjuntamente "VUCA" por sus siglas en inglés, término heredado de la escuela de Guerra de Estados Unidos), pero en el que **debemos adoptar decisiones difíciles** para preservar nuestros principios y valores que comprometen nuestro futuro y el de las generaciones venideras.

Desde el comienzo del presente siglo XXI se han sucedido múltiples **crisis provocadas por acontecimientos inesperados que tenían un impacto sistémico** y ante las que los ciudadanos, gobiernos e instituciones multilaterales no estaban preparadas para responder eficazmente. En mi opinión, algunas de estas crisis correspondían más que a "*cisnes negros*" (metáfora debida a *Nassim Taleb* ampliamente utilizada)[1] totalmente inesperados puesto que diversos informes sí los habían anticipado, a eventos del tipo denominado "*rinocerontes grises*" (metáfora posterior debida a *Michele Wucker*)[2] que "todo el mundo" veía pastar tranquilamente a cierta distancia sin que se les hiciese mucho caso… hasta que embistieron contra la sociedad.

Algunos de esos **rinocerontes grises del siglo XXI** embistieron en la Unión Europea (UE) en el transcurso de pocos años. Un breve repaso de la historia reciente europea nos señala algunos de ellos: la crisis económica global de 2008, la anexión de Crimea por Rusia en 2014, el BREXIT tras el referéndum celebrado en el Reino Unido en junio de 2016, la aceleración del cambio climático con su secuela de inundaciones y sequias en muchos países europeos y ya con un impacto muy visible y creciente en millones de ciudadanos desde 2018, la pandemia COVID-19 desatada en Europa en

1 Nassim Taleb, 2007 "*El Cisne Negro: El Impacto de lo Altamente Improbable*".

2 Michele Wucker, 2016 "*El rinoceronte gris: cómo reconocer y actuar sobre los peligros evidentes que ignoramos*".

2020 por el virus SARS-COV2, la progresiva fragilidad de las cadenas de valor de productos manufacturados agravada por el paulatino proceso de "desacoplo" parcial de Estados Unidos con China en los tres últimos años y su efecto dominó en la política y economía de la UE, las sucesivas crisis migratorias provocadas por conflictos armados o de raíz económica en el Mediterráneo y este de Europa frente a las que la UE no ha sido capaz de ofrecer una respuesta coordinada a largo plazo, o la invasión de Ucrania por Rusia en febrero de 2022. Al escribir estas líneas se reproduce el conflicto entre Israel y el pueblo palestino en la franja de Gaza tras el ataque a Israel por Hamás con riesgo de expansión a otras zonas que, seguramente, también afectará a la UE.

Todos ellos **se gestaron durante muchos años antes de estallar en la UE o en sus fronteras** sin recibir la atención política y social debida pensando en que el riesgo de que sucedieran con alta intensidad sería bajo o, desde una visión tecno-optimista que los instrumentos científicos y tecnológicos, políticos, económicos, o militares disponibles en la UE serían suficientes para hacerles frente… sin afectar demasiado a nuestro modo de vida. La historia ha demostrado repetidamente que no era así.

En ese mundo tan convulso como el dibujado, la UE, ese "*objeto político no identificado*" como le denominaba Jacques Delors, antiguo presidente de la Comisión Europea, ha supuesto, sin embargo, para los europeos un avance extraordinario de paz, estabilidad y desarrollo económico y social tras los terribles acontecimientos acaecidos en suelo europeo durante la primera mitad del siglo XX. Personalmente, estoy convencido de su inmenso valor y de la necesidad de profundizar en su fortalecimiento. Lo mantengo desde el convencimiento de que, a pesar de sus múltiples defectos y problemas, algunos de ellos vividos en primera persona, **el esfuerzo de la construcción europea ha valido y seguirá valiendo la pena**.

Por ello, **me siento obligado a luchar por su fortalecimiento** y convencer a europeos más jóvenes que dan por sentada su existencia o que se desentienden de los avatares de la Unión, a pesar de beneficiarse todos los días de ella, de que nada está conseguido para siempre y que deben implicarse en su defensa por su propio futuro. Hacer pedagogía a favor de la UE, de las raíces de sus principios y valores, de lo que ha supuesto de marco para trascender las fronteras nacionales y regionales y ampliar el horizonte me ha ocupado en los últimos treinta años desde la docencia y desde las diversas responsabilidades políticas e institucionales que he tenido. Quiero creer que los más de 320 viajes que he realizado a Bruselas deben significar algo.

Es verdad que asegurar actualmente el papel de la UE en el mundo exige algo más que palabras y deseos. Desde finales del siglo pasado **vivimos**

en una sociedad tecnológica en la que el despliegue de la tecnología juega un papel fundamental en nuestra vida diaria; de hecho, la sociedad depende del correcto funcionamiento de sistemas tecnológicos muy complejos, aunque el ciudadano no sea plenamente consciente de ello y de la veracidad de la información que corre por las venas mediáticas de la sociedad. En todos los eventos de tipo de "*rinocerontes grises*" mencionados anteriormente la ciencia y la tecnología ha jugado un papel de decisivo en su desencadenamiento, en su desarrollo y, en varios casos, en su solución, como el ejemplo del COVID-19 y el desarrollo de las vacunas ha demostrado.

Nos enfrentamos, además, a un cambio tecnológico de la mano del proceso de digitalización y su convergencia con otras tecnologías emergentes que es, a la vez, profundo y disruptivo. Tras él se producen no solo cambios en la sociedad con la adopción de nuevos modelos económicos y de relaciones humanas, sino también un **reposicionamiento de los países en el contexto internacional** con la emergencia de nuevas potencias tecnológicas, con un grado de interdependencia entre países muy acusado, y con ganadores y perdedores en esa batalla tecnológica de la globalización en la que la información se crea, se transmite y se consume sin saber realmente si es cierta y si alguien se responsabiliza de ello.

Las grandes potencias actuales son conscientes de que **la supremacía mundial en los próximos años se va a jugar en el terreno tecnológico y en la forma en la que la tecnología se controla y se usa**; por ello hacen o deberían hacer el máximo esfuerzo para dominar este nuevo terreno de juego global digitalizado. Dicho de otra manera: l**os "imperios" del siglo XXI serán tecnológicos o no podrán mantenerse como tales**.

Este análisis y mi propia predisposición personal me ha llevado a reflexionar sobre la manera en la que la UE podría **fortalecer su papel** en un mundo en el que los **conflictos geopolíticos** han adquirido una dimensión muy relevante desde la perspectiva del desarrollo tecnológico y la digitalización. En un contexto en el que **casi todo es susceptible de convertirse o interpretarse como un arma** (un proceso de largo alcance hacia la "*weaponization*" de la sociedad); obviamente, el desarrollo, acceso y uso de tecnologías digitales avanzadas también lo es.

El presente documento es, por tanto, una visión personal de esos conflictos geopolíticos marcados por la digitalización y de la forma en la que la UE debería abordarlos si apuesta, como yo lo deseo, en **mantener o incrementar su relevancia global en el futuro como medio de asegurar el mejor escenario posible para los ciudadanos europeos**.

He pretendido elaborar este informe también de un **modo realista**; los deseos no pueden ocultar las realidades ni las limitaciones existentes para

cambiarlas. En el proceso de toma de decisión tenemos que preservar la visión de que los europeos no estamos solos, de que las visiones autárquicas son imposibles, de que nuestra demografía decrece porcentualmente de forma imparable en relación con la población mundial por lo que nuestro mercado interior se empequeñece, y de que **otros países están corriendo más deprisa que la UE para posicionarse mejor en la batalla tecnológica global**.

Nos va a costar mantener en el futuro el peso actual de la UE, no digo ya recuperar la relevancia pasada. No contribuye a ello para nada esa v**isión eurocéntrica del mundo** que las autoridades comunitarias y los países miembros de la UE siguen teniendo o transmiten a los ciudadanos. **Necesitamos aliados tecnológicos estables**.

El presente informe se ha redactado desde una visión que conjuga el rápido desarrollo y despliegue de las tecnologías digitales, muchas de ellas sin liderazgo europeo, con los esfuerzos comunitarios **en desarrollar un marco europeo** de valores y principios compartidos, de desarrollo científico y tecnológico, de leyes y regulaciones centradas en la persona. Se trata de una **estrategia eminentemente defensiva para la que la UE está bien entrenada**, peo que conlleva dudas de si será suficiente.

A lo largo de las páginas del informe he desgranado algunos de los **puntos de fricción geopolítica ligados a la digitalización** que me han parecido más relevantes. Todos ellos afectan en mayor o menor medida a ese concepto poco definido de la **autonomía estratégica digital abierta de la UE**, que se exhibe junto a otro concepto de **soberanía tecnológica**, que, en mi opinión, no es posible ni deseable entendido de manera absoluta. Como se analiza en el informe no en todos los puntos de fricción geopolítica identificados la UE ha sido capaz de mantener una postura propia independiente e influyente en el comportamiento de otros actores mundiales.

En mi opinión, **no basta con realizar un análisis de la situación actual de la autonomía estratégica digital de la UE; debemos realizar un ejercicio de su proyección en los próximos años**, aun a sabiendas de que aparecerán nuevos rinocerontes grises que nos embestirán en el futuro. No existe una receta mágica, pero sí he hecho el esfuerzo de identificar algunas **recomendaciones** que deberían servir, a mi juicio, para enmarcar la evolución de las políticas digitales de la UE, y de España en particular. Al menos, deben servir de base para **alimentar un debate en profundidad** que permita mejorar nuestra autonomía estratégica.

Referido exclusivamente al ámbito digital la f**eroz competencia actual** planteada por Estados Unidos, China y, en menor medida, por otros actores asiáticos, en el ámbito de los semiconductores, la inteligencia arti-

ficial, los sistemas de navegación satelital, las constelaciones de nanosatélites, las comunicaciones móviles 5G, o las plataformas digitales, por citar algunas de ellas, no se solucionan con actuaciones enmarcadas en el plano nacional: requieren **planteamientos paneuropeos** decididos, coherentes, y a largo plazo. Somos demasiado pequeños y pocos para actuar aisladamente. Los países **ganadores de la siguiente revolución tecnológica digital en ciernes**, desde las tecnologías de comunicaciones y computación cuánticas a la nueva generación de comunicaciones móviles (6G) o la neurotecnología se están dirimiendo ahora, durante la presente década; y lo hacen en el contexto de alianzas globales.

Termino reafirmando mi convencimiento de que la UE necesita, una vez más, asumir la necesidad de **repensar y actualizar sus estructuras de gobernanza colectivas para reforzar sus posicionamientos globales ante terceros países y organismos multilaterales**. Es triste que tengan que ocurrir crisis como la derivada de la invasión de Ucrania por Rusia para que la UE actúe con una voz "casi única", y no sé por cuanto tiempo.

En un momento crítico en el que se abre un nuevo **proceso de expansión de la UE hacia las fronteras del este de Europa**, aunque sea un camino largo y no necesariamente culminará de forma exitosa para todos como demuestra el caso de Turquía, la **distribución competencial entre los estados miembros y las instituciones comunitarias en una sociedad digitalizada** requiere disponer de un nuevo marco de actuación que obliga, a mi juicio, a repensar el Tratado de la Unión. ¿Seremos capaces de encontrar el camino para ello?

Corresponderá a todos nosotros, **ciudadanos europeos**, pensar qué Europa digitalizada queremos construir y decidir la mejor forma de conseguirlo. En ello **está en juego la relevancia de la UE** que deseemos legar a la siguiente generación.

Gonzalo León
Colmenar Viejo, octubre 2023

1

INTRODUCCIÓN

1.1. CONCEPTOS BÁSICOS Y CONTEXTO HISTÓRICO

La creación y desarrollo de la **Unión Europea** (UE) desde sus antecedentes históricos de 1951 con la firma del Tratado de la *"Comunidad Europea del Carbón y del Acero (CECA)"* y, sobre todo, desde 1957 con la firma de *los Tratados de Roma* para crear la denominada en esa época "*Comunidad Económica Europea (CEE)*"[3] de seis miembros hasta la actualidad, ha sido considerada un factor clave para fundamentar el desarrollo socioeconómico de sus estados miembros, apuntalar la democracia y el estado del bienestar, y servir de **base para potenciar su papel en el mundo.**

Con la creación de la CEE, y de forma progresiva, los países miembros se dotaron de un **mercado integrado (común) sometido a un conjunto de principios y valores compartidos**; su desarrollo, modificando varias veces los tratados constituyentes de 1957, ha contribuido a la (lenta) construcción de una **identidad europea** apoyada en la **transferencia de competencias soberanas de los estados miembros**[4], algunas de ellas compartidas por un grupo concreto de los miembros de la UE como la construcción de la zona euro o la movilidad transfronteriza (Schengen), hasta lo que ha llegado a ser la actual UE con veintisiete estados miembros. Todo ello supone la construcción de un **modelo único en el mundo, pero no sencillo de gobernar.**

Con su desarrollo progresivo a lo largo de varios decenios, los estados

3 También se firma en esa fecha el Tratado EURATOM creando la comunidad europea de energía nuclear. El Tratado sigue en vigor.

4 El modelo de transferencias de soberanía nacional a los órganos comunitarios se superpone a otras competencias que se mantienen de forma exclusiva por los diferentes estados-nación, junto a otras competencias denominadas "compartidas", en las que tanto la actual Unión como los estados miembros pueden actuar. Este esquema obliga a alinear, como se verá en el ámbito digital durante el presente informe, las políticas comunitarias con las de los estados miembros para optimizar su eficacia.

miembros de lo que llegó a constituirse como la UE buscaban asentarse en el mundo reforzando su **posición estratégica global**, definiendo y manteniendo posturas propias en defensa de sus intereses y valores, concepto no alejado del de **"autonomía estratégica"** empleado hoy día y que se analizará posteriormente.

Las sucesivas **ampliaciones de la UE** desde los seis países iniciales firmantes de los Tratados de Roma a los veintisiete actuales, han supuesto un incremento del volumen de población conjunta, alcanzando los 450 millones de habitantes, y de territorio físico con una fuerte expansión geográfica hacia el Este de Europa, factores clave de la **fortaleza de su mercado interior**. El interés manifestado a lo largo de los años por otros países europeos en formar parte de la UE procedía de su visión de la UE como una comunidad fundamentada en el **respeto a la democracia y a los derechos humanos** que, a su vez, avalaba la permanencia de un contexto de estabilidad socioeconómica prolongada en el tiempo que alejaba los conflictos intraeuropeos de la primera mitad del siglo XX.

La actual lista de **países candidatos** con los que la UE ha acordado el comienzo de negociaciones formales de adhesión[5], incluso en periodos turbulentos como los actuales, explica esta visión del **valor de la integración en la UE de otros países** más allá del mero interés económico en acceder al mercado europeo o a sus programas de ayuda financiados por el presupuesto comunitario, sino también por lo que supone la defensa y fortalecimiento de un conjunto de **principios y valores democráticos** que se convirtió en un **criterio esencial en el proceso de expansión y que la UE intenta proyectar al resto del mundo.**

Además, la UE ha firmado con otros muchos países **acuerdos bilaterales** para su consideración como **países asociados a la UE** empleando diversos modelos y temáticas de asociación que, globalmente, han permitido incrementar la presencia y la influencia de la UE en el mundo, pero también visibilizar sus límites. Algunos de estos países están situados en el corazón de Europa como son Suiza y Noruega; otros como Israel, país clave por su posición geográfica en la frontera oriental, o Turquía, miembro también de la OTAN, estratégico en la confrontación geopolítica del Mar Negro y el Asia Central, y también candidato desde hace mucho a pertenecer a la UE, aunque hoy día con la ilusión en mínimos y las negociaciones paralizadas.

No es extraño que en el seno de los estados miembros **las opiniones**

5 Estos países son los siguientes: Albania, Bosnia y Herzegovina, Macedonia del Norte, Moldavia, Montenegro, Serbia, Turquía y Ucrania. La apertura de negociaciones formales en diversos capítulos no implica que se acuerde ningún plazo temporal para su finalización, ni siquiera que llegue a producirse su incorporación como indican los más de veinte años de negociación entre la UE y Turquía y su estancamiento actual.

y posiciones oficiales sobre el propio proceso de integración europeo y sus consecuencias hayan sido dispares y cambiantes conduciendo en muchos periodos a una *"paralización"* del proceso de integración, y una reflexión continua sobre lo qué es y debe ser la UE, sobre su destino final y su papel en el mundo.

Realmente, **ha sido en los momentos de superación de las diferentes "crisis" acaecidas cuando más se ha avanzado en el proceso de la construcción europea**, aunque su destino final no sea compartido por todos los estados miembros y el **modelo federal** inicial defendido por algunos en el comienzo de su andadura pensando en los *"Estados Unidos de Europa"* esté, por ahora, descartado.

La misma historia del **proceso de la negociación de la adhesión de España**, efectiva desde enero de 1986, describe claramente cómo ese proceso no solo tenía un objetivo de interés económico para apuntalar la transición a un modelo de economía modernizada y abierta, sino también el deseo común, compartido por todo el arco parlamentario español y por la inmensa mayoría de sus ciudadanos, de **pertenencia a un conjunto de países con valores democráticos asentados** que, para España, tras una larga época de aislamiento, se veía, estrenando un régimen democrático, como el **camino de vuelta a nuestra "casa común europea".**

Desde entonces, España ha planteado y asumido posiciones favorables al proceso de integración europea, con independencia del signo ideológico de sus sucesivos gobiernos, aprovechando los periodos en los que ha asumido la presidencia del Consejo para avanzar en ello conciliando los intereses nacionales con los europeos. Durante el ejercicio de una quinta presidencia española en el segundo semestre de 2023 son, de nuevo, ocasión y motivo para **renovar este planteamiento europeísta**. De hecho, y estrechamente ligado a la temática del presente documento, una de las líneas de acción prioritarias propuesta por el Gobierno español para su semestre europeo ha sido la de **reforzar la autonomía estratégica abierta de la Unión Europea**[6]**,** concepto que se desarrollará en la presente monografía.

La UE no ha buscado en las décadas transcurridas desde 1957 hasta la actualidad convertirse en una potencia dominadora en base a un **poder duro** ejercido en el mundo en un sentido convencional. Era difícil que lo pudiera hacer sin disponer de una capacidad militar común, delegada por los propios Tratados a la esfera de la decisión y diversidad de la escala nacional e intergubernamental, y, en la práctica, a la dependencia para su seguridad colectiva de Estados Unidos dado que muchos de sus estados miembros pertenecen simultáneamente a **la Organización del Tratado**

6 https://www.lamoncloa.gob.es/presidente/actividades/Paginas/2023/060223-sanchez-autonomia-estrategica-abierta.aspx

del Atlántico Norte (OTAN).

El reciente proceso del ***BREXIT***[7] con la salida del Reino Unido de la Unión y la incorporación a la OTAN de Finlandia y, en sus últimos pasos, de Suecia ha hecho perder aún más esta **capacidad disuasoria propia de la Unión** que pudiera haber tenido y que fue abandonada en los años cincuenta del siglo XX al fracasar la propuesta francesa en 1950 de creación de una "*Comunidad Europea de la Defensa*" liquidada por sus propios proponentes (Gavin, 2005).

Los europeos hemos sido históricamente conscientes de esa debilidad en nuestro posicionamiento internacional. En 1991 el Ministro de Asuntos Exteriores belga *Mark Eyskens* definió a la UE como "*un gigante económico, un enano político y un gusano militar"* (Broeders, 2022). Al mismo tiempo Charles Delors, Presidente de la Comisión Europea, la denominaba *"un objeto político no identificado",* algo así como un "OVNI" (*objeto volante no identificado*) en el espacio político, que **rara vez, podía actuar con una voz propia en conflictos internacionales en los que primaban las posiciones nacionales de sus estados miembros**.

Las limitaciones existentes en la UE para conseguir la autonomía estratégica son conocidas, y responden a una arquitectura institucional creada exprofeso con **palancas equilibradoras** de control entre los estados miembros y las instituciones comunitarias. Como expresa Morillas (2021), de ello se derivan **tres "deficiencias" fundamentales que limitan la autonomía estratégica europea**[8]:

"En primer lugar, la ***parálisis política a nivel de la UE****, que está vinculada al proceso intergubernamental y basado en el consenso de la toma de decisiones de política exterior de la UE en el que a menudo hay un veto por parte de uno o más Estados miembros. En segundo lugar, los* ***debates divisivos y distractores sobre la votación por mayoría cualificada*** *en asuntos de política exterior y de seguridad, ya que no está claro si la votación por mayoría cualificada contribuiría al objetivo de la autonomía estratégica y la adopción de la votación por mayoría cualificada en la política exterior requeriría cambios en el Tratado en primer lugar, que nuevamente requieren unanimidad para su adopción. En tercer lugar, el* ***enfoque limitado en la seguridad y la defensa*** *al implementar la autonomía estratégica europea".*

En la práctica, como gran potencia económica, las relaciones interna-

7 Con la salida del Reino Unido de la UE, únicamente Francia entre los estados miembros de la UE posee actualmente capacidad disuasoria nuclear. Y hasta el comienzo de la invasión de Ucrania por Rusia, tras la que se anuncian incrementos presupuestarios esenciales, los estados miembros contaban con presupuestos de defensa que fueron perdiendo peso porcentual en el PIB nacional durante las dos últimas décadas, sobre todo, tras la caída de la Unión Soviética. En los últimos años empezaron lentamente a recuperarse, y desde 2022 de forma más intensa.

8 Entiéndase, por ahora, el concepto de autonomía estratégica desde una perspectiva intuitiva.

cionales de la UE con todos los países del mundo se han asentado durante décadas en el **reconocimiento mutuo de la necesidad de un mundo *"sometido a reglas"*** que permitiese el comercio de todo tipo de bienes y productos a través de **cadenas de valor globales** consideradas seguras y estables en función de ese interés mutuo. Realmente, la historia de la evolución de lo que hoy conocemos como Unión Europea ha sido paralela a la expansión del concepto de **"globalización de la economía"** sobre la base de reglas de mercado compartidas que hasta hace muy pocos años era incontestable y en cuya consolidación la UE ha jugado un papel muy relevante (Piqué, 2018).

La realidad de las crisis recientes en el siglo XXI ha demostrado que esa **hipótesis de estabilidad permanente**, y el interés común compartido subyacente de todos los países en preservarla, no era válida para asegurar la estabilidad del modelo de globalización a largo plazo ni para asegurar el peso de la UE en el mismo. Para una UE volcada en intensas relaciones comerciales como base de su modelo económico, el cuestionamiento del proceso de globalización, creciente desde hace diez años, se ha manifestado en la **reestructuración rápida de las cadenas de valor globales** hacia modelos en los que prima la búsqueda de resiliencia y consideraciones sobre el tipo de países participantes por encima de criterios de eficiencia.

Las transformaciones de las cadenas de valor hacia la relevancia de los conceptos de "*reshoring",* retorno de la actividad industrial al país original, "*nearshoring*", reubicación de la actividad en países cercanos, o "*friendshoring*", reubicación en países amigos, suponen el **reconocimiento de un mundo más inestable y complejo en el que la resiliencia y reducción de riesgos en las cadenas de valor adquiere un valor fundamental**[9]. Es en este mundo en el que la UE tiene que continuar su desarrollo y posicionamiento en el mundo, y las claves para hacerlo son muy diferentes de las del pasado.

Al mismo tiempo, el **poder blando de la UE**, concepto acuñado por *Nye* (2005) ligado a la **capacidad de influir en terceros**, se ha asentado durante años en la creación progresiva de un **marco regulatorio** de la UE que imponía condiciones a la comercialización de productos y servicios en base a la protección del consumidor europeo. Era, en palabras de *Anu Bradford* (2021), el "*efecto Bruselas*" el que permitía "**incrementar el impacto de la UE fuera de sus fronteras"** al forzar la necesidad por parte de empresas de todo el mundo de adaptarse a la regulación establecida por la UE para poder entrar y operar en el mercado europeo, no solo en el ámbito digital, y a la mimetización y adaptación (no forzada) de algunas de

9 No voy a entrar en el análisis de las cadenas de valor globales que desborda los objetivos de la presente monografía, pero sí abordaré posteriormente su relación e impacto sobre la autonomía estratégica digital.

sus regulaciones, dadas sus ventajas objetivas, al ordenamiento legislativo de otros países.

Con ello, la UE se ha convertido en un **"gigante regulatorio"** con influencia directa e indirecta en el comportamiento de muchos otros países y de las empresas multinacionales. Más difícil lo ha tenido la UE en asentar su influencia en el mundo mediante el empleo de un conjunto de **instrumentos ligados a lo que se denomina "poder duro**" (basado en la amenaza y uso de la fuerza en su sentido convencional); aunque sí lo tengan y lo hayan ejercido a una escala menor, en algunas ocasiones, sus estados miembros en determinados países de menor capacidad disuasoria cuando han visto amenazados sus intereses nacionales sin que ello haya implicado un posicionamiento común de la Unión en paralelo con la adopción de algunas medidas de poder blando[10].

La derivada del poder regulatorio de la Unión con la capacidad de establecer **controles a la exportación o importación** de determinados productos**,** o la imposición de **sanciones a empresas de otros países** como ocurre en la actualidad en el ámbito digital es la dimensión más "dura" a su alcance en la medida en la que sea posible que el acceso al mercado europeo sea utilizado como "arma" ("*market access weaponization*").

1.2. LA RELEVANCIA ESTRATÉGICA DEL PROCESO DE DIGITALIZACIÓN

Adicionalmente al proceso descrito en la sección anterior, se ha generado otro movimiento tectónico cuya intensidad es creciente y que está jugando un papel esencial en el cambio de paradigma de actuación de la UE: el **reconocimiento de que las bases del cambio geopolítico descansan y se aceleran por un profundo y rápido desarrollo tecnológico**. Este cambio de paradigma encaja con la percepción del papel decisivo que juega la tecnología para mejorar el bienestar de los ciudadanos europeos y fortalecer o debilitar el papel de todos los países, incluida la UE, en el mundo.

Tomo como hipótesis implícita de partida la de que ningún país sin el dominio de las denominadas **tecnologías clave** podría mantener el carácter de gran potencia en sectores como el industrial, el de las comunicaciones, el aeroespacial, el de la medicina, el de transportes, el de educación e investigación, o el militar. Si la UE quiere actuar en el contexto mundial como una potencia mundial, debería afirmar ese carácter **dominando de forma efectiva un conjunto de tecnologías habilitadoras y emergentes**

10 Un ejemplo es el poder duro exhibido por el Reino Unido en la denominada Guerra de las Malvinas (Falkland islands) en 1982 con un apoyo "blando" al RU (sanciones a Argentina y embargo de armas) por parte de la UE. https://www.iprofesional.com/actualidad/339840-guerra-de-malvinas-resumen-que-paso-el-2-de-abril-de-1982 . Esta disputa aún sigue viva en julio de 2023 con el enfado diplomático del Reino Unido por el uso del término "Malvinas" en la cumbre mantenida por la UE con CELAC. https://euroefe.euractiv.es/section/latinoamerica/news/el-reino-unido-y-argentina-se-enzarzan-por-el-pronunciamiento-de-la-ue-sobre-las-malvinas/

frente a una competencia mundial creciente, y haciendo que su marco de uso en la sociedad europea esté alineado con el conjunto de principios y valores democráticos y de derechos sobre las personas y el planeta Tierra con el que quiere ser globalmente identificada.

En las últimos dos décadas hemos asistido también a un proceso continuo y acelerado de un fenómeno que se ha denominado de **"digitalización"** por el que la penetración en la sociedad de productos y servicios digitales con el impulso de un desarrollo tecnológico basado en las tecnologías de la información y las comunicaciones (TIC), habilitada a su vez por la microelectrónica y la nanotecnología, ha **transformado nuestra sociedad**. En los años transcurridos del siglo XXI se ha hecho palpable para el ciudadano medio que la forma de comunicarse personalmente o en grupo, de entretenerse, de trabajar, de fabricar, de realizar operaciones financieras, o de acceder a servicios públicos como la educación, la sanidad, las relaciones con las administraciones públicas, o, menos visible para el ciudadano, la capacidad de los sistemas de defensa y seguridad se han transformado profundamente.

En el contexto del fenómeno de la globalización, el **impacto del proceso de digitalización** ha sumado a la histórica relevancia del concepto clásico de intercambio de materias primas, bienes y productos físicos manufacturados entre países a través de las cadenas de valor aludidas previamente, el **intercambio masivo de información digital**. Sin asegurar este intercambio de datos, la EU no puede jugar un papel relevante a escala global porque su economía depende de esos datos. El anuncio realizado en 2015 por parte de China del lanzamiento de la denominada ***"ruta de la seda digital"*** [11] complementando la de productos físicos lanzada previamente fue un aldabonazo a Occidente de la relevancia que iba a jugar en el futuro: ocho años después del anuncio el impacto es evidente (Xiao y Ding, 2023).

El valor de los **datos**, las capacidades disponibles para su captura o generación, su protección, su intercambio masivo a alta velocidad a través de redes de comunicaciones terrestres, submarinas o satelitales, y las condiciones de acceso a los mismos, constituyen las **bases del funcionamiento de las cadenas de valor digitales globalizadas** cuya resiliencia en época convulsa también es necesaria.

Por este motivo, **asegurar la resiliencia en el intercambio de datos** se ha convertido en un factor geopolítico esencial puesto que la sociedad actual depende, en gran medida, de ese flujo de información para asegurar su funcionamiento diario, aunque los instrumentos técnicos y políticos necesarios para ello sean distintos a los empleados en el caso

11 https://www.cfr.org/china-digital-silk-road/

de los intercambios de bienes físicos, y la sociedad en su conjunto sea menos consciente de la relevancia que han adquirido en ello los satélites de comunicaciones o los cables submarinos. El usuario medio ni siquiera conoce cuál es el camino seguido por sus datos cuando utiliza un servicio digital.

La combinación del rápido desarrollo y maduración de tecnologías emergentes, junto a su convergencia, en paralelo con los cambios de poder global y la divergencia de normas reguladoras entre países, han desencadenado un **cambio de paradigma** en el modelo socioeconómico de la UE y sus estados miembros. Este cambio de paradigma implica un **progresivo alejamiento de la hipótesis de *"economía abierta basada en un mercado global"* sustentada en el intercambio de bienes físicos** que ha dominado la escena política y socioeconómica europea en las últimas décadas para dar cabida a una realidad geopolítica diferente y propia de un mundo en crisis. Se trata de ejercer un "**poder inteligente**" que combine factores *"blandos"* con *"duros"* por usar la terminología de Nye (2009) **en un contexto de realismo geopolítico**.

En consecuencia, la Comisión Europea ha adoptado, con todas sus limitaciones, pero aprovechando su capacidad de iniciativa legislativa, un papel de **liderazgo**, intentando arrastrar con ella al Consejo de la UE y al Parlamento Europeo, hacia un **pensamiento geoestratégico más realista** del que le ha precedido durante muchos años. Este **cambio de enfoque** no se basa ya en asumir la existencia de un comercio abierto y global sin condiciones, independiente de la procedencia del flujo de bienes y productos, sino en otro en el que la tecnología, desde el origen geográfico de su generación al acceso a la misma, se ha convertido en un factor geopolítico básico que debe abordarse políticamente apoyado por una capacidad de actuación más asertiva en sus fronteras, si fuera necesario.

El cambio de paradigma aludido se ha acelerado no solo por la disponibilidad tecnológica digital, sino porque la **situación estable**[12] a grandes rasgos en el contexto internacional que se creía (o se quería creer) permanente **se ha ido deteriorando poco a poco** con la aparición, casi simultánea o cercana en el tiempo, de **diversos acontecimientos no previstos o a los que no se hacía caso** (los *rinocerontes grises* mencionados anteriormente).

Todos estos acontecimientos han provocado un profundo revulsivo en las políticas e instrumentos de actuación de todos los países avanzados

12 La estabilidad general aludida no impedía la existencia de múltiples y frecuentes discusiones internas para conciliar propuestas y poder avanzar. Esas dificultades, en parte derivadas del propio proceso de ampliación, obligó a sucesivas modificaciones de los tratados constituyentes desde 1957 hasta alcanzar la situación actual. Pero la velocidad de los cambios era manejable para que las instituciones comunitarias discutieran y acordaran a su ritmo. Me temo que la aceleración de los cambios en el contexto actual las está empujando a una situación límite en la toma de decisiones.

y, concretamente, en la Unión Europea y sus estados miembros que han obligado a la UE a pensar en la **necesidad de otro marco geopolítico de actuación más resiliente y realista.**

1.3. AUTONOMÍA ESTRATÉGICA ABIERTA

La UE se adentra en la presente década del siglo XXI en un **mundo mucho más convulso** en el que, como decía la presidenta de la Comisión Europea Ursula von der Leyen al presentar su equipo de comisarios en 2019 debería considerarse como "la Comisión geopolítica… que Europa necesita urgentemente".

Otra cosa bien distinta es que ese objetivo sea sencillo o rápido de implementar por la UE; **tampoco el objetivo es compartido e interpretado de igual manera por todos los estados miembros**. Afecta a parcelas tan diferentes como el suministro energético, la ciberseguridad, los flujos migratorios, la transformación de las cadenas de valor o las alianzas internacionales; en muchos casos, basado en interpretaciones estrechamente ligadas a visiones nacionales antagónicas muy arraigadas en los países que componen la UE. No es extraño, por tanto, que **la adopción de posiciones comunes, en algunos casos con la necesidad de adoptarlas por unanimidad, encontrase dificultades, retrasos o contundencia, que les hacía perder eficacia.** Además, el diablo comunitario se esconde en los detalles de su implementación.

Sin embargo, es de justicia reconocer que, en los últimos años, azuzada por el impacto de la COVID-19, la Guerra de Ucrania de 2022 y por las crisis de suministros derivados que afectan a sectores industriales estratégicos europeos como el del automóvil, **la UE ha avanzado en materias sensibles de manera mucho más rápida de lo que era habitual** (Borrell, 2023), aunque, en mi opinión, no haya sido suficiente ni prejuzga el que lo haga en el futuro si se llega a un nuevo estado de "equilibrio inestable". La UE deberá saber cómo aprender las lecciones extraídas de las sucesivas crisis.

Se trata, en definitiva, de la necesidad de **reafirmar la soberanía europea en un mundo convulso** buscando el óptimo de un concepto que se ha convertido en el eje de actuación política: la **autonomía estratégica abierta de la UE**, objetivo que enmarca esta nueva época (puede ser pretencioso denominarla "cambio de era" como el canciller alemán Olaf Scholz indicaba con el término "Zeitenwende" en 2022) (Hartmann et al., 2023).

La **definición de "autonomía estratégica abierta"**[13] que utilizaré es la proporcionada por el Servicio de Estudios del Parlamento Europeo (Damen, 2022): "capacidad de actuar de forma autónoma, de confiar en los propios recursos en ámbitos estratégicos clave y de cooperar con los socios cuando sea necesario"[14].

La **"autonomía estratégica"** se concibe como una **fortaleza deseable de la Unión** que, si se utilizase eficazmente, podría permitir a la UE cumplir los objetivos fijados por el Consejo Europeo en su agenda estratégica 2019-2024: **proteger los intereses de la UE y promover sus valores en todo el mundo**. Concretamente, "permitiría a la UE estar a la altura de su nivel de ambición autoimpuesto, proteger a sus ciudadanos, responder a los conflictos y crisis exteriores y ayudar a sus socios a desarrollar su capacidad" (Van den Abeele, 2021).

La inclusión del calificativo **"abierta"** parece, a priori, una contradicción puesto que conseguir la autonomía puede (¿debe?) implicar el **condicionamiento de la cooperación con otros actores externos a la Unión a la priorización de los intereses propios**, y solo hacerlo **"cuando sea necesario"** tal y como se indica en la definición aportada anteriormente. En la práctica, la interpretación del término **"abierto"** ha sido el de promover y asegurar la existencia de relaciones comerciales (importación y exportación de productos y servicios) en un mercado internacional equitativo y sujeto a reglas definidas y estables[15], aunque ello conlleve a un equilibrio dinámico inestable y borroso.

La clave interpretativa reside en la última parte de la definición: determinar quiénes son los **"socios"** y cuál es el nivel de **"necesidad"** que obligue a cooperar. Ambos términos apelan a un **carácter dinámico e interpretable de la "apertura"** en el que las visiones de los estados miembros, de la UE en sus órganos comunitarios, y en los países externos no tienen por qué coincidir. Su implementación revela la existencia de opiniones diferentes entre los estados miembros y entre los grupos políticos del Parlamento Europeo sobre las condiciones e intensidad de la ambigua "apertura"[16].

Si bien **el concepto de autonomía estratégica abierta se aplica a**

13 La autonomía estratégica (Strategic Autonomy, SA) está intrínsecamente vinculada a la política de defensa común de la UE y a la definición del pilar europeo de la OTAN. El término apareció por primera vez en 1994 y luego nuevamente en 1998. Resurgió en 2003, justo antes de la guerra en Irak, para afirmar la independencia de Europa y responder al debilitamiento del vínculo con los Estados Unidos en un contexto de tensiones internacionales con los Estados vecinos de la UE.

14 Desde un punto de vista interpretativo la Comisión Europea subrayaba recientemente que "la autonomía estratégica abierta significa cooperar multilateralmente siempre que podamos, actuando de manera autónoma cuando debamos" (S&D, 2023).

15 Básicamente, se trata de las reglas definidas por la Organización Mundial del Comercio (OMC) desde mediados del siglo XX a la que se han adherido la mayor parte de los países.

16 Estoy seguro de que las próximas elecciones al Parlamento Europeo de 2024 harán resurgir el debate sobre estas diferentes interpretaciones y sus consecuencias.

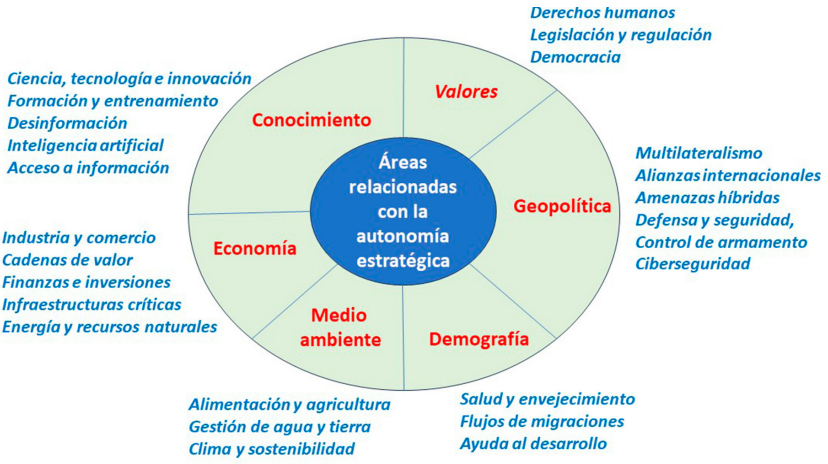
todos los ámbitos y sistemas tecnológicos, es en el **sector digital** en el que se manifiesta con mayor impacto por el doble factor de su carácter habilitador y por una tasa de evolución tecnológica muy rápida. El acceso al conocimiento tecnológico y el despliegue de redes de comunicaciones móviles 5G-6G, de cables submarinos de alta capacidad, de constelaciones de miles de nanosatélites de órbita baja para el acceso a Internet, y muy pronto del despliegue de comunicaciones cuánticas ultraseguras, no se ha limitado a asignar cuantiosas inversiones públicas, sino que la procedencia de los suministros, las propiedades de las infraestructuras o las alianzas tecnológicas entre los actores ha adquirido tintes de confrontación geopolítica con impacto en otros muchos ámbitos y, en especial, en el de la defensa y la seguridad.

Históricamente, **el concepto de autonomía estratégica apareció en el contexto de la defensa y la seguridad**[17], con visiones posibilistas más o menos atlantistas (referidas a la autonomía o no de la UE con respecto a la OTAN) de los estados miembros de la UE, pero es a partir de 2018 cuando se empieza a extender el concepto a otras áreas de intervención política para cubrir con diferentes énfasis otras **muchas áreas en la medida en la que éstas contribuyen a la seguridad** europea como las políticas comerciales, de salud, de alimentación, de energía y de la estructura de las cadenas de provisión. Se hace eco así del **creciente uso como "arma**" ("weaponization") de muchas de estas políticas en conflictos geopolíticos.

Por este motivo, no debe interpretarse la autonomía estratégica como una herramienta al **servicio exclusivo de la política exterior de la Unión**. Su implementación se desarrolla mediante actuaciones que pueden afectar a **múltiples áreas de intervención política** (Damen, 2021). La figura 1 pretende señalar que existen múltiples relaciones entre ellas por lo que es posible agrupar en áreas principales (clústeres) como geopolítica, demografía, medioambiente, economía, información y valores que, a su vez, implican subáreas más específicas.

Grevi (2019) indica, referido a la UE, que "*la autonomía estratégica no es sólo una cuestión de política exterior, sino un requisito fundamental para sostener y fomentar la integración europea".* Cumple también, por tanto, una función clave como un instrumento conceptual para avanzar en el **objetivo interno de incremento de la cohesión política** al proporcionar un objetivo compartido por el que vale la pena esforzarse, y como **guía de un proceso colectivo que conduzca a una mayor integración europea.**

17 La formulación inicial del Consejo Europeo en 2016 (Consejo Europeo, 2016) estuvo limitada al ámbito de la seguridad y defensa. https://www.consilium.europa.eu/media/22459/eugs-conclusions-st14149en16.pdf



elaboración propia inspirada en Lieve van Woensel, Kjeld van Wieringen and Mario Damen, EPRS, 2021/2022.

La formación de Competitividad del Consejo de la UE[18] adoptó en noviembre de 2020 unas "conclusiones"[19] que pretendían ofrecer un marco interpretativo de la autonomía estratégica abierta más definido y concreto que pudiera conducir a un conjunto de acciones operativas. En el párrafo 3 de las conclusiones se lee:

"El Consejo destaca que lograr la autonomía estratégica preservando al mismo tiempo una economía abierta es un objetivo clave de la Unión para autodeterminar su trayectoria económica y sus intereses. Recuerda que esto incluye identificar y reducir las dependencias estratégicas y aumentar la resiliencia en los ecosistemas industriales más sensibles y áreas específicas, como la salud, la industria de defensa, el espacio, lo digital, la energía y las materias primas críticas. Subraya que esto puede incluir la diversificación de las cadenas de producción y suministro, la garantía de almacenamiento estratégico, el fomento y la atracción de inversiones y producción en Europa, la exploración de soluciones alternativas y modelos circulares, y la promoción de una amplia cooperación industrial entre los Estados miembros"

De su lectura se desprende que las conclusiones del Consejo ofrecen un **marco operativo mucho más concreto,** aunque muy abierto en cuanto a la forma y extensión en la que puede implementarse. Pesaba

18 A efectos operativos la actividad del Consejo de la UE se subdivide en un conjunto de "formaciones" temáticas o sectoriales. Una de ellas es la denominada de "competitividad". Incluye las discusiones y acuerdos sobre investigación, innovación, industria y espacio entre los responsables de los estados miembros.

19 https://www.consilium.europa.eu/es/press/press-releases/2020/11/16/towards-a-more-dynamic-resilient-and-competitive-european-industry-council-adopts-conclusions/

en la redacción de ese párrafo la necesidad de dar respuesta a los efectos económicos de la crisis de la COVID-19 y a la creciente competencia internacional fomentando una **cooperación e integración europea reforzada y más intensa** para crear **un entorno empresarial sostenible, atractivo y competitivo**[20].

El marco conceptual presentado en 2020 fue sometido en menos de dos años (desde el 24 de febrero de 2022) a un baño de realidad con la **invasión de Ucrania por Rusia** con graves consecuencias en la seguridad europea. La agresión armada implicó un cambio de contexto de las relaciones con Rusia con la congelación de la cooperación, la aprobación de progresivas **sanciones económicas y políticas**, perturbaciones en las cadenas de provisión de productos como los cereales o minerales, choque energético (en el precio y en el suministro) cuando muchos de los estados miembros mantenían un nivel de dependencia muy elevado con Rusia… suponiendo, equivocadamente, la existencia de un contexto permanentemente estable.

Los ciudadanos europeos, no solo los gobiernos y, por supuesto, las autoridades comunitarias, fueron conscientes, de repente, de las **consecuencias de su escasa soberanía militar, industrial y energética**. Y decidieron hacer algo.

1.4. SOBERANÍA TECNOLÓGICA

Las conclusiones del Consejo mencionadas en la sección anterior retrotraen la discusión al objetivo de dominar (o conseguir el liderazgo) en un conjunto de tecnologías: concepto de **"soberanía tecnológica",** estrechamente relacionado con el de autonomía estratégica, que será presentado seguidamente. El **párrafo 5** de las conclusiones del mismo Consejo Europeo de 2020 subraya la relevancia del liderazgo tecnológico para conseguir una mayor resiliencia europea.

"El liderazgo tecnológico –basado en la investigación, la transferencia de conocimientos y la innovación–, la especialización inteligente, la sostenibilidad, el fortalecimiento de las cadenas de valor europeas y la seguridad del suministro de materias primas en Europa son requisitos previos para un mayor nivel de resiliencia de la industria europea. A este respecto, el Consejo invita a la Comisión a identificar las dependencias estratégicas y proponer medidas para reducirlas".

20 De hecho, en 2020 ocho Estados miembros enviaron una carta a las instituciones comunitarias expresando que es necesaria una "buena combinación de autodeterminación y apertura". Equilibrio cuya realización está sometida a múltiples consideraciones geopolíticas y que van a marcar el devenir de las actuaciones que se pongan en marcha en el futuro como se abordará posteriormente.

Tampoco existe una definición canónica del **concepto de soberanía tecnológica**[21]**.** Una de las **definiciones de soberanía tecnológica** más empleadas es la formulada por el Instituto Fraunhofer (Alemania) en 2021 (Elder et al., 2021):

"capacidad de un territorio, estado o agrupación de estados para proveerse de aquellas tecnologías que considera críticas para su bienestar y competitividad, bien a través de la propia generación de dichas tecnologías o bien garantizando su suministro desde otros territorios sin que esto comporte relaciones de dependencia unilaterales".

Otra definición, propuesta por Da Ponte, León y Álvarez (2022) permite **considerar otros aspectos como los recursos humanos o la densidad del tejido productivo** con el fin de acercar su implementación a políticas clave como la de recursos humanos o la industrial sin cuya reforma no se conseguiría cumplir los objetivos de soberanía tecnológica:

"la capacidad interna y externa relativa de un país o grupo de países para tomar y aplicar decisiones relativas a la generación, absorción y explotación de una tecnología, de acuerdo con los objetivos del actor en condiciones favorables u hostiles".

La autonomía estratégica y la soberanía tecnológica no son conceptos aislados. En la figura 2 se puede ver cómo la **autonomía estratégica** depende de alcanzar un nivel adecuado de **soberanía tecnológica**, la que, a su vez, depende de **asegurar el suministro de productos críticos**, **y el acceso e intercambio de información (datos)** como corresponde a una sociedad progresivamente digitalizada.

En la figura se sugiere que **la soberanía tecnológica actúa como un "habilitador" necesario para alcanzar una autonomía estratégica efectiva** influyendo tanto en la definición de las prioridades y capacidades nacionales, como en la formulación de las alianzas internacionales.

21 El concepto de soberanía se define por la Real Academia Española de la Lengua como "Poder supremo e ilimitado, tradicionalmente atribuido a la nación, al pueblo o al Estado, para establecer su constitución y adoptar las decisiones políticas fundamentales tanto en el ámbito interno como en el plano internacional". De forma similar, en ciencias políticas y derecho internacional, se entiende por soberanía "la suma del poder político, supremo e ilimitado, que posee un Estado independiente y que le confiere la autoridad necesaria para tomar autónomamente sus propias decisiones a todo nivel". Este concepto de soberanía es el que se toma en la Carta de las Naciones Unidas como base de la integridad de todos sus miembros y uno de los factores clave que explica la posición de la UE ante la invasión de Ucrania por Rusia en febrero de 2020.

Figu UE.

En l reta con ninguna . **aplicar la "misma receta"**, es decir, **implementar el mismo conjunto de políticas públicas basadas en la existencia de un marco legislativo y regulatorio común**. Sin embargo, no es así.

Si bien la relevancia de la autonomía estratégica es similar en todos los países avanzados (de hecho, todos los países la buscan… y (casi) ninguno la consigue), en el caso de la UE su relevancia está también ligada al alineamiento con las **prioridades políticas establecidas**. Concretamente, debe estar alineada con el esfuerzo europeo en **dos "transiciones tecnológicas"** del modelo socioeconómico de la Unión perseguido prioritariamente desde hace años: la **transición verde** y la **transición digital**. Ambas están estrechamente relacionadas, pero es sobre esta última, la transición digital, y su relación con la autonomía estratégica y la soberanía tecnológica (digital) de la UE sobre la que se focaliza la presente monografía.

Conseguir una **autonomía estratégica abierta digital** por parte de la UE implica establecer unas condiciones adicionales a la transición digital que reduzca las diferencias internas y asegure la competitividad externa industrial, de defensa o energética. Concretamente, el enfoque pretendido por la UE de alcanzar su **soberanía digital** se orienta hacia un mayor liderazgo digital mediante una *"acción inteligente y selectiva que permita garantizar la capacidad donde sea necesario, preservando mercados abiertos y fortaleciendo la cooperación global"*. Este objetivo es más sencillo de proponer que de conseguir como el caso de la **soberanía sobre los datos** europeos (parte de la soberanía digital) ha demostrado (Karisdat, 2023).

En la figura 3 puede verse esquemáticamente cómo **la soberanía digital de la UE** depende de conseguir la soberanía (sin apellidos) en un conjunto de áreas temáticas relacionadas entre las que destaco la **soberanía tecnológica** (sobre todo, en lo que se refiere al control de datos, microelectrónica, inteligencia artificial, y ciberseguridad que será necesario abordar conjuntamente), la soberanía **regulatoria** (capacidad de impulsar autónomamente regulaciones, no sólo en el ámbito digital, que fuercen el cumplimiento de un conjunto de principios y valores asociados a la Unión),

la **soberanía industrial** (capacidad de poder desarrollar y fabricar en la UE los productos y servicios que requiere), y la **soberanía militar** (capaz de disponer de los sistemas de armas avanzados y las capacidades operativas que requiere para su defensa) (León, 2023c)**.**

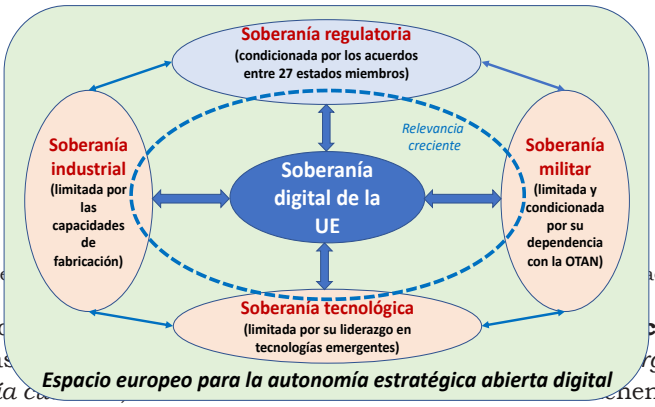


Figura 3. Re ación propia

Es po cas”, además de las rgética”, la “*soberanía* nen relevancia en la sociedad europea actual, pero, en mi opinión, o su influencia es escasa en relación con el ámbito geopolítico (como es el caso de la cultural o educativa[22]) o no están directamente relacionadas con la soberanía digital más allá de su uso como tecnología habilitadora para la generación de servicios (como es el caso de la energética ligada a asegurar el suministro de materias primas). Por estas razones, he limitado el **análisis del impacto de la soberanía digital de la UE a las tres indicadas expresamente en la figura: la industrial, la tecnológica y la militar.**

Todas las soberanías temáticas representadas en la figura 3 interaccionan entre sí y para conseguir sus fines no pueden considerarse como "soberanías disjuntas" con su propio marco de actuación independiente. En mi opinión, **el peso que adquirirán para conformar la autonomía estratégica de la UE dependerá de la forma en la que la soberanía digital de la UE se desarrolle** desde una perspectiva realista y coordinada como se analizará más adelante.

En conjunto, definen lo que he denominado el **"espacio europeo para la autonomía estratégica abierta digital".** Un "*espacio*" cuya construc-

22 Ambas lo han tenido históricamente como factores relevantes del poder blando de los estados miembros, pero menos de la UE en su conjunto al no formar parte de las competencias transferidas en los tratados a los órganos comunitarios. Es incipiente la relevancia geopolítica actual en el contexto comunitario de los flujos internacionales de personal tecnológico especializado, aunque probablemente crezca en el futuro al hilo de políticas de migración STEM selectivas.

ción efectiva durante la presente década, la forma en la que se logre, y su éxito en su despliegue interno y externo, se constituirá en el elemento clave para reafirmar el papel de la UE en el mundo.

En el contexto indicado, tras justificar la **relevancia geopolítica de la autonomía estratégica y su relación con la soberanía tecnológica** para reforzar el papel de la UE en el mundo, comenzaré, tras la presente introducción, describiendo un **modelo multinivel de la autonomía estratégica digital** que permite analizar los condicionantes existentes.

Seguidamente, se analiza el caso de la UE, fundamentalmente la **regulación de la UE en relación con la autonomía estratégica en tecnologías digitales** con el fin de identificar los problemas actuales y el impacto que puede tener en sus relaciones internacionales. Ello servirá para determinar las actuaciones puestas en marcha y determinar hasta qué punto contribuyen al objetivo indicado.

El análisis del ámbito digital realizado se focaliza en un conjunto de tecnologías habilitadoras como son la tecnología de **microelectrónica y semiconductores**, y la **inteligencia artificial** cuya penetración social es enorme y para las que conseguir un nivel adecuado de autonomía estratégica de la UE es esencial como instrumento para reafirmar su papel en el mundo.

Se ha prestado atención por su relevancia y relación con la autonomía estratégica a la **digitalización en el sector de la Defensa**. La relevancia del proceso de digitalización procede no solo por la importancia que ha adquirido en la evolución del campo de batalla, sino también por lo que supone de complejidad en la gobernanza digital debido a la confluencia de intereses en el marco de la OTAN[23], de la UE y de los diferentes estados miembros.

Tras el análisis, es posible extraer un conjunto de **recomendaciones de actuación para la mejora de la autonomía estratégica** aplicables al conjunto de la UE, y para España en la medida en la que puede contribuir a ella desde una visión pragmática y realista de acuerdo con sus recursos y capacidades.

23 Téngase en cuenta que gran parte de los estados miembros de la UE son, asimismo, miembros de la OTAN.

2

MODELO MULTINIVEL DE AUTONOMÍA ESTRATÉGICA DIGITAL

2.1. REQUISITOS PARA ALCANZAR LA SOBERANÍA DIGITAL

Para evaluar la importancia del sector digital (TIC[24]) y analizar las potencialidades digitales europeas partiré de unos datos básicos recogidos por Eurostat. En la estimación realizada se considera que **el mercado global de las TIC alcanzará un tamaño de 6 billones de euros en 2023**. El valor añadido total del sector digital en la UE superó los 604.000 millones de euros en 2021, lo que representa el 4,9 % del PIB de la UE.

Parecería que un conjunto de países avanzados con un nivel de vida elevado como es la UE debería ocupar un puesto de liderazgo en el concierto digital mundial. No es así; de hecho, a pesar del carácter esencial de la industria de las TIC para la competitividad de muchos sectores, **la cuota global de la UE en el mercado mundial de las TIC ha disminuido del 21,8 % en 2013 al 11,3 % en 2022**. En 2022, solo el 69% de las PYMEs europeas alcanzó un nivel básico de intensidad digital y únicamente el 8% de las empresas utilizó en 2021 tecnologías de inteligencia artificial.

En la figura 4 puede verse un **análisis comparativo entre Estados Unidos, China y la UE** en algunos aspectos del ámbito digital en la que la UE no sale favorecida; dicho de otra manera, su posición mundial se ha deteriorado comparativamente frente a otras grandes potencias. Preocupantes son, de acuerdo con indicadores de otros análisis, los indicadores de intensidad de innovación, desarrollo de hardware para IA, y en inversiones en I+D.

24 El clásico concepto de "tecnologías de la información y las comunicaciones" (TIC) está siendo sustituido por otro más amplio que es el de "digitalización" o "sector digital" que requiere, obviamente, el empleo de las TIC, pero que añade otros factores ligados a la forma en la que estas tecnologías penetran en la sociedad y contribuye al poder inteligente de las naciones.

Figura 4. Comparación entre UE, Estados Unidos y China. Fuente: adaptada de https://www.oliverwyman. com/our-expertise/insights/2020/sep/european-digital-sovereignty.html

Esta visión se completa con la figura 5 procedente del informe de situación del Decenio digital europeo publicado en septiembre de 2023 en el que el esfuerzo relativo en áreas clave como IA, semiconductores, ciberseguridad o 5G es menor que el de sus competidores (European Commission, 2023d).

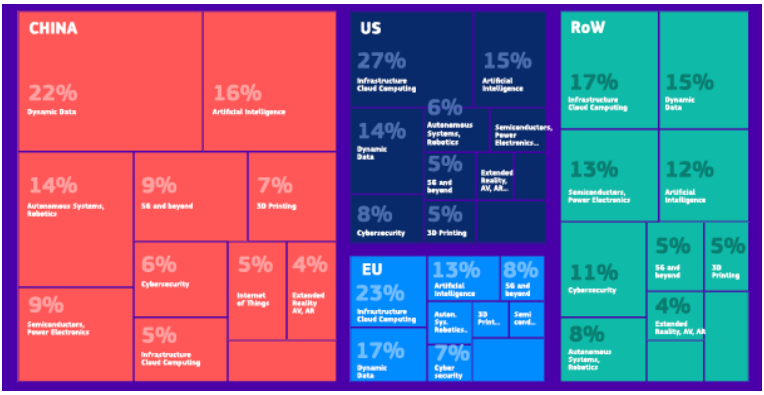


Figura 5. Peso comparado por actividades de la UE en el sector digital en el periodo 2009-2022. Fuente: European Commission (2023d)

Estas cifras indican que **Europa se enfrenta a muchos retos que deberá afrontar en el camino para fortalecer su posición digital global.**

De hecho, la UE lo ha intentado desde una perspectiva de **"soberanía regulatoria digital"** en la que, alentada por la exitosa mimetización internacional conseguida con el **Reglamento General de Protección de Datos (RGPD)** aprobado en 2016, la UE se ha convertido en pionera en la creación de **normas para regular la implantación de productos y servicios**

digitales a través de un conjunto de "***reglamentos***" (leyes europeas) con la esperanza de configurar un mercado interior protector de sus ciudadanos y, en la medida de lo posible, inspirar esfuerzos legislativos similares en otros países. Se pretende con ello, contribuir a establecer una **soberanía digital basada en reglas** comúnmente aceptadas en todo el planeta.

La **voluntad política de aplicar el RGPD** se ha puesto manifiesto con la decisión de aplicar **sanciones** a empresas de Estados Unidos por su incumplimiento[25]. Por poner un ejemplo, este es el caso de la sanción impuesta por Irlanda (sede de la empresa en Europa) a *Meta* (ex Facebook) de 1.200 millones de euros en 2023 por infringir el derecho a la privacidad de 500 millones de usuarios por transferir datos a Estados Unidos sin garantías suficientes[26].

Con mayor o menor énfasis y ritmo de implantación, los estados miembros han tenido que **acomodar sus legislaciones nacionales a la europea**. Asimismo, la mayor parte de los países avanzados se ha dotado de un marco legislativo equivalente, aunque no necesariamente con planteamientos coincidentes a los de la Unión al tener un carácter voluntario.[27]

Entre las regulaciones relevantes aprobadas o en proceso de discusión por la UE en los últimos años alrededor de la soberanía digital[28] se encuentran la **Ley de inteligencia artificial**, la **Ley de Chips**, la **Ley de Mercados Digitales** la **Ley de Servicios Digitales** y la **Ley de Datos**. En muchos casos, su entrada efectiva en vigor implica la transposición de las directivas europeas al marco legislativo nacional de los estados miembros lo que hace que este proceso sea inherentemente lento y con una entrada en vigor paulatina para los diferentes países[29].

Aunque la UE ha realizado un encomiable esfuerzo en los últimos años para dotarse de una legislación adecuada, otra cosa es evaluar si con

25 El RGPD permite a los gobiernos de los estados miembros de la UE la capacidad de imponer multas de hasta el 4% de los ingresos anuales de una empresa por las infracciones más graves.

26 Amazon fue sancionada con 780 millones en 2021 por causas similares, y a la misma Meta se suman en los últimos seis meses, otras multas de 400, 265 y 390 millones de euros. Debe tenerse en cuenta que, a pesar de ser una cuantía que parece muy elevada, se realiza sobre un volumen de facturación que ha crecido de una manera muy rápida en pocos años. Más importante que la sanción económica es la amenaza de no poder ofrecer el servicio digital si no se modifica el tratamiento de datos.

27 Es interesante comparar cómo el "principio de precaución" de las administraciones públicas está bien asentado y es compartido por la ciudadanía en ámbitos como la regulación del uso de fármacos o productos químicos y, sin embargo, lo está mucho menos en el ámbito digital.

28 El Anexo de este informe resume la situación actualizada del proceso legislativo digital a diciembre de 2023 que la UE ha emprendido en los últimos años.

29 Durante el proceso de aprobación de los reglamentos comunitarios los estados miembros buscan su entrada en vigor de forma progresiva en varios años para permitir adaptar no solo su legislación nacional, sino también para dar tiempo a todas las partes interesadas (como la industria nacional y las propias administraciones públicas) en realizar las reformas estructurales que puedan necesitar. Ello conlleva un proceso de cambio regulatorio relativamente lento y no sincronizado en el tiempo en el conjunto de la Unión Europea.

ello **ha logrado los objetivos de mejora de su soberanía digital**. Algunas preguntas clave para contestar a la pregunta serían:

- ¿La posición relativa de la UE en el concierto mundial digital es ahora mejor que la que tenía hace una década?
- ¿Se sienten los ciudadanos europeos mejor protegidos en el uso de productos y servicios digitales?
- ¿Ha conseguido la UE acortar la brecha tecnológica digital con otras potencias mundiales?
- ¿Ha mejorado la cuota de mercado mundial de las empresas digitales europeas?
- ¿Ha conseguido atraer y retener en la UE el talento digital que necesita?
- ¿Ha alcanzado la población europea, desde adolescentes a la tercera edad, el nivel mínimo de competencias digitales para hacer uso consciente y seguro de los productos y servicios digitales?

Debe reconocerse que la UE ha prestado atención a todas las preguntas indicadas; pero es en el análisis de estas respuestas en las que descansa la **valoración de la efectividad de las medidas regulatorias y presupuestarias** adoptadas por la Unión. Y en esa valoración hay puntos de vista positivos y negativos.

Algunos analistas como Carnap (2023) opinan que este esfuerzo no ofrece ninguna protección real. Para él, las recientes *Leyes de Servicios Digitales y Mercados Digitales* (DSA y DMA) fueron diseñadas *"para hacer frente a las tendencias monopolísticas de los gigantes tecnológicos estadounidenses",* no a las crecientes restricciones que está imponiendo China a usuarios de otros países[30] por lo que a la UE se le abre otro frente, ahora con China, además del de Estados Unidos. Es cierto, que Estados Unidos estaba en el punto de mira de la UE, pero el que existan otras potencias como China ante la que también es necesario prestar atención desde la regulación, no invalida, en mi opinión, una valoración positiva.

En todo caso, **no bastará con llevar a cabo un enfoque regulatorio defensivo** por ambicioso que éste sea, y por elevadas que sean las multas que se impongan, si la UE no logra extender los productos y servicios digitales desarrollados en la UE en todo el mundo. Y eso depende de la **fortaleza de su tejido industrial** y su **capacidad para desarrollar productos y servicios digitales disruptivos** que se impongan en los mercados mundiales.

30 Como ejemplo, las normas de registro con nombre real de las empresas chinas infringen el Reglamento General de Protección de Datos (RGPD) de la UE si no es necesario para prestar sus servicios (Carnap, 2023).

Incrementar la contribución de la industria europea al desarrollo de áreas digitales emergentes que se traducirán posteriormente en productos y servicios disruptivos con tasas de penetración social elevadas se convierte en un **factor condicionante clave** para que el esfuerzo regulatorio se traduzca en la mejora de posiciones a nivel mundial: para ello, deben tejerse **ecosistemas digitales innovadores** con estrechas relaciones entre actores clave públicos y privados, con un marco presupuestario, regulatorio y fiscal que aliente la inversión.

Conseguirlo implica **conjugar actuaciones** con presupuestos adecuados al nivel de ambición perseguido. Requiere, por tanto, diseñar e implementar una **política holística** ante el fenómeno de la digitalización que implique la definición y puesta en marcha de actuaciones coordinadas en el ámbito industrial, en el comercio exterior, en la defensa, en la migración, en la educación, en el despliegue de infraestructuras digitales, o en las relaciones exteriores, por citar los ámbitos más relevantes.

Un informe de 2021 del Centro Común de Investigación (JRC) de la UE (Cagnin et al., 2021) identificó las tendencias tecnológicas y oportunidades para el **futuro de la autonomía estratégica abierta de la UE en el horizonte de 2040**. En el ámbito tecnológico digital preconizaba actuar en tres aspectos:

- *El aumento de la competencia en el ámbito de las tecnologías digitales ofrece oportunidades para garantizar la soberanía tecnológica digital de la UE mediante mayores esfuerzos en investigación excelente y su traducción en crecimiento económico. Esto podría lograrse a través del escalado de las empresas emergentes de la UE en ecosistemas favorables a la innovación, y manteniendo y atrayendo talento a la UE con un fuerte apoyo de la educación y la creación de empleo.*
- *La omnipresencia de las tecnologías digitales en nuestras vidas exige un enfoque conjunto de su gobernanza a través de la cooperación internacional con democracias de ideas afines. Los marcos regulatorios podrían diseñarse de manera que fomenten la innovación en consonancia con los valores de la UE y las normas establecidas para aprovechar la capacidad de liderazgo de la UE.*
- *La salvaguarda de los sistemas de ciencia, tecnología e innovación que podrían verse perturbados en los años venideros, junto con la mejora de las asociaciones internacionales y la competitividad de los investigadores y del sistema educativo podría ser clave para lograr la soberanía digital en el futuro.*

En definitiva, se trataría de encontrar la **correcta combinación sinérgica** entre **querer** (voluntad política sostenida en el tiempo de conver-

tirse en una potencia digital), **saber** (disponer de los recursos y legislaciones adecuadas y efectivas para lograrlo en un contexto de tecnologías emergentes que evolucionan muy rápidamente), y **poder** (tener la capacidad y los recursos necesarios aplicados mediante un poder inteligente para imponer sus visiones a los demás países sin disponer de un poder duro más allá de las sanciones impuestas a empresas foráneas que permita la regulación).

Como punto de partida, la siguiente sección analiza la situación de la UE en relación con el proceso de digitalización en base a un conjunto de **indicadores**, y su recogida y seguimiento anual.

2.2. EVOLUCIÓN DE LA TRANSFORMACIÓN DIGITAL DE LA UE

2.2.1.Índice DESI de "Sociedad y economía digital"

La **transformación digital** se ha considerado por la Unión Europea como un objetivo fundamental para conseguir mantener el nivel de vida de los europeos y la competitividad de la UE en el mundo. Para ello, anualmente, **la Comisión Europea monitoriza la evolución del proceso de digitalización de la UE y de sus veintisiete estados miembros**. Con el aprendizaje mutuo asociado derivado del análisis de los datos obtenidos se pretende detectar cuellos de botella, áreas de mejora, y así comprobar la eficiencia de las políticas públicas ideadas para **acelerar esta transición hacia una completa digitalización.**

El **indicador compuesto** creado por la Comisión Europea denominado **DESI** (*Digital Economy & Society Index*) proporciona una imagen de las diferentes posiciones de los estados miembros en el proceso de digitalización atendiendo a cuatro grandes áreas: **capital humano**, **conectividad**, **integración de tecnología digital**, y **servicios públicos digitales**.

La figura 6 resume la situación de la UE en el año 2021 de acuerdo con el último informe publicado en julio de 2022 (DESI, 2022). Es evidente que entre los 27 estados miembros el valor anual de los indicadores individuales ofrece valores diferentes como resultado de una trayectoria histórica diferente, de la situación económica de cada estado miembro, y de las decisiones políticas adoptadas por la Unión y los países.

Obviamente, la situación de Finlandia, el país con un valor del índice mayor, comparada con la de Rumanía, con el menor valor del índice, implica que el punto de partida entre los estados miembros de la UE es muy diferente. **España ocupa en el séptimo lugar del indicador DESI global en 2021 una posición destacada.**

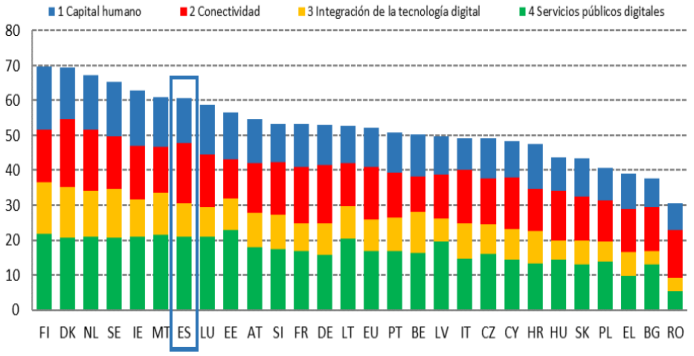


Figura 6. Índice compuesto de economía y sociedad digital en cada uno de los estados miembros. Fuente: DESI, 2022

Los resultados del último informe publicado (DESI, 2022) muestran que, si bien la mayoría de los Estados miembros está avanzando en su transformación digital, la **adopción de tecnologías digitales clave por parte de las empresas**, como es la inteligencia artificial o la gestión de grandes volúmenes de datos, sigue siendo baja; esta situación también aparece entre los países líderes digitales de la UE. En relación con España, el informe de seguimiento del Decenio Digital Europeo de septiembre de 2023, datos extraídos por el gobierno español[31], indica algunos elementos de posición relevantes:

- ***Competencias digitales**: el 64% de la población española cuenta con habilidades digitales básicas, diez puntos por encima de la media de la UE de un 54%. El porcentaje de especialistas en TIC se sitúa ligeramente por debajo de la media de la UE (4,3% frente al 4,6%) pese al crecimiento en los últimos años, mientras que el porcentaje de graduados en TIC supera la media de la UE (4,8% frente al 4,2%).*
- ***Infraestructuras digitales**: En redes fijas de muy alta capacidad, España, está significativamente por encima de la media de la UE (93% frente al 73%). También supera la media de la UE en la cobertura de fibra (91% frente al 56%) y está por encima del promedio de la UE en la cobertura general de 5G (82% frente a 81%).*
- ***Digitalización de empresas**: El porcentaje de pymes con un nivel de intensidad digital básico se encuentra alrededor de la media de la UE (68% frente 69%). Sin embargo, Espala se encuentra por detrás en el uso de big data y cloud en las empresas (9% vs 14% y 27% vs 34% respectivamente), aunque en la media en el uso de IA (8%, al igual que el promedio UE).*

31 https://espanadigital.gob.es/actualidad/publicado-el-primer-informe-de-la-decada-digital-que-situa-espana-en-la-vanguardia

- ***Digitalización de los servicios públicos****: España se sitúa por encima del promedio de la UE en casi todos los indicadores de esta dimensión, con una posición aventajada en las metas de la Década Digital de servicios públicos para ciudadanos (86% vs 77%) y servicios públicos para empresas (91% vs 84%) así como el acceso al historial médico electrónico (83% vs 72%).*

Tan importante como conocer la "foto fija" en un año determinado es **conocer cómo la posición relativa de un país en el índice varía en el tiempo**. La figura 7 (DESI, 2022) permite ver el crecimiento relativo en el periodo 2017 a 2022 (cinco años), tiempo suficiente para valorar la evolución de la efectividad de las medidas impulsadas en cada país y el grado en el que evoluciona la **cohesión digital** de la Unión.

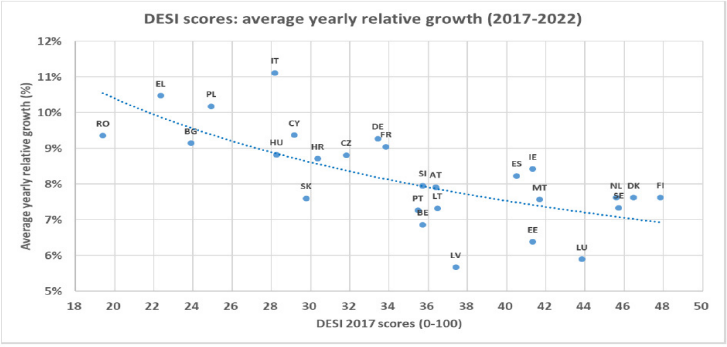


Figura 7. Crecimiento relativo medio en el periodo 2017-2022. Fuente: DESI, 2022.

Además, en el ámbito de la **conectividad digital**, algunos países están en niveles del indicador muy elevados, cerca de la saturación (es decir, han alcanzado la cobertura total de su población y territorio con una tecnología madura), pero eso no indica que lo seguirán estando ante un **cambio disruptivo de tecnología de comunicaciones** que obligue, de nuevo, a realizar cuantiosas inversiones y reiniciar el proceso[32].

Por otro lado, los **niveles insuficientes de competencias digitales** de la población obstaculizan las perspectivas de crecimiento futuro, profundizan la brecha digital y aumentan los riesgos de **exclusión digital** a medida que más y más servicios, incluidos los esenciales, requieren su acceso telemático; problema creciente en Europa ante una población en-

32 El ejemplo se puede ver con el despliegue de las tecnologías de comunicaciones móviles celulares 5G. Tener cubierto todo el territorio y la población con 4G no implica que se ocupe la misma posición en unos años con el despliegue de 5G. Pueden ser superados por otros países que decidan efectuar inversiones cuantiosas en 5G sin las rémoras derivadas de una inversión 4G previa que haya que amortizar. La misma situación se puede dar con la siguiente generación de comunicaciones móviles 6G en desarrollo y de la que se espera su despliegue masivo en la próxima década.

vejecida y que limita la expansión de los servicios digitales financieros o de las administraciones públicas.

Finalmente, es necesario intensificar los esfuerzos para garantizar el pleno **despliegue de la infraestructura de conectividad ubicua** (móvil celular, en particular 5G, y de internet de las cosas) que se requiere para el despliegue de servicios y aplicaciones altamente innovadores (DESI, 2022). **Sin una extensa cobertura no será posible acceder a servicios avanzados, pero sin servicios digitales, la inversión para incrementar la cobertura es inútil.**

En todos los Estados miembros, la evolución futura de las políticas digitales se verá facilitada en gran medida por los recursos dedicados a inversiones y reformas digitales contenidos en los **planes nacionales de recuperación y resiliencia** (FRR) presentados por los estados miembros y adoptados por el Consejo en respuesta al programa *Next Generation EU*. En virtud del Reglamento de *Next Generation EU*, cada Estado miembro debe dedicar al menos el **20 % de la asignación total de su Plan de Recuperación y Resiliencia a medidas que contribuyan a la transición digital o a abordar los retos derivados de ella**[33], aunque las diferencias entre países de acuerdo con los planes aprobados son muy diferentes (del 20% al 53%) como se indica en la figura 8.

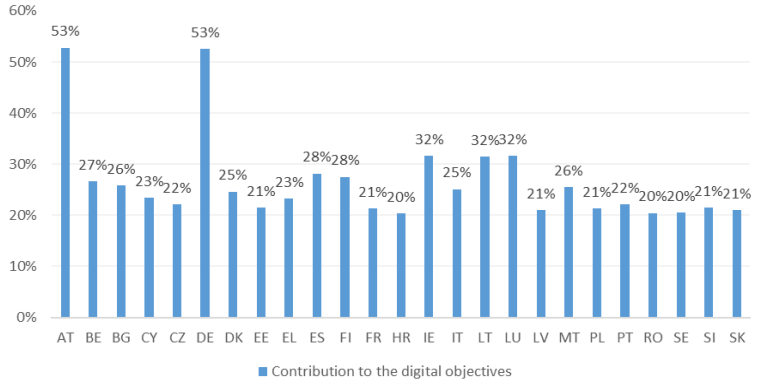


Figura 8. Contribución a los objetivos digitales en los planes de recuperación y resiliencia de los estados miembros de la UE. Fuente: DESI, 2022

Estos recursos se verán complementados en el periodo 2021 a 2027 por las inversiones en el marco de la política de cohesión territorial. Los programas operativos **FEDER** (*Fondo Europeo para el Desarrollo Regional*) focalizados en apoyar el despliegue de infraestructuras digitales, y el **FSE+** (*Fondo Social Europeo Plus*) para la adquisición de habilidades digitales,

33 Ese porcentaje supone destinar 127.000 millones de euros a reformas e inversiones digitales en los planes nacionales de recuperación y resiliencia. https://digital-strategy.ec.europa.eu/es/policies/desi

contribuirán al esfuerzo conjunto para alcanzar los objetivos a nivel de la UE establecidos en la denominada *"Década Digital Europea"* (2021-2030)[34]. En la tabla 1 se pueden ver los recursos inicialmente asignados a FEDER, FSE+ y al Fondo de Cohesión (FC).

Fondo	Aportación de la CE	Cantidad total
FEDER	29,589,219,267.042	44,890,153,048.576
FSE+	6,815,446,031.6	10,505,316,746.726
FC	789,085,818.6	995,042,140.522

Tabla 1. Recursos en la política de cohesión para la transformación digital 2021-2027. Fuente: https://cohesiondata.ec.europa.eu/stories/s/Cohesion-policy-supporting-the-digital-transition-/vaxt-7rsr/

El efecto de la priorización digital se ha empezado a notar en los dos últimos años (evolución de los datos DESI de 2019 y 2021). En tan solo dos años, **la mejora de conectividad global en la UE ha crecido de manera muy relevante tanto en territorio como en población**. Estas buenas cifras globales de conectividad no pueden ocultar las **relevantes diferencias internas de unos países con otros** como se pueden ver en la figura 9 atendiendo a los cuatro indicadores empleados por DESI para medir el nivel de conectividad alcanzado[35].

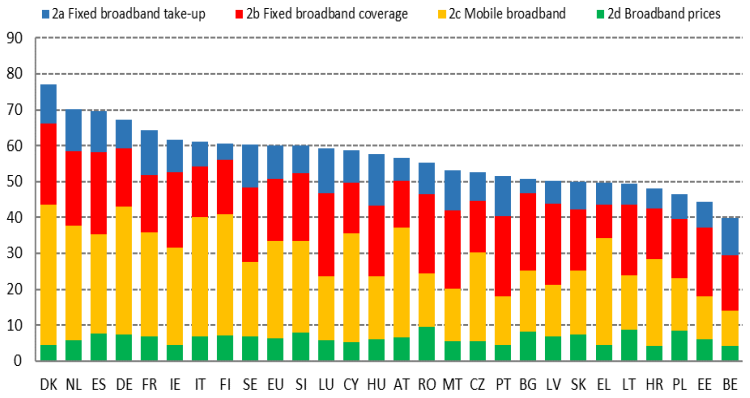


Figura 9. Conectividad digital por países. Fuente: DESI, 2022.

Esta situación refleja, de nuevo, la **falta de cohesión interna en el conjunto de la UE** a pesar del elevado volumen de recursos empleados

34 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es

35 Este análisis puede hacerse de igual forma sobre el resto de los grandes grupos de indicadores, pero para los objetivos marcados en este informe es suficiente. Obsérvese que la posición de Finlandia y Rumania ya no se corresponde con el primer y último puesto respectivamente en el DESI global (figura 5).

en la estrategia de cohesión y en los fondos de recuperación y resiliencia (*Next Generation EU*) puestos a disposición de los estados miembros para lograr la completa digitalización. En el caso de **España** la tabla 2 indica la situación existente en los indicadores correspondientes de 2020 a 2022 comparadas con la media de la UE en 2022.

	España			UE
	DESI 2020	DESI 2021	DESI 2022	DESI 2022
2a1 Implantación global de la banda ancha fija % hogares	78 % 2019	82 % 2020	83 % 2021	78 % 2021
2a2 Implantación de banda ancha fija de al menos 100 Mbps % hogares	53 % 2019	65 % 2020	72 % 2021	41 % 2021
2a3 Implantación de al menos 1 Gbps % hogares	< 0,01 % 2019	< 0,01 % 2020	0,02 % 2021	7,58 % 2021
2b1 Cobertura de banda ancha de nueva generación (NGA) % hogares	90 % 2019	92 % 2020	94 % 2021	90 % 2021
2b2 Cobertura de la red fija de muy alta capacidad % hogares	89 % 2019	92 % 2020	94 % 2021	70 % 2021
2b3 Cobertura de la fibra óptica hasta las instalaciones (FTTP) % hogares	80 % 2019	85 % 2020	89 % 2021	50 % 2021
2c1 Espectro 5G Espectro asignado como un % del total del espectro 5G armonizado	30 % 04/2020	65 % 09/2021	65 % 04/2022	56 % 04/2022
2c2 Cobertura 5G[4] % áreas pobladas	NP	13 % 2020	59 % 2021	66 % 2021
2c3 Implantación de la banda ancha móvil % personas	85 % 2018	85 % 2018	94 % 2021	87 % 2021
2d1 Índice de precios de la banda ancha Puntuación (0 a 100)	52 2019	73 2020	83 2021	73 2021

Tabla 2. Conectividad digital de España 2020-2022. Fuente: DESI, 2022.

Puede observarse que la situación de España es buena comparada con la de la UE en todos los indicadores con excepción del de *"implantación de al menos 1Gbps"* en términos del porcentaje de usuarios que poseen ese acceso mínimo que es muy inferior a la media de la UE en 2022.

2.2.2. Modelo de análisis cualitativo

Para entender el proceso de digitalización europeo es necesario profundizar en la dimensión tecnológica y no limitarse a un análisis de los presupuestos asignados o gastados. Desde el punto de vista tecnológico las **"tecnologías digitales"** incluyen y están relacionadas con otras muchas tecnologías que es necesario tener en cuenta para asegurar que los usuarios puedan utilizar plenamente productos, aplicaciones y servicios digitales adecuados a sus necesidades (individuales o institucionales).

La figura 10 representa de manera esquemática estas relaciones desde los **materiales** necesarios para fabricar componentes, ordenadores y pro-

ductos digitales, hasta las aplicaciones en forma de **productos y servicios digitales** al servicio de entidades y ciudadanos en múltiples dominios[36].

He situado por encima de la capa de **computación** (arquitecturas de sistemas basados en procesadores digitales) un nivel en el que se destaca la **inteligencia artificial** (empleando o no procesadores especializados para la ejecución de algoritmos). Al mismo nivel, sobre la de **conectividad digital** (despliegue de redes digitales fijas, móviles o satelitales) se encuentra la denominada de **plataformas digitales** con crecientes relaciones con la inteligencia artificial.

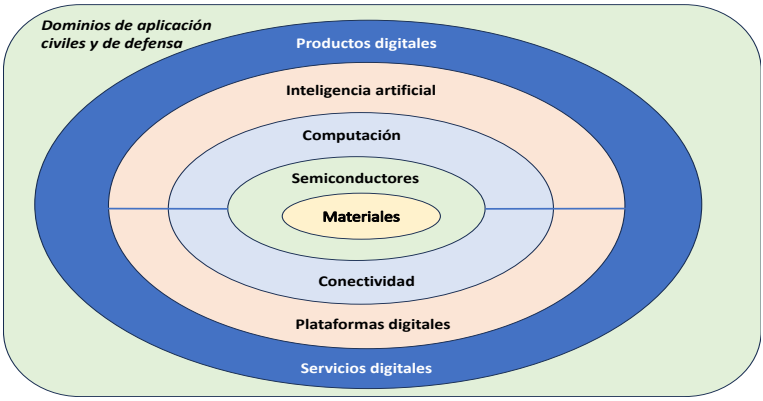


Figura 10. Estructura en niveles de las tecnologías digitales. Fuente: elaboración propia

En la figura 10 no he explicitado, sin embargo, las múltiples subdivisiones posibles en el **nivel de aplicación**, pero todas están basadas en la comercialización de un número muy elevado de **productos y servicios digitales** en prácticamente, todos los ámbitos de la sociedad, tanto civiles como de defensa. Es habitual distinguir entre aplicaciones de entretenimiento, sanidad, educación, finanzas, industria, defensa, energía, transportes, servicios de las administraciones, etc. que combinan soluciones integradas y dan origen a mercados con características y actores relevantes muy diferentes.

Lo que he querido señalar en la figura 10 es que para que sea posible acceder a aplicaciones en cualquiera de esos sectores de los que depende la competitividad de todo tipo de entidades, se requiere **disponer de suficiente capacidad de actuación en todas las capas inferiores**. De hecho, en todos los niveles se pueden encontrar **puntos de fricción de carácter geopolítico** que condicionan el acceso y disponibilidad de esas aplicaciones. De

36 He tratado de simplificar al máximo la figura no incluyendo otro tipo de elementos que también son relevantes (p.ej. baterías, células solares, sensores) o tecnologías que dependen fuertemente de las representadas (p.ej. las tecnologías cuánticas) cuyo desarrollo requeriría mucho más espacio.

manera más explícita, disponer de una buena **conectividad** tanto en redes fijas como móviles con gran ancho de banda permite poner a disposición de las empresas y los ciudadanos europeos el acceso a múltiples servicios digitales; es una **condición necesaria, pero no suficiente** porque depende de la resiliencia con la que estos servicios sean accesibles y su coste frente a eventos externos que no son controlados en su totalidad por la UE.

Desde mi punto de vista, la **evolución positiva** de la situación mostrada por DESI en las tablas y gráficas de las figuras anteriores **no implica necesariamente que la UE haya mejorado su autonomía estratégica digital.** Es verdad que se han dado pasos en los ámbitos indicados durante la última década, pero no me parecen suficientes. Los países competidores también lo han hecho.

El nivel real de autonomía estratégica está condicionado en la situación en los niveles anteriores. Describo seguidamente este problema identificando algunos de los **puntos críticos en la UE**, más relevantes desde mi perspectiva personal.

- Europa no dispone de materias primas o de facilidades suficientes para fabricar dispositivos semiconductores, por lo que la UE depende de proveedores externos cuya producción no controla.
- Los servicios digitales más extendidos en Europa son proporcionados por empresas foráneas con las que la UE mantiene un alto nivel de dependencia y, además, no existen alternativas europeas suficientes de similar funcionalidad y capacidad.
- Los datos de los ciudadanos y entidades europeas son capturados por aplicaciones de empresas no europeas y residen en servidores ubicados en otros países perdiendo la capacidad de control de estos datos.
- Las grandes entidades propietarias de plataformas digitales no pagan sus impuestos en los países europeos en los que realizan sus operaciones, ni existe una homogeneidad en el marco fiscal.
- Las decisiones clave de inversiones sobre infraestructuras digitales, grandes parques de servidores, o la ubicación de centros de I+D, en Europa se toman fuera de la UE.
- Y, por último, el desarrollo de tecnologías digitales emergentes se realiza en empresas consolidadas o por start-ups no europeas o que escalan de tamaño fuera de la UE.

Cada uno de estos puntos es relevante de forma aislada, pero mucho más si suceden todos ellos con realimentaciones positivas. **Si ocurriera**

todo ello, el nivel real de autonomía estratégica digital conseguido en la UE sería bajo con impactos potenciales elevados. El problema es que, en mi opinión, **eso es lo que ocurre.**

Estos problemas son conocidos y analizados extensivamente, pero interpretados en su gravedad de distinta manera por los estados miembros. En mi opinión, si la UE no es capaz de poner en marcha medidas correctoras decididas y ambiciosas, apoyadas por una regulación favorable, complementada con recursos económicos suficientes durante periodos prolongados, y con la disponibilidad de recursos humanos suficientes, la evolución previsible es el **reforzamiento de la posición dominante en la UE de empresas digitales de otros países**, sobre todo, de Estados Unidos.

Tomando en cuenta este hecho surgen algunas preguntas relevantes para la UE y los gobiernos europeos: ¿se prefiere ralentizar el despliegue de nuevos productos y servicios digitales para conseguir que sean proporcionados por la industria europea?[37] o ¿sería mejor aceptar la dependencia de empresas de fuera de la UE, pero asegurar con ello que la última generación de productos y servicios digitales estén lo antes posible a disposición de los usuarios europeos para asegurar su competitividad a nivel global?[38]

Razones para la decisión no faltan en uno y otro sentido: la **polémica tecnológica, geopolítica y presupuestaria**, imbricando las tres dimensiones, está servida. Seguidamente, la monografía aborda la problemática geopolítica específica del acceso internacional a productos y servicios digitales abordando algunos de los puntos de fricción identificados.

2.3. CLAVES GEOPOLÍTICAS DEL ACCESO A PRODUCTOS Y SERVICIOS DIGITALES

2.3.1. Identificación de puntos de fricción geopolítica

Para los propósitos de esta monografía denominaré **"punto de fricción geopolítica"** a un problema de base tecnológica en el que su origen, complejidad y evolución están condicionados por conflictos geopolíticos entre los principales actores que intervienen. Me focalizaré exclusivamente en aquéllos relacionados con la autonomía estratégica digital de la UE.

37 Una situación de este tipo se está produciendo con el despliegue de la tecnología 5G de comunicaciones móviles en la que se ha decidido por varios países europeos prescindir de un suministrador como Huawei (de China) por razones de seguridad y por presiones por parte de Estados Unidos, aunque esa decisión haya ralentizado su despliegue. En este caso, los suministradores alternativos no son solo de la UE sino también de Estados Unidos que tampoco estaban preparados para suministrarlos a gran escala y supondrá un coste mayor.

38 A nadie se le ha ocurrido impedir el acceso en la UE a GPS (sistema de navegación satelital dependiente de Estados Unidos) sobre el que se basan múltiples aplicaciones digitales hasta la disponibilidad de Galileo (sistema de navegación satelital desarrollado y desplegado por la UE), aunque el desarrollo de este último se ha considerado esencial para asegurar la autonomía estratégica europea a largo plazo.

Actualmente, se pueden identificar **múltiples puntos de fricción geopolítica abiertos en cada uno de los niveles** presentados en la figura 10 de la sección anterior. La emergencia de cada uno de estos puntos de fricción ha derivados de situaciones históricas, de la estructura del tejido industrial o de las decisiones adoptadas por varias potencias tecnológicas con intereses contrapuestos. Su abordaje ha tenido como resultado la necesidad de **diseñar instrumentos políticos y económicos paliativos** y, en la medida de lo posible, resolverlos mediante **negociaciones y acuerdos** bilaterales y multilaterales entre países.

Sin pretender ser exclusivo, he representado en la figura 11 **algunos de estos temas de fricción** que afectan actualmente a la autonomía estratégica digital europea[39]. En casi todos los casos los países han pretendido abordarlos a nivel nacional para reducir sus efectos negativos mediante el desarrollo de legislaciones y normativas *ad hoc* junto a una política de sanciones, aranceles y controles a la exportación e importación. En definitiva, mediante el uso de un conjunto de instrumentos de poder blando y duro a su alcance.

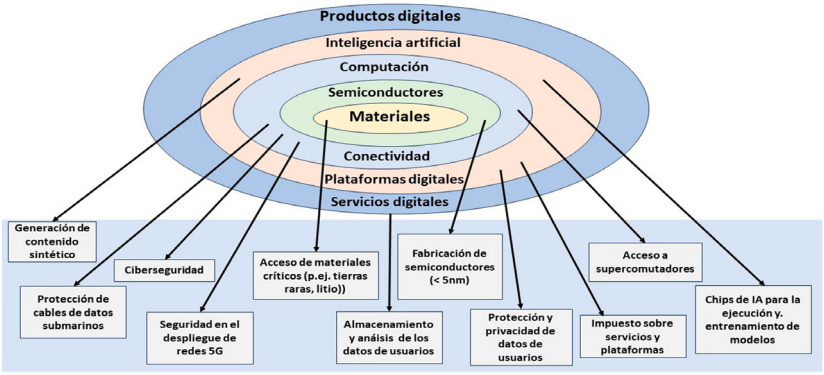


Figura 11. Puntos de fricción geopolítica digital. Fuente: elaboración propia

Ante este panorama, **la UE está actuando de forma coordinada** consciente de que únicamente una acción conjunta podría reducir significativamente los riesgos, aunque ello suponga conceder un papel de liderazgo a las instituciones comunitarias apoyadas en la prerrogativa de iniciativa de la Comisión Europea.

Como es lógico suponer, las medidas puestas en marcha por la UE no son necesariamente compartidas globalmente por terceros países; de

39 Por simplicidad del esquema, he hecho depender cada uno de los puntos de fricción de un único nivel o subnivel. En la práctica, algunos de ellos tienen origen e impacto en más de un nivel.

hecho, han provocado en muchos casos la puesta en marcha de **contramedidas** por parte de países que se sienten directamente amenazados, lo que ha conducido a una **espiral de acciones proteccionistas** que dificulta aún más la obtención de acuerdos de gobernanza global de las tecnologías digitales, e incrementa el **riesgo de fragmentación de los mercados digitales globales**.

La UE está directamente afectada por todos los puntos de fricción identificados. No es el objetivo de este estudio desarrollar en detalle desde el punto de vista tecnológico todos los puntos de fricción, sino **reflejar cómo condicionan y están condicionados por factores geopolíticos relacionados con la autonomía estratégica de la Unión Europea**.

En el modelo en niveles de la figura 10 se ha representado como segunda capa la de los **semiconductores**, esenciales para la gran mayoría de productos digitales[40]. Se trata de una tecnología denominada *"habilitadora"* que se encuentra en la base de productos tan dispares como un juguete, un teléfono móvil o un misil por citar algunos de ellos. La problemática asociada a la disponibilidad de dispositivos semiconductores y la capacidad de su fabricación se ha convertido en otro punto de fricción geopolítico internacional de enorme relevancia. No olvidemos que se trata de una **tecnología dual** de interés tanto civil como militar con impacto y con una penetración social enorme en los países desarrollados y creciente en los países en desarrollo[41].

Basada en la disponibilidad de semiconductores se encuentra un área que he englobado en la capa de **computación**, desde los microprocesadores hasta los supercomputadores (integrando miles de ellos) incluyendo no solo el desarrollo hardware, sino también el software de base necesario para asegurar su funcionamiento (como son los *sistemas operativos*) y múltiples herramientas software empleadas en el desarrollo de sistemas (p.ej. compiladores, depuradores, librerías de componentes). Durante muchos años todo esto era lo que se necesitaba para poder desarrollar cualquier tipo de producto o aplicación digital.

También en este nivel se encuentran puntos de fricción geopolítica como demuestra las restricciones impuestas por Estados Unidos a China

40 Es cierto que un producto digital, supongamos un teléfono móvil inteligente, requiere de muchos otros componentes, además de semiconductores (cámara, baterías, pantalla); pero son ellos lo que, a la postre, definen sus prestaciones básicas: procesadores, memorias, comunicaciones, sensores, etc. Todos ellos son dispositivos semiconductores.

41 Como ejemplo de las diferencias existentes, en el África subsahariana el uso de telefonía móvil había alcanzado en 2021 una penetración del 46% de la población y la estimación para 2025 era que ascendiera al 50%. https://www.gsma.com/mobileeconomy/sub-saharan-africa/. Sin embargo, en la UE ya había alcanzado el 86% de la población en 2021 https://www.gsma.com/mobileeconomy/europe/

para la fabricación de supercomputadores con procesadores avanzados diseñados por empresas americanas. Las razones esgrimidas de seguridad nacional se refieren al **posible uso para el diseño y la simulación de modelos de armas como misiles o armamento nuclear**, pero esconden la decisión política de Estados Unidos de mantener su supremacía en una tecnología habilitadora fundamental. En la práctica, estas restricciones afectan a otros tipos de aplicaciones de carácter civil en múltiples campos (electrodomésticos, automóviles, equipos médicos, juguetes, etc.) por lo que delimitar su efecto en sectores concretos es imposible.

He querido identificar en el mismo *nivel* las tecnologías de comunicaciones como base de la **conectividad digital** que ha permitido que la mayor parte de los dispositivos actuales estén conectados a redes digitales. No se trata solo de comunicaciones entre dispositivos personales, sino de todo tipo de "objetos" a los que se quiere dotar de inteligencia en lo que se denomina *"Internet de las cosas".* En este nivel es en el que se ha configurado un punto de fricción geopolítico asociado al problema de seguridad nacional en el empleo de chips para el **despliegue de redes de comunicaciones móviles 5G** procedentes de empresas privadas, pero supuestamente "controladas" por países con los que existe un enfrentamiento geopolítico**.**

El siguiente nivel agrupa las tecnologías de **inteligencia artificial** y las **plataformas digitales** que permiten la puesta en marcha de servicios avanzados basados en la existencia de redes y procesadores de nueva generación. La evolución de los últimos años hace que puedan considerarse ambas como **tecnologías habilitadoras de segundo nivel** (realmente, como un grupo de tecnologías). Son ellas las que permiten incorporar de forma creciente un conjunto de funcionalidades integradas en una multitud de productos y servicios que les permiten alcanzar su competitividad global. Pueden considerarse como tecnologías independientes, aunque se refuerzan mutuamente. En este nivel también está surgiendo un punto de fricción geopolítica creciente con el **acceso a grandes volúmenes de datos para entrenar a algoritmos de inteligencia artificial.**

Como resumen, la tabla 3 resume estos aspectos, y algunos otros que influyen en la conflictividad digital actual.

Nivel estructural	Tecnologías implicadas	Puntos de fricción geopolítica
Materiales	• *Extracción y purificación de silicio, tierras raras, litio, etc. necesarios para la fabricación de productos digitales.* • *Síntesis de nuevos materiales (p.ej. superconductores a temperatura ambiente).*	• *Concentración de yacimientos de algunos minerales y tierras raras en pocos países.* • *Regulación medioambiental (p.ej. procesos que reduzcan la huella de carbono).* • *Posicionamiento de grandes potencias en terceros países (África, Asia. Latinoamérica) para el acceso a materias primas ligadas a las necesidades de digitalización.*
Semiconductores	• *Fabricación de dispositivos semiconductores de alta resolución (<10nm).* • *Diseño abierto de dispositivos lógicos y procesadores (p.ej. RISC V).* • *Dispositivos fotónicos.*	• *Control del uso de dispositivos semiconductores avanzados en sistemas duales.* • *Acceso restringido a equipos de fabricación de circuitos integrados de alta resolución.*
Computación	• *Arquitecturas de computación distribuidas y supercomputación.* • *Sensores inteligentes.* • *Computación neuromórfica.* • *Servidores para centros de datos requeridos para IA.*	• *Acceso a conjuntos de instrucciones propietarias por terceros países.* • *Herramientas software para el desarrollo de sistemas duales.* • *Acceso remoto a sistemas supercomputadores.*
Conectividad digital	• *Comunicaciones móviles celulares (5G, (6G)),* • *Cables submarinos,* • *Constelaciones de satélites.* • *Computación en el borde.* • *Internet de los sentidos.*	• *Protección de infraestructuras digitales críticas.* • *Distribución inteligente del espectro de frecuencias.* • *Uso regulado del espacio para constelaciones de nanosatélites de comunicaciones.*
Plataformas digitales	• *Arquitecturas interoperables.* • *Ciberseguridad embebida.* • *Tecnologías de nube.* • *Big data.* • *Interfaces de aplicación (API).*	• *Privacidad de datos de usuario.* • *Control del acceso a servicios mediante plataformas digitales desde otros países.* • *Restricciones en el uso de datos personales fuera de la UE.* • *Pago de impuestos en los países en los que se opera.*
Inteligencia artificial	• *Redes neuronales.* • *Aprendizaje de máquinas.* • *IA generativa.* • *Circuitos integrados específicos para ejecución (en operación y en entrenamiento) de algoritmos de IA.*	• *Acceso a procesadores específicos para ejecución de algoritmos de IA (chips basados en redes neuronales, FPGAs,* • *Control de la captura y acceso a grandes volúmenes de datos para entrenamiento.* • *Confiabilidad de los algoritmos de IA (problema de caja negra).*
Productos digitales (conectados)	• *Integración de varias de las tecnologías indicadas previamente en productos de consumo o profesionales (teléfonos móviles, wearables, receptores (TV), etc.)*	• *Limitaciones en el acceso y uso dependiente de la aplicación final.* • *Restricciones en la importación y exportación de productos duales.*
Servicios digitales	• *Servicios generados sobre plataformas de acceso a servicios.*	• *Condiciones de generación, acceso y control de contenidos (p.ej. fake news) por parte de las plataformas.* • *Responsabilidades jurídicas.*

Tabla 3. Puntos de fricción geopolítica relevantes (visión personal). Fuente: elaboración propia

Con el fin de acercarse a la problemática existente, fijaré la atención únicamente en **seis aspectos relacionados con la conectividad digital internacional** que han adquirido una **dimensión geopolítica relevante** en un momento de crecimiento de la conflictividad internacional y en los

que el posicionamiento político de los países se entremezcla con las capacidades tecnológicas. Estos puntos de fricción son:

- el acceso a **"tierras raras"** para la fabricación de semiconductores,
- el despliegue de la nueva tecnología de **comunicaciones móviles celulares 5G,**
- el desarrollo, protección, y gobernanza de los **cables de datos submarinos**,
- el desarrollo y acceso a **sistemas de supercomputación**,
- la influencia de las **plataformas digitales** en el acceso a los servicios digitales,
- y la protección frente a ataques de **ciberseguridad**.

2.3.2. Acceso a tierras raras para la fabricación de semiconductores

En la figura 10 he identificado un primer nivel relativo a la disponibilidad de los **"materiales"** necesarios para el desarrollo de todo tipo de producto digital. Entre ellos se encuentran los necesarios para la fabricación de baterías, semiconductores, cables (de cobre o fibra óptica), sensores, etc.; todos ellos son productos esenciales en el proceso de digitalización empleados en todos los sectores industriales.

Algunos de estos materiales están ampliamente distribuidos por todo el planeta, se obtienen con **procesos conocidos a costes reducidos** desde hace años[42], y asegurar su disponibilidad a medio o largo plazo no ocasiona un problema ni técnico ni político salvo el adecuar las capacidades de extracción y refino a la demanda lo que puede implicar inversiones recurrentes para mejorar la eficiencia de los procesos, la reducción del consumo de energía, o consideraciones medioambientales en el tratamiento de los residuos[43].

En otros casos, por el contrario, su disponibilidad está concentrada en unos pocos países, su obtención y purificación implica procesos muy costosos y especializados, con **conocimientos protegidos por patentes y secreto industrial** dominados por un pequeño grupo de empresas, y están sometidos a una dura batalla geopolítica por su control.

La existencia de **yacimientos de metales importantes para la fabricación de productos digitales en países en desarrollo** ha llevado a gran-

42 Salvo en lo que se refiere a su alta dependencia del consumo de electricidad necesario con costes muy volátiles sometidos a tensiones geopolíticas como sucede actualmente. También deben tenerse en cuenta los costes derivados de las amortizaciones de inversiones en los robots industriales introducidos para la automatización de procesos.

43 Estas inversiones pueden también proceder de la necesidad en la UE de acomodar los procesos de extracción y refino a legislaciones medioambientales más estrictas como sucede, por ejemplo, con la amplia oposición a la minería a cielo abierto, y los problemas de competitividad derivados de otros países fuera de la UE cuya legislación sea más permisiva.

des empresas mineras, apoyados por sus gobiernos respectivos a una "*batalla*" por el acceso a estos yacimientos en países que se decantan por unos u otras grandes potencias en función de las ayudas recibidas o afinidades ideológicas. Así, el caso de África es especialmente relevante puesto que su acceso se produce en una zona altamente inestable en el que se conjugan los intereses nacionales, de grandes potencias, y de grupos terroristas[44]. En África tanto Estados Unidos, China, Rusia y la UE compiten por el acceso a yacimientos relevantes. Si esa competición favorece o no a los países africanos ha sido debatido con posiciones optimistas (Müller, 2023): "*Los países africanos pueden utilizar el aumento de una nueva geopolítica de las cadenas de suministro de minerales y la competencia entre las principales economías para transformar sus sectores extractivos en una dirección que desbloquee el potencial económico, cree contenido local en el sector minero y contribuya al desarrollo sostenible".* Veremos.

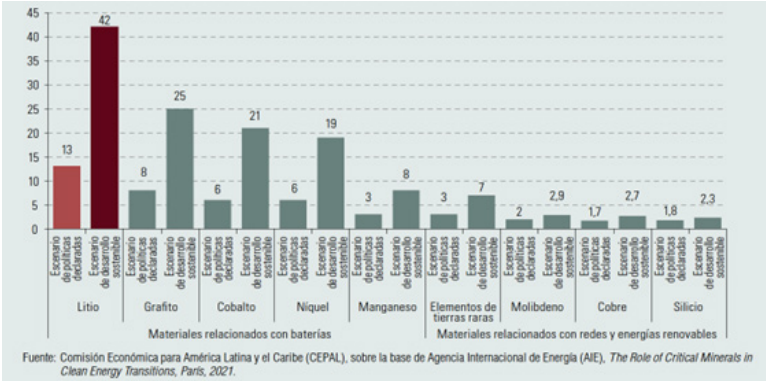


Figura 12. Crecimiento relativo de la demanda de minerales seleccionados utilizados en energías limpias. Fuente: CEPAL, 2023.

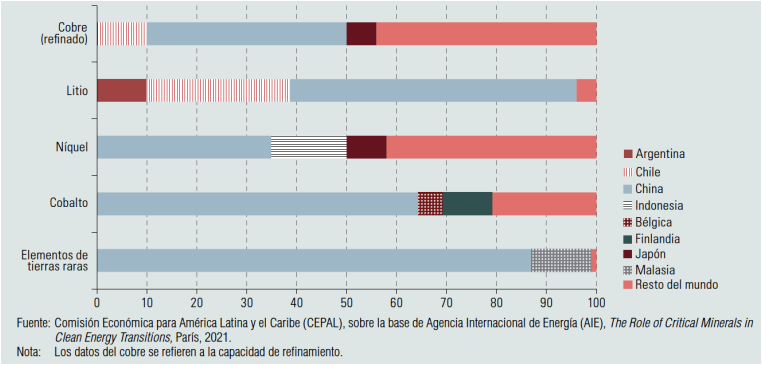
En la figura 12 se puede ver el crecimiento relativo de la **demanda de minerales seleccionados utilizados en energías limpias**, proyección hacia 2040, indicando el número de veces de crecimiento en relación con la demanda existente en 2020. Como se puede ver en la figura 12 el **crecimiento de la demanda de litio** en un escenario de desarrollo sostenible, alimentado por el despegue del vehículo eléctrico y no solo para las baterías de productos digitales como el teléfono móvil, es enorme y no será posible cubrir con la producción actual[45].

Debe distinguirse la ubicación de las **reservas estimadas** de un mi-

44 La franja del Sahara es especialmente rica en fosfatos de los que se obtienen algunas de las tierras raras. Sin embargo, la mayor parte de los yacimientos de tierras raras se encuentran en la zona subsahariana: los más abundantes están en Sudáfrica, Tanzania, Malawi y Mozambique, pero también los hay en Kenia, Burundi, Zambia y Namibia.

45 La demanda de la UE de metales de tierras raras, utilizados en turbinas eólicas y vehículos eléctricos, aumentará de 5 a 6 veces para 2030 (de 6 a 7 veces para 2050). https://ec.europa.eu/commission/presscorner/detail/en/fs_23_1663

neral con la **capacidad de procesamiento** del material que puede concentrarse en otros países como se indica en la figura 13. Obsérvese la situación de fuerza de China en relación con el litio y las tierras raras[46] por su relevancia en el modelo digital.



Fuente: Comisión Económica para América Latina y el Caribe (CEPAL), sobre la base de Agencia Internacional de Energía (AIE), *The Role of Critical Minerals in Clean Energy Transitions*, París, 2021.
Nota: Los datos del cobre se refieren a la capacidad de refinamiento.

Figura 13. Participación en el procesamiento de minerales seleccionados, 2019 Fuente: CEPAL, 2023

Directamente relacionado con la digitalización es necesario también analizar el caso de las **tierras raras empleadas para fabricar dispositivos semiconductores**. No hay transición verde, ni internet, ni investigación en nanomedicina, ni armamento avanzado, básicamente prácticamente no hay soluciones técnicas a nuestros problemas planetarios, sin ellas. En este sector de las tierras raras **China juega un papel decisivo** con un 70% de la distribución mundial en 2022, seguida de Estados Unidos con el 14,3%, según datos de Statista[47]. El padre de la revolución económica de China, Deng Xiaoping, entendió su importancia, señalando: "*El Medio Oriente tiene petróleo. China tiene metales de tierras raras*". (Glenny, 2022).

La producción mundial de tierras raras en 2022 llegó a 300.000 TM, frente a las 290.000 TM del año anterior (datos del Servicio geológico de Estados Unidos)[48]. China ha sido consistentemente el mayor productor de tierras raras, y su producción en 2022 representó 210.000 TM de las 300.000 TM del mundo. En términos de minas específicas de tierras raras, el principal productor es la mina Bayan Obo (figura 14) en Mongolia Interior, una región autónoma en el norte de China.

46 Las "tierras raras" son un conjunto de 17 elementos naturales compuestos por 15 elementos de la serie de lantánidos, más itrio y escandio. Aparte del escandio, todas las tierras raras se pueden dividir en categorías ligeras y pesadas en función de su peso atómico. Las tierras raras pesadas son generalmente más buscadas, pero los elementos ligeros de tierras raras también pueden ser importantes.

47 https://www.statista.com/statistics/270277/mining-of-rare-earths-by-country/

48 Hace solo una década, la producción mundial estaba en las 100.000 TM lo que indica el fuerte incremento de la demanda y la necesidad de incrementar la producción. https://investingnews.com/daily/resource-investing/critical-metals-investing/rare-earth-investing/rare-earth-reserves-country/

Figura 14. Mina de Bayan Obo propiedad de la empresa estatal china Baotou Iron and Steel Group. Fuente: https://www.investmentmonitor.ai/extractive-industries/china-rare-earths-dominance-mining/

En enero de 2022, China anunció la creación de una **empresa estatal**, *China Rare Earth Group*, que controlará el 60-70% de la producción de tierras raras del país (el 30-40% del suministro mundial).

Europa no posee grandes yacimientos de tierras raras en explotación. Sin embargo, a principios de 2023, la empresa estatal sueca LKAB anunció que había identificado el depósito de tierras raras más grande del continente, el depósito *Per Geijer*, con recursos de tierras raras de más de 1 millón de TM de óxidos lo que puede cambiar la situación relativa de la UE si se pusiera en explotación lo que implica inversiones considerables[49]. También en España se han identificado cuatro zonas con reservas de tierras raras[50].

Con la situación de la producción de tierras raras indicada en los párrafos anteriores no es extraño que se hayan producido **tensiones en el acceso a depósitos y en el control del proceso de refinamiento de tierras raras** (similar al caso del litio), pero en este caso como parte de la batalla alrededor de los semiconductores (Fan et al., 2023). El origen de su **planteamiento como un arma geopolítica** es más antiguo y ha sido usada así por China (Zhang et al., 2014).

49 Para extraer solo pequeñas cantidades de los 17 metales de tierras raras se requieren eliminar muchas toneladas de agregado y roca. Sin controles estrictos, esta operación es altamente contaminante. Además, los depósitos de tierras raras están mezclados, por lo que es difícil y costoso separarlos y aprovechar sus propiedades individuales. Finalmente, están ligados a depósitos minerales con un elemento radiactivo de bajo nivel, torio, cuya exposición se ha relacionado con un mayor riesgo de desarrollar cáncer.

50 En España hay identificadas al menos cuatro áreas con presencia de tierras raras: Campo de Montiel (Ciudad Real), la sierra de Galiñeiro (Pontevedra), la Rambla de las Granatillas (Almería) y el complejo basal de Fuerteventura (Las Palmas)

Es evidente para la UE la importancia que ha adquirido la diversificación de sus suministros de tierras raras, aunque el proceso está siendo lento. En 2017, la UE formó la **Alianza Europea de Materias Primas**[51] para comenzar a diversificarse. En ese momento, China suministraba a la UE un asombroso 98% de sus necesidades de tierras raras. Cinco años después, China todavía proporciona el 90% de las tierras raras a nivel mundial (Glenny, 2022). A esta situación se suma las restricciones impuestas por China desde el 1 de agosto de 2023 para la exportación de galio y germanio, materiales necesarios para la fabricación de semiconductores y células solares[52].

El factor positivo es que se van encontrando **nuevos yacimientos en Europa** y parece existir una mayor predisposición en los estados miembros a interpretar las regulaciones medioambientales de una manera más proclive a ponerlos en explotación (p.ej. con minería subterránea y no a cielo abierto) a lo que ayudará la nueva regulación de la UE propuesta por la Comisión Europea en marzo de 2023 y actualmente en discusión (*The Critical Raw Materials Act*) (European Commission, 2023b) con el objetivo de mejorar la capacidad de la UE para supervisar y mitigar los riesgos de perturbaciones en la provisión de materiales críticos, y mejora la circularidad y la sostenibilidad[53].

Para **garantizar la resiliencia de las cadenas de suministro**, El Reglamento propuesto prevé la monitorización continua de las cadenas de suministro de materias primas críticas y la coordinación de las existencias estratégicas de materias primas entre los Estados miembros. En el **contexto internacional** se ha previsto un esfuerzo para coordinar el suministro de materias primas críticas con otros países aliados:

"*La UE tendrá que* ***reforzar su compromiso global con socios fiables para*** *desarrollar y diversificar la inversión y promover la estabilidad en el comercio internacional y reforzar la seguridad jurídica para los inversores****.*** *En particular, la UE buscará asociaciones mutuamente beneficiosas* ***con los mercados emergentes y las economías en desarrollo, especialmente en el marco de su estrategia Global Gateway"***.

51 European Raw Materials Alliance. La alianza se centrará inicialmente en las necesidades más apremiantes: aumentar la resiliencia de la UE en la cadena de valor de los imanes y motores de tierras raras. Son vitales para los ecosistemas industriales clave de la UE, como la automoción, las energías renovables, la defensa y la industria aeroespacial. La alianza se ampliará para abordar otras necesidades críticas y estratégicas de materias primas, incluidas las relacionadas con materiales para el almacenamiento y la conversión de energía (baterías y celdas de combustible). https://erma.eu/

52 A partir de ahora las empresas chinas se ven obligadas a obtener una licencia de exportación del gobierno chino. Se hace valer con ello la fuerte posición de China en galio (el 94% de la producción mundial) y de germanio (alrededor del 60%). https://www.anandtech.com/show/19989/china-imposes-new-export-restrictions-on-gallium-and-germanium

53 Algunas grandes empresas tendrán que realizar una auditoría de sus cadenas estratégicas de suministro de materias primas, que comprende una prueba de resistencia a nivel de empresa. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1661

El reglamento en proceso de negociación en la UE establece cuatro objetivos cuantitativos ambiciosos[54]:

- *Como mínimo, debe conseguirse un 10% del consumo anual extraído en la UE.*
- *Como mínimo, debe conseguirse un 40% del consumo anual procesado en la UE.*
- *Como mínimo, debe conseguirse un 15% de reciclado del consumo anual en la UE.*
- *Como máximo, el 65% del consumo anual de cada materia prima estratégica en cualquier fase relevante del procesamiento, procederá de un único país fuera de la UE.*

Confío en que con el paso del tiempo la explotación de nuevos yacimientos, y si se cumplen los objetivos del reglamento europeo en discusión, la reducción de los riesgos de suministros, las tierras raras serán "*menos raras*".

2.3.3.Comunicaciones móviles celulares 5G

Unas decisiones que han alcanzado cotas especialmente relevantes de confrontación geopolítica entre potencias tecnológicas son las relativas al **despliegue de la tecnología 5G**. Sobre ellas, se está generando una feroz **competencia tecno-política** (sobre todo, entre China y Estados Unidos) con ramificaciones en todo el mundo en las que la UE también está implicada. Esta batalla se prolongará previsiblemente con la siguiente generación 6G en desarrollo actualmente (Nocetti, 2022).

Se trata de un despliegue tecnológico costoso que requerirá gran parte de esta década para que alcance a toda la población y territorio europeos. La actual **quinta generación de comunicaciones móviles celulares (5G)** es una tecnología que servirá de base para el despliegue de multitud de aplicaciones de comunicaciones móviles de banda ancha no solo entre personas, sino también y fundamentalmente entre máquinas, ligada a otra tecnología que es el **Internet de las cosas (IoT)** y el abaratamiento de los sensores inteligentes asociados con aplicaciones tanto civiles como militares.

La figura 15 permite ver los datos fundamentales entre **generaciones de comunicaciones móviles**, sin incluir (Tufail et al., 2021) la que se denomina 6G que se encuentra actualmente en pleno proceso de desarrollo y normalización, pero que su despliegue se realizará básicamente durante la siguiente década de los años 2030.

54 https://ec.europa.eu/commission/presscorner/detail/en/fs_23_1663

El desarrollo del vehículo autónomo, por ejemplo, requerirá acelerar el despliegue de 5G con anchos de banda y latencias muy inferiores a los ofrecidos por la generación actualmente desplegada casi totalmente (la denominada 4G) para que sea factible. Pero otros muchos ámbitos innovadores como la telecirugía en tiempo real o las redes móviles en defensa incorporando señales de múltiples sensores dependerán también de ella para poder incorporar aplicaciones disruptivas. En el campo de la defensa, las redes 5G junto con algoritmos de inteligencia artificial y el despliegue de pequeños sensores permitirán conectar soldados, vehículos y robots autónomos a gran velocidad. 5G también jugará un papel importante en la creación de la "nube de combate", debido a su capacidad para conectar millones de sensores dentro de una determinada área.

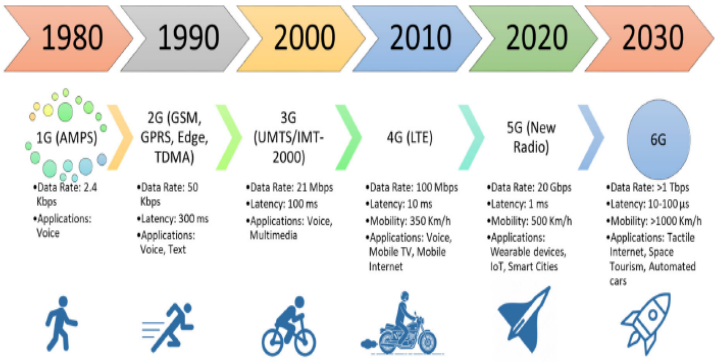


Figura 15. Evolución de las comunicaciones móviles celulares. Fuente: Tufail et al., 2021

La gobernanza de las comunicaciones móviles es **un ámbito tecnológico fuertemente regulado** con el fin de asegurar el **uso del espectro radioeléctrico** de manera eficiente y sujeto a licitaciones de las administraciones públicas nacionales para la concesión de las bandas de frecuencia concretas en las que se pueden proveer servicios de comunicaciones en función de la tecnología. En la práctica los gobiernos *"subastan"* entre potenciales proveedores de servicios estas frecuencias (se trata de una competencia nacional) con unas condiciones ligadas a la forma en la que deben desplegarse, y las coberturas territoriales y poblacionales requeridas en determinados periodos.

La UE que mantuvo una posición central en el desarrollo de la tecnología 3G consiguiendo la autonomía estratégica completa en este ámbito, la perdió en el desarrollo de 4G, y ahora se encuentra en una **situación compleja en relación con 5G** con la que se juega en muy pocos años su relevancia en un enorme mercado creciente durante esta década[55].

55 El mercado de 5G tenía una valoración de solo 5.130 millones de dólares en 2020, pero se estima que alcance los 798.000 millones en 2030 (un CAGR del 65,8%). https://www.alliedmarketresearch.com/5g-technology-market

Tras las asignaciones de frecuencias efectuadas para 5G, 25 Estados miembros de la UE habían iniciado **despliegues comerciales de redes 5G a mediados de 2021**, sobre todo, en zonas urbanas densamente pobladas. La cobertura 5G aumentó sustancialmente del 14% de las áreas pobladas en 2020 al 66% en 2021. Una parte significativa de esta cobertura se logró utilizando inicialmente tecnología de red 4G (se denomina *NSA "non-stand alone"*) con el fin de facilitar a los operadores resarcirse de las inversiones realizadas en el despliegue de 4G y facilitar que los usuarios dispusieran de terminales adaptados (p.ej. terminales móviles)[56] que, posteriormente, se transformarán en redes 5G nativas (*SA, stand alone*).

Lograr una **cobertura universal en 5G** para toda la población en territorios extensos requiere una decisión política prolongada en el tiempo puesto que las inversiones para sustituir las infraestructuras de red existentes son elevadas, y el interés de los usuarios dependerá de las aplicaciones específicas que requieran realmente disponer del ancho de banda y la baja latencia de 5G. Por este motivo, en casi todos los países los planes de despliegue de 5G pueden durar más de una década. La figura 16 permite ver la situación actual comparada del despliegue de 5G entre la UE y otros grandes países avanzados. Obsérvese la posición de liderazgo de China en el número de estaciones base y de usuarios.

	China	South Korea	Japan	USA	EU
5G Mode	NSA/SA	NSA/SA	NSA/SA	NSA	NSA/SA
Approximate number of 5G base stations	1,850,000	215,000	50,000	100,000	256,074
Total country population	1,402,000,000	51,780,000	125,800,000	329,500,000	447,706,000
5G base stations per 100,000 inhabitants	132	415	40	30	57
Indicative 5G subscribers	**357 million** (source: Ericsson 2022)	**25 million** (source: Ministry of Science and ICT)	**14.19 million** (source: Japan times)	**79 million** (including Canada; source: Ericsson 2022)	**31 million** (including all of western Europe; source: Ericsson 2022)

Figura 16. Situación global del despliegue 5G. Fuente: Observatorio europeo de 5G https://5gobservatory.eu/observatory-overview/interactive-5g-scoreboard/

La realidad es que en 2019 **China tenía una posición privilegiada en 5G** (aunque fuese en bandas de frecuencias bajas y medias con sistemas más baratos). Una de sus empresas, ***Huawei,*** y, en menor medida, **ZTE**,

56 A pesar de ello, en los dos últimos años los modelos de teléfonos móviles inteligentes de gamas media y alta comercializados en la UE ya incorporan la capacidad de emisión y recepción 5G, aunque las redes básicas sigan siendo de 4G.

habían logrado una cuota de mercado muy elevada y habían comenzado a desplegar equipos de red en muchos países, entre ellos los de la UE, puesto que podía ofrecer sistemas con **prestaciones elevadas y bajos costes** cuando las empresas de otros países desarrollados no estaban preparadas para competir comercialmente.

En 2019, el gobierno de Estados Unidos, aduciendo la existencia de problemas de **seguridad nacional** derivados de las relaciones entre los proveedores (empresas privadas) y el gobierno chino, con implicaciones en el ámbito de defensa[57], y el posible acceso a información sensible a través de los sistemas de telecomunicación, **veta el acceso al mercado de Estados Unidos para el despliegue de 5G a Huawei, y presiona a otros países aliados para que hagan lo mismo**. Con ello, además, gana tiempo para que las empresas de Estados Unidos reduzcan el retraso y estén preparadas para ofertar productos y servicios avanzados 5G.

El efecto perseguido al negar el acceso al mercado estadounidense a las empresas chinas y aquellas cuyos productos contienen más del 25% de componentes fabricados en Estados Unidos era frenar el desarrollo de China. La administración de Estados Unidos (del presidente Trump) **frenó significativamente la expansión internacional de Huawei** y servía de recordatorio al mundo del considerable margen de maniobra que Estados Unidos tiene sobre cadenas de valor tecnológicas globales al ligarlo a su política restrictiva sobre semiconductores[58]. La diferencia con respecto a otras políticas previas de sanciones económicas es que ahora se aplicaba a cualquier empresa que utilizase tecnología de Estados Unidos, independientemente de si esa empresa fuese americana o no.

Aunque inicialmente, Huawei podría seguir suministrando equipos 4G, **la decisión supuso en 2022 una reducción en el beneficio neto de Huawei del 68,7% frente al año anterior** dado que afectó también a su mercado de teléfonos móviles 5G. Ello ha forzado a Huawei y a SMIC (empresa china fabricante de semiconductores) a acelerar el desarrollo de chips compatibles 5G sin depender de Estados Unidos, aunque con una producción y resolución menor (7nm) de lo que podría obtener fabricando con TSMC[59].

La decisión de Estados Unidos arrastrando a otros países avanzados no ha frenado a China en continentes como África, pero encontraba a Eu-

57 No se olvide que se trata de una tecnología dual que empieza a utilizarse en aplicaciones militares por lo que su relevancia geopolítica crecerá.

58 En mayo de 2020, la administración Trump anunció que prohibiría a todos los productores de componentes electrónicos que utilizan tecnología estadounidense fabricar chips para Huawei, sin importar dónde se encontraran. Tres meses después, el Departamento de Comercio reforzó las medidas que prohíben todas las ventas de semiconductores a Huawei. A finales de año, Washington había ampliado las restricciones para apuntar a docenas de otras compañías chinas, incluida SMIC, la fábrica de semiconductores más importante de China (Nocetti, 2022).

59 https://www.phonearena.com/news/huawei-to-release-5g-phone-later-this-year_id148836.

ropa a comienzos de 2020 en una buena posición en el despliegue de 5G con un **uso elevado de equipos de Huawei o ZTE en sus redes** (casi el 60% de las redes 5G que se han desplegado en 2022 en la UE cuentan con presencia de componentes procedentes de Huawei o ZTE, aunque con diferencias significativas entre los estados miembros[60]).

El problema para la UE, evidentemente, no es técnico sino político y económico. Si la UE frenase su despliegue de 5G perdería una posición de ventaja relativa frente a otros países que no podría recuperar fácilmente, y debería realizar nuevas inversiones para sustituir los equipos adquiridos a Huawei. Tampoco puede la UE ser competitiva en toda la cadena de valor de 5G (da Ponte, León y Álvarez, 2022). Dado que **la autonomía estratégica de la UE en 5G es limitada** y los gobiernos europeos han actuado con "*pies de plomo*" en la adopción de decisiones que, formalmente, corresponden a los operadores privados de telecomunicación, aunque se fuerce la situación actuando sobre las condiciones de las nuevas licitaciones públicas que se hagan para su despliegue.

En el marco del conjunto de instrumentos de la UE, con el objetivo último de **garantizar la seguridad y la resiliencia de las redes 5G y su sostenibilidad**, los Estados miembros convinieron en la necesidad de **evaluar el perfil de riesgo de los distintos proveedores** y, en consecuencia, de aplicar las restricciones pertinentes a los proveedores considerados de alto riesgo, incluidas las exclusiones necesarias para reducir eficazmente los riesgos, en el caso de los activos clave. La Comunicación de la Comisión Europea en junio de 2023 (European Commission, 2023b) expresaba la **preocupación sobre la ciberseguridad 5G** en los siguientes términos:

"*Debido a estos graves riesgos, y sobre la base de una evaluación de los criterios establecidos en el conjunto de instrumentos para identificar a los «proveedores de alto riesgo», la Comisión considera que las decisiones adoptadas por los Estados miembros en el sentido de aplicar restricciones o excluir a Huawei y ZTE están justificadas y son conformes con el conjunto de instrumentos de la UE para la seguridad de las redes 5G… Como parte de su política institucional de ciberseguridad, y en aplicación del conjunto de instrumentos de la UE para la seguridad de las redes 5G, la Comisión adoptará medidas para evitar la exposición de sus comunicaciones corporativas a las redes móviles que utilizan Huawei y ZTE como proveedores. Estas medidas incluirán la no adquisición de nuevos servicios de conectividad que dependan de equipos de esos proveedores en aplicación de las condiciones de seguridad pertinentes".*

60 Como ejemplo de esta diversidad, a finales de 2022, toda la red 5G de Chipre es de Huawei, Rumanía (79%), Países Bajos (72%), Bulgaria (62%), Austria (61%), Alemania (59%), España (38%), Francia (17%). https://www.elconfidencial.com/tecnologia/2022-12-21/huawei-medula-redes-europeas-operadoras_3543416/

A pesar de ello, en junio de 2023 **únicamente diez estados miembros de la UE habían seguido las prohibiciones a Huawei y ZTE** impulsadas por Estados Unidos, a pesar del alineamiento de la Comisión Europea en relación con la ciberseguridad en 5G[61]. La UE cuenta con dos grandes fabricantes de sistemas móviles 5G "de confianza": Ericsson (Suecia) y Nokia (Finlandia), aunque compitan entre ellos y tengan costes más elevados que los de Huawei, la desaparición de competidores contribuirá a crear un "*oligopolio 5G*" de hecho[62]. El riesgo puede reducirse si se aceptase una arquitectura abierta de acceso abierto a las redes[63].

La historia de los problemas geopolíticos del despliegue de 5G se puede repetir en torno a la **siguiente generación de comunicaciones móviles celulares (6G)** cuyo desarrollo técnico y normalización se realizará durante la presente década (en paralelo con la evolución y despliegue de 5G). Esto explica también la batalla alrededor de los estándares 6G y el interés en "dominar" los grupos técnicos dedicados a ello.

Si un país consiguiera **desplegar rápidamente redes 6G** en zonas de su territorio, dotar a los usuarios de los terminales adecuados, y desarrollar casos de prueba convincentes, adelantándose en el tiempo dos o tres años a los planes de sus competidores, sus empresas serían capaces de desarrollar aplicaciones específicas para 6G y asegurarse una cuota elevada en un enorme mercado futuro. Esto es lo que está intentando China. Otros desarrolladores que entren después procedentes de otros países tendrán más dificultades para acceder al mercado y probar sus soluciones.

Esta rápida evolución hacia 6G ha llevado a la UE y a Estados Unidos a comprometerse a colaborar en estos años para desarrollar una visión común basada en los siguientes principios rectores (European Commission, 2023c):

- *Las tecnologías 6G deben estar en consonancia con principios y valores comunes como la sostenibilidad, la privacidad, la accesibilidad, la apertura y la inclusión. Los sistemas de comunicación inalámbrica 6G deben ser confiables, resistentes y asequibles y contribuir a cerrar las brechas digitales tanto en los países desarrollados como en los países en desarrollo.*
- *Del mismo modo, las normas 6G deben permitir una conectividad mejorada, incluida, entre otras, la conectividad satelital directa al dispositivo (D2D) en un entorno abierto e interoperable. Esto ayudaría a*

61 https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3309

62 Nokia es el único fabricante, aparte de Huawei, que domina todo el espectro de la tecnología 5G, desde el acceso a la red hasta el transporte, pasando por la agregación de tráfico, la transmisión óptica, la conmutación, el enrutamiento e incluso el acceso a los cables submarinos.

63 Este es el objetivo de la iniciativa OPEN-RAN a la que se han sumado muchos fabricantes y operadores de comunicaciones de todo el mundo. https://www.o-ran.org/resources

garantizar la conectividad de banda ancha en todo el mundo, incluso en las zonas rurales y de bajos ingresos.

- *Las tecnologías 6G también deben ser un facilitador de la sostenibilidad, teniendo en cuenta las perspectivas ambientales, sociales y económicas. Una huella de carbono reducida y la eficiencia energética serán objetivos de diseño importantes para las redes 6G. En términos más generales, 6G debería permitir reducir el consumo de energía en todos los sectores de la economía y la sociedad.*
- *Los estándares 6G deben desarrollarse con seguridad por diseño, estar dirigidos por el sector privado y basarse en principios basados en el consenso para permitir un ecosistema de soluciones 6G resilientes, abiertas, interoperables y basadas en software. Las normas 6G deben ser establecidas de manera transparente por las organizaciones de normalización de conformidad con los principios pertinentes de la OMC sobre obstáculos técnicos al comercio.*

Los próximos años serán cruciales para ver si este acercamiento se concreta en medio de la confrontación geopolítica actual o, por el contrario, servirá para que la UE acepte los postulados de Estados Unidos. En mi opinión, las posiciones de fuerza respectivas no son simétricas.

2.3.4. Comunicaciones internacionales mediante cables submarinos

El tercer punto de fricción geopolítica que deseo mencionar es el de las **comunicaciones de datos internacionales** empleadas para el acceso a servicios digitales de internet. Ya no se trata, por tanto, de asegurar el intercambio de productos físicos, utilizando rutas terrestres, marítimas o aéreas, sino del intercambio de **información**, lo que implica el uso de un medio físico de transmisión digital terrestre, inalámbrico, espacial o submarino.

Desde el punto de vista de la transferencia de datos internacionales, la UE está conectada al resto del mundo en base, fundamentalmente, al empleo de **cables internacionales submarinos de gran capacidad** (actualmente, estos cables transportan el 95% del tráfico de datos); el resto del tráfico no terrestre se realiza mediante **comunicaciones satelitales**[64]. El **tendido y mantenimiento en aguas internacionales** de estos cables submarinos de datos supone, además, un problema de gobernanza puesto que se trata de tendidos que no se circunscriben a aguas territoriales de ningún país y para los que la legislación internacional aplicable no es muy adecuada[65].

64 Salvo, obviamente, las comunicaciones terrestres entre países que compartan frontera; básicamente, mediante cables de fibra óptica de gran capacidad.

65 La Convención de las Naciones Unidas sobre el Derecho del Mar (UNCLOS) es un tratado que establece un marco legal integral que regula las actividades dentro de las zonas marítimas. Describe los derechos y responsabilidades con respecto al uso de los recursos en estas regiones, incluidos los cables submarinos. Para ver los problemas de UNCLOS: https://jamestown.org/program/laying-down-the-law-under-the-sea-analyzing-the-us-and-chinese-submarine-cable-governance-regimes/

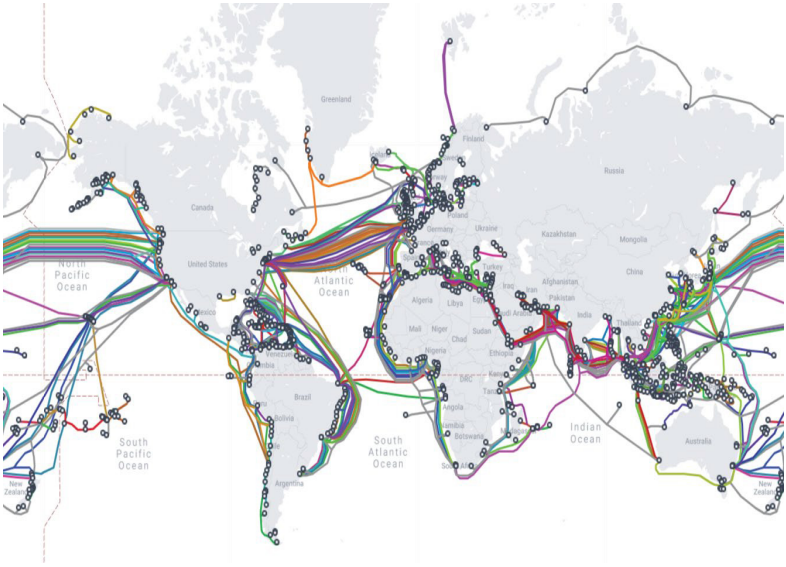


Figura 17. Tendido de cables submarinos.
Fuente: Telegeography https://www.submarinecablemap.com

La figura 17 representa en un mapa la **situación actual de los principales cables submarinos**. Obsérvense los dos grandes focos de concentración de cables: las conexiones entre Estados Unidos y Europa, y las de Estados Unidos con Asia, reflejando también la relevancia de los flujos de datos y la relación entre las economías mundiales.

España ha sido de hecho la receptora de algunos de los cables de última generación que unen el continente americano con el europeo, a través del cable **Marea** (propiedad de Meta, Microsoft y Telxius, anclado a Vizcaya en 2018), el **Grace Hopper** (terminado por Google en 2022, en la misma zona) y el **Anjana** (también propiedad de Meta, cuya construcción terminará a finales de 2024 y unirá Carolina del Sur y Santander).

Las inversiones para el tendido de estos cables siguen, en su mayor parte una **lógica comercial**: asegurar la capacidad necesaria para el creciente tráfico internacional de datos. Sin embargo, también se han tenido en cuenta **consideraciones políticas** de servir de instrumento para mejorar las relaciones internacionales entre países, evitar el estrangulamiento o no depender de cables que supongan un riesgo político. Un ejemplo en este sentido *("poder blando")* en el que está implicada la UE es el programa ***BELLA***.

El programa **BELLA II** (*Building the Europe Link to Latin America and the Caribbean*)[66] firmado en diciembre de 2022 para dar continuidad al anterior surge en un contexto geopolítico de fortalecer y expandir el ecosistema digital de América Latina y el Caribe, posibilitando relaciones e intercambios entre empresas, centros de investigación, instituciones educativas y redes académicas latinoamericanas y europeas para "*contribuir al logro de los objetivos estratégicos de la región enfocados en el fortalecimiento de la educación, la ciencia, la tecnología y la innovación".*

La consideración de BELLA 2 como parte de la iniciativa *Global Gateway EU*, respuesta de la UE a la iniciativa de la **Ruta de la Seda de China**[67] (Cheng and Zheng, 2023b) (Xiao y Ding, 2023) basada en préstamos a largo plazo de bajo interés, le confiere un valor geopolítico mayor en la batalla por la influencia en Latinoamérica de las grandes potencias[68].

Estas comunicaciones submarinas no están exentas de riesgos. La **rotura**, intencionada o no, de unos cuantos cables submarinos de los de mayor capacidad tendidos en el Atlántico tendría un impacto enorme en el funcionamiento de la mayor parte de los servicios digitales del mundo y, sobre todo, entre Europa y Estados Unidos (y de ahí a las de Europa con Asia).

En un estudio de junio de 2022 presentado al Parlamento Europeo (Bueger et al., 2022) se analizaban los **riesgos derivados de la rotura de los cables submarinos**, tanto los **accidentales** (p.ej. derivado de una erupción volcánica submarina) como los **intencionados** (p.ej. derivado de un ataque terrorista sobre un cable o de un sabotaje para robar el material)[69]. En todo caso, parece más sencillo atacar (físicamente o mediante ciberataques) las **estaciones en tierra** (*Cable Landing Stations, CLS*) que conectan los cables en la costa y proporcionan electricidad. Las zonas en las que decenas de cables entran en una estación, como ocurre en Marsella (Francia) o en Sesimbra (Portugal), son objetivos tentadores y puntos débiles significativos.

66 Está cofinanciado por la DG INTPA de la Comisión Europea (CE), a través del Instrumento de Vecindad, Desarrollo y Cooperación Internacional – Una Europa Global (IVDCI). La contribución de la CE es de 13.000.000 de euros; RedCLARA, la institución ejecutora y coordinadora, buscará complementar -a través de la alianza con gobiernos, empresas privadas, bancos y otros- esta cantidad 15 millones de euros para cumplir todos los objetivos. https://www.bella-programme.eu/index.php/en/

67 El concepto fue planteado por el presidente de China Xi Jinping en 2017: "Debemos perseguir el desarrollo impulsado por la innovación e intensificar la cooperación en áreas fronterizas como la economía digital, la inteligencia artificial, la nanotecnología y la computación cuántica, y avanzar en el desarrollo de macrodatos, computación en la nube y ciudades inteligentes para convertirlas en una ruta de la seda digital del siglo XXI".

68 https://international-partnerships.ec.europa.eu/policies/programming/programmes/bella-building-europe-link-latin-america_en

69 A principios de febrero de 2023, los dos cables que conectan las Islas Matsu en el extremo norte del Estrecho de Taiwán con el propio Taiwán fueron rotos por barcos chinos en incidentes separados en el transcurso de una semana; no se ha demostrado que fuera un hecho fortuito o provocado. https://rogeliogonzalez.mx/geopolitica/taiwan-riesgos-en-infraestructura-y-geopolitica-causan-salida-de-cias-como-apple-y-microsoft-a-terceros-paises/

Parecería que esa hipótesis no supone un peligro real en Europa. Sin embargo, el **atentado sobre *Nord Stream II*** en septiembre de 2022 en el mar Báltico (aunque fuese una conducción de gas), e independientemente de su autoría, indica que todo es posible. La presencia de submarinos rusos en las rutas de estos cables y su seguimiento por submarinos de la OTAN demuestra hasta qué punto se ha convertido en un peligro real (Hartmann, 2023)[70]. Esta situación ha llevado a que diez países europeos Noruega, Suecia, Finlandia, Estonia, Letonia, Lituania, Dinamarca, Países Bajos, Reino Unido e Islandia, hayan firmado en junio de 2023 una **alianza militar para proteger los cables de datos del Mar Báltico, el Mar del Norte y las aguas del norte del Océano Atlántico**.

El problema de gobernanza se complica porque **muchos cables submarinos son propiedad principalmente de conglomerados de empresas privadas de telecomunicaciones** que comparten sus costes. Si bien la información sobre los propietarios de cables es conocida, existe poca información sobre los operadores y compradores de las capacidades de esos cables. Los gigantes tecnológicos que proporcionan contenidos digitales como Microsoft, Amazon, Meta y Google han construido y cofinanciado sus propios sistemas de cable en los últimos años, solos o formando parte de consorcios, **para asegurar el tráfico requerido para el funcionamiento y expansión de sus servicios digitales.**

En el contexto geopolítico actual derivado de la invasión de Rusia a Ucrania, la competencia sistémica creciente entre Estados Unidos y China, o la inestabilidad en varias partes del mundo hace que la **seguridad de estos cables submarinos** sea aún más relevante (Bueger et al., 2022). Un ejemplo de las crecientes turbulencias geopolíticas se manifiesta en los **cambios de ruta de algunos cables submarinos** entre Asia y Estados Unidos que se encuentran en el proceso de tendido en el Océano Pacífico y que han modificado su planificación inicial para evitar determinados destinos potencialmente conflictivos como Hong Kong (Mok, 2023). Esto ha llevado también a retirar al gobierno de China o a sus grandes empresas como uno de sus inversores como parte de una política de **"desacoplamiento de infraestructuras digitales"**[71]. En definitiva, no es posible aislar el despliegue de las infraestructuras de comunicaciones avanzadas entre países de los conflictos geopolíticos.

70 Atacar los cables de datos en aguas profundas, donde su posición permanece clasificada y puede ser desplazada por las corrientes, es más difícil. Sin embargo, una vez localizados, pueden ser destruidos por explosivos activados a distancia y vehículos sumergibles tripulados o no tripulados. Un informe reciente, identificó varios presuntos barcos espías rusos disfrazados de buques de pesca e investigación en el Mar Báltico de los que se sospechaba que recopilaban información sobre la ubicación exacta de la infraestructura submarina

71 Como ejemplo, el cable submarino denominado Bay-to-Bay (BtoBE), con Meta, Amazon, y China Mobile como socios, debía conectar California directamente con Hong Kong, y luego Singapur y Malasia. Se ha reconfigurado para terminar en Filipinas eliminando a Hong Kong como destino final.

En este ámbito tanto la UE como Estados Unidos han decidido aunar esfuerzos para conseguir **cables submarinos confiables**. En la Declaración conjunta de 31 de mayo de 2023 del *Trade and Technology Council* (TTC) entre la UE y Estados Unidos, órgano creado para la cooperación entre ambos, se acordó[72]:

"La Unión Europea y los Estados Unidos reconocen la importancia estratégica de la conectividad internacional para la seguridad y el comercio. Con este fin, nuestro objetivo es avanzar en la cooperación para promover la selección de proveedores de cable submarino de confianza para nuevos proyectos de cable, en particular para proyectos de cable digitales intercontinentales que promuevan proveedores confiables, reduzcan la latencia y mejoren la diversidad de rutas. Tenemos la intención de continuar las discusiones para garantizar la conectividad y la seguridad de los cables submarinos transatlánticos, incluso en rutas alternativas que conecten Europa, América del Norte y Asia.

Es evidente que en el futuro la **relevancia geopolítica de los cables submarinos** hará que la participación de los gobiernos en su desarrollo y despliegue se convierta en un **elemento clave que modulará los intereses puramente comerciales de las grandes empresas.**

2.3.5. Desarrollo y acceso a sistemas de supercomputación

El desarrollo continuo de sistemas de computación (ordenadores en la terminología española derivada de la francesa) desde la II Guerra Mundial ha estado impulsado por la necesidad de realización de **cálculos cada vez más complejos** que no era posible llevar a cabo en tiempos razonables con los equipos de computación existentes hasta entonces.

A los ordenadores más potentes en cada momento se les ha denominado históricamente **"supercomputadores"** y a las tecnologías informáticas que permitían desarrollar estos equipos, incorporando un número creciente de unidades de procesamiento, y aprovechar al máximo su potencia de cálculo **"computación de altas prestaciones"** ("*high performance computing", HPC*). Se generaba con ello una ***"carrera tecnológica en supercomputación"*** entre países y grandes empresas con el objetivo de conseguir (super)ordenadores más potentes frente a los disponibles anteriormente y frente a los que poseían otras potencias tecnológicas en cada momento con el fin de conseguir la superioridad en el ámbito de uso deseado.

La velocidad de estas máquinas se mide en **petaflops** (miles de billones de operaciones de punto flotante por segundo) que indica la capacidad de cálculo que pueden alcanzar. El ordenador más potente del mundo ha ya superado la capacidad de cálculo de 1 EXAFLOP. Dos veces al año se publica por la organización TOP500 una lista de los 500 supercomputado-

72 https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2992

res más potentes de acuerdo con los resultados de una serie de pruebas controladas "High-Performance Linpack Benchmark test" (el primer listado se publicó en 1993). En el último listado de mayo de 2023[73] los tres equipos más potentes están situados en Estados Unidos, en Japón y en la UE:

- ***Frontier*** *es el sistema número 1 en el TOP500. Este sistema HPE Cray EX es el sistema de Estados Unidos más potente con un rendimiento superior a un Exaflop/s. Está instalado en el Laboratorio Nacional de Oak Ridge (ORNL) en Tennessee, EE. UU., donde es operado por el Departamento de Energía (DOE). Actualmente ha alcanzado 1.194 Eflop/s utilizando 8.699.904 núcleos.*
- ***Fugaku****, el sistema n.º 2, está instalado en el Centro RIKEN de Ciencias Computacionales (R-CCS) en Kobe, Japón. Tiene 7.630.848 núcleos, lo que le permitió alcanzar una puntuación de referencia HPL de 442 Pflop/s.*
- ***LUMI****, otro sistema HPE Cray EX instalado en el centro EuroHPC[74] de CSC en Finlandia, ocupa el tercer puesto con un rendimiento de 0,3091 Eflop/s.*

En las siguientes posiciones se encuentran: el 4º es **Leonardo** situado en otro nodo de EurpoHPC (CINECA) en Italia, el 5º puesto es de **Summit**, en Oak Ridge National Laboratory (ORNL) (Tennessee, Estados Unidos), el 6º puesto pertenece a **Sierra**, en el Lawrence Livermore National Laboratory (California, Estados Unidos), el 7º puesto corresponde a **Sunway TaihuLight**, instalado en el National Supercomputing Center en Wuxi (Juangsu, China). En la figura 18 se puede ver una imagen de ***"Frontier"*** el supercomputador más potente del mundo en junio de 2023.

Figura 18. Supercomputador "Frontier" (Oak Ridge, National Lab, Estados Unidos). Fuente: https://www.ornl.gov/news/frontier-supercomputer-debuts-worlds-fastest-breaking-exascale-barrier

73 https://www.top500.org/news/frontier-remains-sole-exaflop-machine-and-retains-top-spot-improving-upon-its-previous-hpl-score/

74La Empresa Común Europea de Informática de Alto Rendimiento (Empresa Común EuroHPC) está poniendo en común recursos europeos para desarrollar superordenadores de exaescala de gama alta para el procesamiento de macrodatos. Uno de los superordenadores paneuropeos de pre-exaescala, LUMI, se encuentra en el centro de datos de CSC en Kajaani, Finlandia.

En España, el equipo más complejo que ha sido adquirido es el que posee el Centro Nacional de Supercomputación en el *Barcelona Supercomputing Center (BSC)* denominado ***MareNostrum 4*** (el primero de ellos fue instalado en 2004) con una potencia pico máxima de 13,9 Petaflops. La figura 19 permite ver una imagen del mismo situado en el campus de la Universidad Politécnica de Cataluña. La siguiente versión el **MareNostrum 5 disponible desde diciembre 2023**, ya no es una máquina pagada por el Gobierno español, sino también por la Generalitat y los gobiernos de Portugal, Turquía y Croacia junto a la Comisión Europea aportando un 50% con una inversión total cercana a 600 millones de euros.

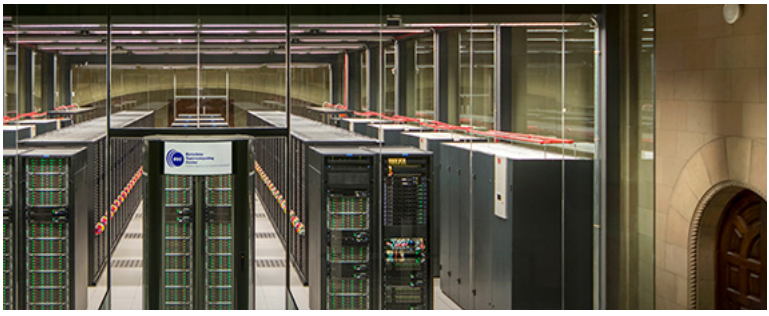


Figura 19. Supercomputador MareNostrum 4 del BSC. Fuente: https://www.bsc.es/marenostrum/marenostrum

Debe tenerse en cuenta que China decidió en 2018 no presentar los datos de sus supercomputadores candidatos al TOP500 para evitar sanciones de Estados Unidos. Por este motivo, no aparecen formalmente, aunque científicos indican que el nuevo supercomputador chino **New Generation Sunway** tiene cuatro veces más núcleos de proceso que el *Frontier* americano que es el supercomputador más rápido del planeta según el ranking Top500 y, habrá alcanzado mucha mayor potencia de cálculo que el de Estados Unidos[75].

En resumen, **Estados Unidos, la UE, Japón y China, cuatro grandes potencias tecnológicas, compiten en disponer de los supercomputadores más potentes**. Rusia ya no se encuentra en los primeros puestos.

El uso de supercomputadores permite la **ejecución y simulación de modelos muy complejos de múltiples sistemas en campos civiles** (p.ej. modelos climáticos o del funcionamiento de drogas en el cuerpo humano) **o militares** (p.ej. modelos de simulación de armas nucleares o de misiles)

75 Un informe no confirmado asegura que la nueva Sunway ha llegado a alcanzar los 4,4 exaflops. La New Generation Sunway es sólo uno de tres superordenadores de exaescala chinos. Tianhe 3 del Centro Nacional de Supercomputación de Tianjin y la tercra es construida por la compañía de supercomputadores Sugon, una de las 12 empresas chinas relacionadas con este sector que está en la lista negra del gobierno federal de los EEUU. https://www.elconfidencial.com/tecnologia/novaceno/2022-06-24/china-sunday-superordenador_3448866/

que dotaba a quienes lo poseían de ventajas sobre otros competidores. Sus campos de aplicación se extienden a áreas tan diversas como la armamentística, la industria farmacéutica, la gestión de grandes volúmenes de datos (*big data*), la bioinformática, la astrofísica, la educación, las finanzas, la geofísica, la ingeniería, la seguridad pública o las ciudades inteligentes por citar algunas de ellas. Este interés se ha incrementado por la necesidad de **entrenar a algoritmos de inteligencia artificial** basados en modelos grandes de lenguaje empleando un volumen muy elevado de datos.

Dado el **carácter dual** de estos grandes sistemas de computación, la implicación de los gobiernos de los países en su financiación, la posibilidad de usarlos de forma remota, y su relevancia estratégica, no es extraño pensar en la relevancia que se ha dado a controlar el uso de los mismos por parte de los países que lo poseen, limitando el acceso a posibles usuarios no nacionales, y a controlar la transferencia de tecnología para poder fabricar uno similar mediante restricciones a la exportación de componentes críticos (p.ej. circuitos integrados empleados en su desarrollo) y software de gestión del mismo.

Como muestra de esta preocupación, en noviembre de 1997, en una sesión del *Comité de Seguridad Nacional del Congreso de Estados Unidos* en relación con los controles de exportación de supercomputadores y las dificultades en controlar el cumplimiento de los controles establecidos, el Presidente del Comité decía[76]:

"Desde que la administración relajó su política el año pasado sobre las exportaciones de supercomputadoras, ha habido numerosas revelaciones sobre el envío no autorizado o el desvío de supercomputadoras fabricadas en Estados Unidos a países y entidades de preocupación por la proliferación. Nos hemos enterado de que las supercomputadoras de los Estados Unidos han sido enviadas de manera inapropiada a instalaciones de investigación militar en China y a laboratorios de armas nucleares en Rusia. Según admiten los funcionarios rusos, estas computadoras se utilizarán para ayudar a mantener el arsenal de armas nucleares de Rusia. Artículos de prensa recientes también indican que otros 16 ordenadores de alto rendimiento fabricados en los Estados Unidos fueron obtenidos ilegalmente por un laboratorio ruso de armas nucleares utilizando intermediarios europeos, en violación de las normas de control de las exportaciones de los Estados Unidos".

En estos momentos, la preocupación de Estados Unidos por el uso indebido de grandes supercomputadores se ha focalizado en **China** que ocupa un puesto destacado en el TOP500 y que su uso en aplicaciones duales es aceptado (igual que en el caso de Estados Unidos). El 13 de octubre de 2022 el gobierno de Estados Unidos (U.S. Department of Commerce,

76 https://commdocs.house.gov/committees/security/has317000.000/has317000_1.HTM

Bureau of Industry and Security, BIS) publicó en el Registro Federal una **Norma Final Provisional, 87 Fed. Reg. 62186**, por la que se modifican los *Reglamentos de Administración de Exportaciones (EAR) (15 CFR partes 730-774)* para imponer nuevos controles a la exportación de circuitos integrados (CI) de computación avanzada (CI) chinos, productos informáticos que contengan dichos CI y ciertos artículos de fabricación de semiconductores. En la justificación de la regulación en relación con la República P0pular de China (RPC) se puede leer (Patel aet al., 2023)

"Estos sistemas están siendo utilizados por la RPC para sus esfuerzos de modernización militar para mejorar la velocidad y precisión de su toma de decisiones militares, planificación y logística, así como de sus sistemas militares autónomos, como los utilizados para la guerra electrónica cognitiva, el radar, la inteligencia de señales y la interferencia. Además, estos elementos informáticos avanzados y "supercomputadoras" están siendo utilizados por la República Popular China para mejorar los cálculos en el diseño y las pruebas de armas, incluidas las armas de destrucción masiva, como las armas nucleares, los hipersónicos y otros sistemas de misiles avanzados, y para analizar los efectos en el campo de batalla. Además, la República Popular China está utilizando herramientas avanzadas de vigilancia de IA, habilitadas por el procesamiento eficiente de grandes cantidades de datos, sin tener en cuenta los derechos humanos básicos para monitorear, rastrear y vigilar a los ciudadanos, entre otros fines. … Estados Unidos debe limitar la capacidad de la RPC para obtener chips informáticos avanzados o desarrollar aún más las capacidades de IA y "supercomputadoras" para usos contrarios a la seguridad nacional y los intereses de política exterior de Estados Unidos".

Específicamente, se aborda el control de exportaciones a China para el caso de los **supercomputadores que superen los 100 Petaflops a 64 bits en un determinado espacio físico** (centro de cálculo centralizado). En consecuencia, **no se puede exportar, reexportar o transferir (dentro del país) estos artículos sin una licencia** cuando se tenga "conocimiento" en el momento de la exportación, reexportación o transferencia (en el país) de que está destinado a:

- *El "desarrollo", la "producción", el "uso", la operación, la instalación, el mantenimiento, la reparación, la revisión o el reacondicionamiento de una "supercomputadora" ubicada en China o destinada a China; o*
- *La incorporación, el "desarrollo" o la "producción" de cualquier "componente" o "equipo" que se utilizará en una "supercomputadora" ubicada en China o destinada a China.*

Estos controles también se aplican a los artículos fabricados en el extranjero para los que se requiere una licencia[77] para exportar, reexportar o transferir (en el país) a China o dentro de China artículos producidos en el extranjero que son el producto directo de cierto software o tecnología sujetos a la EAR, o un producto de una planta completa o componente principal de una planta que es a su vez el producto directo de cierta "tecnología" o "software" de origen estadounidense si tiene conocimiento de que el artículo de producción extranjera se utilizará en:

- *El "desarrollo", la "producción", el "uso", la operación, la instalación, el mantenimiento, la reparación, la revisión o el reacondicionamiento de una "supercomputadora" ubicada en China o destinada a China; o*
- *La incorporación, el "desarrollo" o la "producción" de cualquier "componente" o "equipo" que se utilizará en una "supercomputadora" ubicada en China o destinada a China.*

En definitiva, **Estados Unidos ha endurecido sus regulaciones de control de exportaciones en componentes para supercomputadores de más de 100 Petaflops,** no solo desde Estados Unidos sino **obligando a terceros países a obtener una licencia para exportación** cuando usen equipos o componentes de Estados Unidos.

La eficacia de estas restricciones sobre tecnología de supercomputadores es discutible (Patel et al., 2023), igual que las que se han aplicado en otros casos anteriormente como el del GPS (BeiDou, 2022) o 5G[78]. Más allá de la necesidad de disponer de sistemas de monitorización de su cumplimiento que no son sencillos de implementar cuando se utilizan terceros países para el flujo de componentes sometidos a control de exportación, también suele provocar un **incentivo para acelerar el desarrollo de tecnología propia** cuando se aplican a países con capacidad tecnológica demostrada.

Desde un punto de vista comercial estas **restricciones a la exportación también hacen daño a las empresas de Occidente** en su penetración y cuotas de mercado en el mercado chino. Si China adquiere capacidades comparables en supercomputación a las de Occidente, también influirá en el mercado de otros países en su órbita que serán más difíciles de acceder para fabricantes de Estados Unidos o de la UE.

77 En virtud de una nueva Regla FDP en EAR § 734.9 (i). En virtud de la Regla FDP de Supercomputadoras en EAR § 734.9(i) https://www.tradepractitioner.com/2022/11/bis-implements-new-chinese-supercomputer-and-semiconductor-manufacturing-export-controls/

78 Un ejemplo en este sentido es el desarrollo del sistema chino de navegación por satélite BeiDou puesto en marcha poco después de que Estados Unidos estableciera restricciones al uso de GPS. Otro ejemplo similar es el anuncio en agosto de 2023 por parte de Huawei de un teléfono móvil (Mate 60) con chip de 5G de 7nm desarrollado en China a pesar de las restricciones impuestas por Estados Unidos y otros países a la transferencia de esta tecnología.

La evolución de las capacidades de la supercomputación convencional para la ejecución de modelos de sistemas complejos se está viendo reforzada por su **uso en inteligencia artificial**. Los supercomputadores especializados en IA son procesadores de alto rendimiento diseñados para manejar grandes cantidades de datos y ejecutar algoritmos complejos de IA (HPC-AI). Por lo general, los requisitos de HPC provienen de métodos de IA computacionalmente costosos (por ejemplo, aprendizaje profundo) y/o conjuntos de datos a gran escala (por ejemplo, redes masivas). La explosión de la IA generativa ha generado una demanda enorme de supercomputadores para el entrenamiento de grandes modelos de lenguaje. El equipo más relevante es el denominado ***Condor Galaxy 1*** que con 54 millones de núcleos podrán alcanzar una capacidad de cálculo de 4 ExaFLOPS (véase figura 20). CG-1[79], está en funcionamiento desde julio de 2023 y se encuentra ubicado en Santa Clara, California. Se ha diseñado específicamente para grandes modelos lingüísticos e IA generativa[80] y previsiblemente aparecerá a final de año en el primer lugar del TOP500. Desde un punto de vista geopolítico es relevante indicar que la empresa que lo ha anunciado, **Cerebras**, lo ha realizado en partenariado con **G42** que es una empresa de los *Emiratos Árabes Unidos* lo que supone la entrada de un nuevo país en este campo.

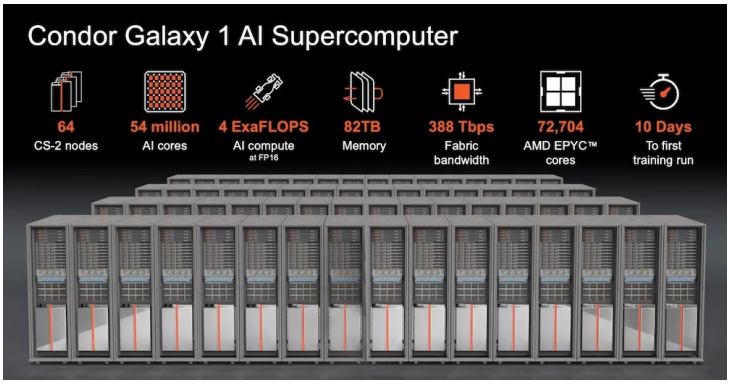


Figura 20. Condor Galaxy 1 AI Supercomputer. Fuente: https://www.chatgptguide.ai/2023/07/20/worlds-largest-supercomputer-for-ai-training-is-out/

Las previsiones de evolución suponen (véase figura 21) que las nuevas versiones llegarán a una potencia de cálculo de 36 ExaFLOPS en 2024 (combinando 9 supercomputadores) con una reducción significativa en el tamaño del código y complejidad.

79 https://www.cerebras.net/blog/introducing-condor-galaxy-1-a-4-exaflop-supercomputer-for-generative-ai/

80 Puede manejar hasta 600 mil millones de modelos de parámetros como estándar y puede ampliar sus configuraciones para admitir modelos con hasta 100 billones de parámetros. Además, está disponible como un servicio en la nube.

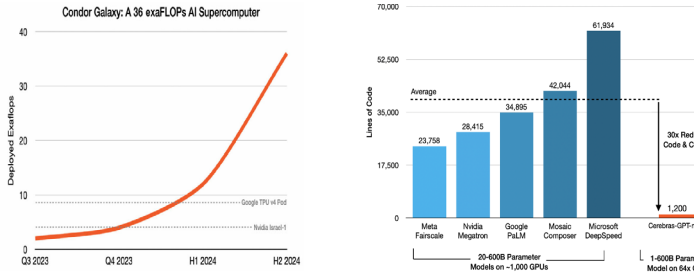


Figura 21. Evolución del Condor Galaxy y su impacto en el entrenamiento de modelos de IA generativa. Fuente: *https://www.cerebras.net/blog/introducing-condor-galaxy-1-a-4-exaflop-supercomputer-for-generative-ai/*

La UE que tiene una posición avanzada en supercomputación, a pesar de su dependencia en semiconductores, debe también posicionarse en su uso para IA generativa. Una de las actuaciones anunciadas[81] en septiembre de 2023 es la de permitir a las start-ups europeas acceder a estas grandes máquinas para el desarrollo de sus aplicaciones y herramientas de IA generativa y poder así "entrenar" sus modelos si lo hacen de forma "responsable" alineado con los principios de la próxima Ley de IA.

En el futuro, probablemente al final de la presente década, aparecerán de forma comercial los **supercomputadores cuánticos** que supondrán, de nuevo, una revolución en la computación y la muy probable emergencia de controles para evitar la transferencia indiscriminada de tecnología. No abordaré en este documento el caso de la computación cuántica.

2.3.6. Plataformas de servicios digitales

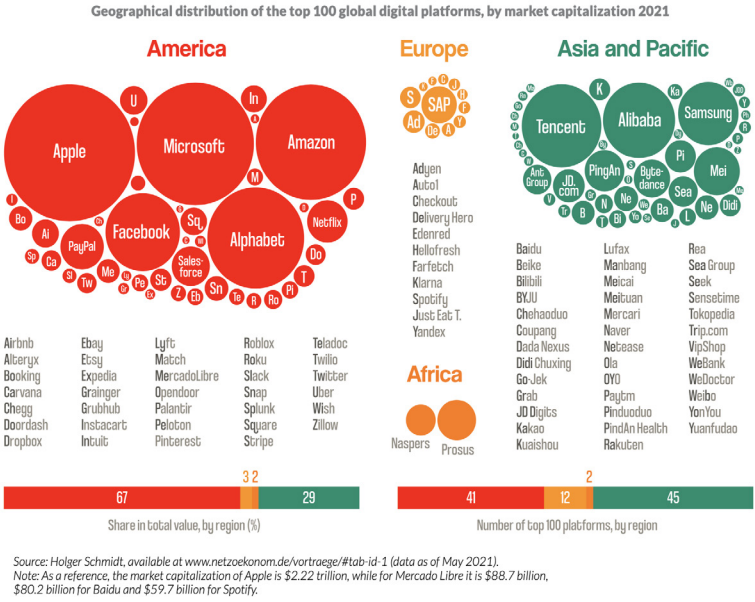
El proceso de digitalización masivo impulsado políticamente desde el comienzo del siglo XXI y acelerado en la última década ha implicado la **generalización del acceso a Internet** para la utilización de un conjunto muy elevado de servicios digitales para (todas las) empresas, administraciones y ciudadanos de muy variada índole. Las estrategias ligadas a las redes de comunicaciones móviles o a los cables submarinos presentadas brevemente en la sección anterior, cobran mayor relevancia al razonar en términos de su relevancia en el **acceso a servicios digitales**.

Es el **acceso universal** de estos servicios a costes reducidos, aprovechando el despliegue de las **infraestructuras de telecomunicaciones**, lo que ha permitido hacer realidad el **enorme cambio social** acaecido en los últimos veinte años. Entre los **servicios digitales** ampliamente difundidos hoy día se encuentran los ligados al comercio electrónico, los financieros, los servicios ofrecidos por las administraciones públicas en su relación con el ciudadano, los de seguridad y la defensa, la salud, la educación,

81 https://techcrunch.com/2023/09/13/eu-supercomputers-for-ai/

el transporte entre particulares, el entretenimiento, las comunicaciones interpersonales, el intercambio de datos, videos, etc. a través de correo electrónico y redes sociales, etc., así como los que permiten incrementar la ciberseguridad aplicados a todos los anteriores como son la firma electrónica o los certificados digitales biométricos.

Desde un punto de vista más técnico, la base para operar los servicios indicados anteriormente son las denominadas **plataformas de servicios digitales.** Son ellas las encargadas de la captura, almacenamiento, procesamiento e intercambio de datos personales o corporativos, así como de su comercialización posterior. Alrededor de ellas, se han creado y desarrollado grandes empresas cuyo valor bursátil en pocos años ha superado a la de las empresas de sectores tradicionales (Colback, 2023). No es extraño, por tanto, que los gobiernos hayan fijado gran parte de la **atención regulatoria y la disputa en términos geopolíticos** en el control de las plataformas digitales por el impacto e influencia que ejercen[82].



Source: Holger Schmidt, available at www.netzoekonom.de/vortraege/#tab-id-1 (data as of May 2021).
Note: As a reference, the market capitalization of Apple is $2.22 trillion, while for Mercado Libre it is $88.7 billion, $80.2 billion for Baidu and $59.7 billion for Spotify.

Figura 22. Plataformas digitales dominantes por continente de acuerdo con el valor bursátil en mayo de 2021. Fuente: https://systemicalternatives.org/2022/10/18/the-platform-economy/

La figura 22 indica en términos cualitativos el **valor bursátil de las plataformas digitales** más relevantes del mundo (a mayo de 2021) agru-

82 El mercado global de plataformas digitales supuso 96.900 millones de dólares en 2021 y 109.100 millones en 2022 a una tasa de crecimiento anual compuesta (CAGR) del 12.55%. Se estima que el mercado alcanzará los 175.800 millones de dólares en 2026 a una tasa compuesta anual del 12.67%. https://www.globenewswire.com/news-release/2022/09/14/2515724/0/en/Digital-Experience-Platform-Market-Global-Market-Report-2022.html#:~:text=The%20global%20digital%20experience%20platform,at%20a%20CAGR%20of%2012.67%25

padas por continentes. La situación comparada de la UE en relación con las plataformas digitales a nivel mundial que puede extraerse de la figura es claramente deficitaria. De la figura 22 se desprende que Europa era claramente dominada en 2021 no sólo por las **grandes empresas ofreciendo servicio de plataformas de Estados Unidos,** sino también por las **plataformas digitales con sede en Asia y Pacífico**[83]. Es muy difícil en estas condiciones asegurar una influencia en el devenir y gobernanza de estas plataformas digitales a nivel mundial y que los servicios que ofrecen se acomoden totalmente a los deseos de la UE teniendo en cuenta su rápido desarrollo previsto.

La importancia de las plataformas digitales no se circunscribe al valor bursátil que tienen o pueden alcanzar las empresas que las operan sino en el valor estratégico que alcanzan en la denominada **"economía basada en plataformas".** En la figura 23 puede verse la relación con las plataformas digitales. Es en ese contexto en el que debe analizarse la debilidad de la UE.

Figura 23. Evolución hacia una economía de plataformas. Fuente: Inspirada en Drewel et al., 2020

Son numerosas las discusiones sobre la **forma en la que las empresas que poseen estas grandes plataformas digitales están controladas o pueden controlarse por los gobiernos** y las consecuencias de ello. En el caso de *TikTok*[84], la discusión política en Estados Unidos ha girado desde 2020 en evaluar si *ByteDance*, la empresa china propietaria de la red

83 Únicamente la empresa europea SAP con base en Alemania tiene un peso bursátil destacable. Spotify, muy conocida en la UE como proveedora de servicios de música tiene poco peso en el resto del mundo.

84 Se trata de una plataforma de intercambio de videos cortos que no pertenece a ningún gran grupo empresarial chino (Tencent, Alibaba, Baidu) y que, con su decisión de crearse en las islas Cayman, tiene influencia creciente fuera de China. Sólo en Estados Unidos ya tenía 40 millones de usuarios en 2021 (Gray, 2021) y a finales de 2022 ascendía a 814,5 millones en todo el mundo (más de 113 millones en Estados Unidos). Francia y Alemania rondaban los 21 millones de usuarios cada uno en abril de 2023. https://es.statista.com/previsiones/1194946/usuarios-de-tiktok-en-el-mundo-por-pais . España no está lejos con 16,6 millones de usuarios.

social protege suficientemente los datos de los usuarios de su acceso por el gobierno chino (Gray, 2021) y si éste está utilizando la plataforma para "**influir en los usuarios de Estados Unidos**".

La regulación sobre plataformas digitales puede tener efectos **extraterritoriales** puesto que sus usuarios y datos procesados se encuentran en todo el mundo. Como ejemplo, la Ley sobre la tecnología y servicios en la ***"nube"*** de Estados Unidos ("*Cloud Act*: *Clarifying Lawful Overseas Use of Data"*) de 2018 no solo afecta a entidades de Estados Unidos, sino que también afecta a entidades que operan en Europa en caso de requerimiento judicial lo que supone una **extraterritorialidad de aplicación** a la que la UE intentó oponerse[85].

Estos problemas no son muy distintos a los que puede achacarse a otras plataformas digitales de Estados Unidos actuando en otros países, incluidos los de la UE, aunque con una relación gubernamental menor y sin las mismas consecuencias en el ámbito de la defensa. En todo caso, para un usuario europeo de las grandes plataformas digitales le afecta desconocer dónde están "sus" datos o los **criterios poco transparentes** empleados para la obtención de información, moderación de contenidos, o venta de información. Evidentemente, se trata de un problema mucho más relevante si se trata de datos pertenecientes a entidades públicas o bancarias que pueden contener contenidos sensibles.

Una iniciativa ideada en 2019 para mejorar la autonomía estratégica digital en relación con los **datos** para evitar que pudieran quedar a merced de empresas de otros países es la denominada **Gaia-X**[86]. El objetivo técnico era disponer de una **infraestructura de datos segura y federada** que representase los valores europeos, la soberanía digital de los propietarios de los datos, la interoperabilidad de diferentes plataformas, basada en el uso de código abierto y no propietario.

El objetivo político perseguido era **crear un ecosistema en el que los datos de entidades europeas estén disponibles y sean compartidos en un entorno confiable y gestionado "***de acuerdo con los principios europeos de descentralización, apertura, transparencia, soberanía e*

85 Esta situación obligó al Departamento de Justicia de Estados Unidos en 2019 a publicar un documento (Departamento de Justicia, 2019) justificando la Ley CLOUD: "La Ley está diseñada para permitir que nuestros socios extranjeros que tienen protecciones sólidas para la privacidad y las libertades civiles celebren acuerdos ejecutivos con los Estados Unidos para obtener acceso a esta evidencia electrónica, dondequiera que se encuentre, para combatir delitos graves y terrorismo... La Ley CLOUD autoriza acuerdos ejecutivos entre los Estados Unidos y socios extranjeros de confianza que harán que los ciudadanos de ambas naciones estén más seguros, al tiempo que garantizan un alto nivel de protección de los derechos de esos ciudadanos"

86 Iniciativa francoalemana del sector privado, pero con el apoyo de los gobiernos de ambos países. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

interoperabilidad"[87]**.** La estandarización e interoperabilidad deseada intenta evitar los efectos de una dependencia de un entorno de nube específico proporcionado por una empresa concreta e incrementar los servicios ofrecidos por estas empresas a través de una **red de pequeños proveedores europeos con servicios de datos interoperables** y, conjuntamente, convertirse en un actor relevante[88].

El concepto de **soberanía de datos** propugnado por Gaia-X se traduce en la autonomía y la autodeterminación que los usuarios necesitan para operar sus opciones tecnológicas. Gaia-X permite e impulsa la **creación de espacios de datos a través de plataformas confiables** que cumplen con reglas comunes, permitiendo a los usuarios y proveedores confiar entre sí sobre una base tecnológica objetiva, para compartir e intercambiar datos de forma segura y libre entre múltiples actores. A principios de 2022, la implementación inicial de Gaia-X comenzó con el lanzamiento de los primeros espacios de datos y servicios relacionados promovidos por diversos gobiernos europeos[89]. En España tomará forma en torno a los **espacios de datos sectoriales**[90] alineados con el marco regulador europeo, así como con la gobernanza y los instrumentos diseñados para garantizar la interoperabilidad, y sobre los que articular un mercado único de datos.

Si bien el libre flujo de datos y ausencia de restricciones regulatorias se consideraron un motor de innovación y el control rígido de los datos como un obstáculo, el caso de GAIA-X muestra que **mantener los datos y la infraestructura bajo control europeo** y dentro de sus fronteras se traduciría en un factor potencial para **incrementar la innovación y la fortaleza económica** de la UE, lo que refuerza la soberanía en el sentido político tradicional (Baur, 2023). Todavía el impacto de GAIA-X es reducido, tras un lanzamiento lento y no exento de discusiones entre los estados miembros como para atestiguar que este esfuerzo ha tenido éxito.

En definitiva, se está produciendo un "pulso" a nivel mundial entre grandes empresas de plataformas digitales (apoyadas directa o indirectamente por sus gobiernos), y los países o conjuntos de países como es el caso de la UE que pretenden **regular la forma en las que deben prestar estos servicios digitales a los usuarios nacionales**. De hecho, la aplica-

87 En España, a mediados de 2021, el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, impulsa la creación del "hub nacional de Gaia" integrándose en su estructura de gobernanza https://datos.gob.es/es/noticia/gaia-x-y-el-impulso-de-la-economia-del-dato

88 Desde el punto de vista comercial será difícil que Gaia-X, pueda desplazar a los servicios en la nube de grandes empresas digitales como Amazon Web Services, Microsoft Azure o Google Cloud.

89 El Ministerio Federal Alemán de Asuntos Económicos y Acción Climática lo hizo posible con una convocatoria sobre "Aplicaciones innovadoras y prácticas y espacios de datos en el ecosistema digital Gaia-X". Los once proyectos seleccionados tienen la tarea de mostrar cómo se puede implementar Gaia-X y desarrollar innovaciones con alto potencial de mercado. https://www.bmwk.de/Redaktion/EN/Dossier/gaia-x.html

90 Incluidos en el Plan de Recuperación, Transformación y Resiliencia (C12. I1 y C14. I2) https://datos.gob.es/en/noticia/qu%C3%A9-es-un-nodo-de-interoperabilidad-en-gaia-x

ción a estas plataformas digitales de las regulaciones europeas está generando **problemas políticos entre la UE y Estados Unidos.**

2.3.7. Ciberseguridad

Un elemento clave en el esfuerzo regulatorio de la UE que tiene un carácter transversal en todos los sistemas digitales ha estado dirigido a **incrementar el nivel de ciberseguridad de la UE**, muy fragmentada entre los diferentes estados miembros, con un **incremento muy elevado de ataques** con diversos fines (económicos, reputacionales, de influencia, políticos, etc.) que han ocasionado un daño económico elevado, afectando a particulares, empresas, infraestructuras críticas, hospitales y a los propios servicios de las administraciones públicas. En el sector privado un ataque que deje al descubierto datos de miles o millones de usuarios puede suponer la **pérdida de reputación y clientes a escalas muy elevadas**.

Repetidas encuestas muestran una preocupación creciente en los ciudadanos y entidades europeas ante el incremento continuo de los **ciberataques**[91] cuya formación básica para enfrentarse a ellos es reducida. No es extraño, por tanto, el interés manifestado por la UE y por sus estados miembros en **incrementar el nivel de "ciber resiliencia"**[92] de individuos e instituciones cuando, además, un porcentaje creciente proviene de **ciberataques deliberados llevados a cabo por entidades gubernamentales de otros países como parte de la "guerra híbrida" actual**, aunque sea difícil asegurar la atribución de un ataque a una agencia gubernamental de un país hostil**.** Como ejemplo, Ucrania ha sufrido 4.500 ataques de Rusia en 2022, tres veces más que en 2021[93].

Desde el punto de vista geopolítico[94], el riesgo de ciberseguridad en el contexto de los estados surge del objetivo de ciertos países de establecer un dominio sobre sus adversarios perturbando sus sistemas informáticos no solo en defensa sino también en sectores críticos (banca, energía, telecomunicaciones, etc.). Esto incluye el desarrollo de **capacidades ofensivas que permitan a un país atacar los activos y la infraestructura de un adversario**. Tales delitos generalmente provienen directamente del ámbito

91 Para valorar la situación en ciberseguridad desde un estado miembro de la UE como España, con datos obtenidos del informe de la Oficina de Ciencia y Tecnología del Congreso referido a 2021 (Oficina C, 2022), puede resumirse que en España se han recibido y gestionado centenares de miles de ciber-incidentes que han afectado alrededor del 28 % de la población. El Plan Nacional de Ciberseguridad (2022-2025) ha sido dotado con algo más de 1.000 millones de euros y el creciente mercado de la ciberseguridad se estima que alcance los 2.000 millones de euros en 2024 a nivel nacional.

92 Ciber resiliencia es la habilidad de prepararse, absorber, recuperarse y adaptarse a los efectos adversos de los ciberataques. Con ella se pretende la continuidad de la actividad económica y social de forma que, a pesar de un ciberataque, se mantenga el funcionamiento normal o parcial de los sistemas, servicios, industria, etc. (Oficina C, 2022).

93 https://www.eiu.com/n/cyber-risks-go-beyond-geopolitics/

94 Salvo el caso de grupos ciber-terroristas alentados en sus actuaciones por los gobiernos de ciertos países cuyo objetivo sea inhabilitar infraestructuras o hacerse con información sensible.

militar o relacionado con él, lo que implica que las capacidades son avanzadas y efectivas.

Aunque las fronteras entre objetivos puedan ser tenues, mi interés es focalizar el factor geopolítico con independencia de la delincuencia cibernética común que generalmente, busca acceder a sistemas y datos digitales con los que pueda pedir un rescate o vender la información a terceros, pero no tiene, en principio, consecuencias geopolíticas. El reto para las empresas que se conviertan en blanco de estos ataques es que, si bien la ofensiva está controlada por capacidades militares, la defensa debe provenir en gran medida de las medidas que adopte el sector privado.

La Comisión Europea ya empezó a preocuparse de la ciberseguridad en 2013 con una **Estrategia de ciberseguridad** y una primera directiva **NIS** (*Network and Information Security*) (European Union, 2016) presentada en julio de 2016 que entró en vigor en 2018 con un objetivo que su título dejaba claro: **alcanzar un nivel común de seguridad en toda la UE**. Este proceso se ha complementado con una Ley (EU) 2019/881: **Reglamento sobre ENISA** (*Agencia de la Unión Europea para la Ciberseguridad*) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación en abril de 2019.

El 16 de diciembre de 2020 la Comisión Europea presentó una nueva directiva denominada **NIS 2.0** sustituyendo a la directiva anterior de 2016 que se ha demostrado difícil de implementar en todos los estados miembros y no cubría todas las necesidades. Como resultado, la nueva directiva obligará a más entidades y sectores económicos a adoptar medidas de incremento de la ciberseguridad[95] (Negreiro, 2022)[96].

El informe anual de *ENISA Threat Landscape 2022 (ETL)* sobre el estado del **panorama de amenazas a la ciberseguridad** (julio de 2021 a julio de 2022) indica que, con más de 10 terabytes de datos robados mensualmente, el *ransomware* sigue siendo una de las principales amenazas, y el *phishing* se identifica como el vector inicial más común de tales ataques. Las otras amenazas que ocupan lugar destacado son los ataques contra la disponibilidad, también llamados ataques de *denegación de servicio distribuido* (DDoS)[97].

La evaluación de impacto de las amenazas realizado por ENISA revela

95 La Directiva se extiende a PYMEs y micro-PYMES, pero, a petición del Consejo, no se aplicaría a las entidades que llevan a cabo actividades en ámbitos como la defensa y la seguridad nacional, la seguridad pública, la aplicación de la ley y el poder judicial. Los parlamentos y los bancos centrales también están excluidos del ámbito de aplicación.

96 Complementariamente, se han desarrollado propuestas del Reglamento sobre la resiliencia operativa digital del sector financiero (DORA), de la Directiva relativa a la resiliencia de las entidades críticas (REC) y la del nuevo Reglamento sobre el Marco para una Identidad Digital Europea (eIDAS).

97 https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape

5 tipos de impacto; daños de naturaleza reputacional, digital, económica, física o social. Aunque en la mayoría de los incidentes el impacto sigue siendo realmente desconocido porque las víctimas no revelan la información o la información permanece incompleta.

Las principales amenazas se analizaron en términos de motivación. El estudio revela que el *ransomware* está motivado exclusivamente por ganancias financieras. Sin embargo, la motivación de los grupos patrocinados por el Estado puede extraerse de la geopolítica con amenazas como el espionaje y las interrupciones. La ideología también puede ser el motor detrás de las operaciones cibernéticas de los activistas. En la figura 24 puede verse la importancia relativa de los diferentes tipos de amenazas en 2022 clasificados en función de la motivación existente detrás de ellos.

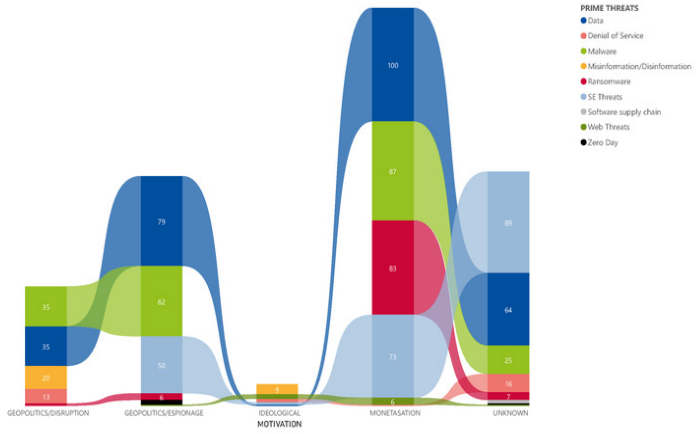


Figura 24. Amenazas relevantes de ciberseguridad. Fuente: https://www.enisa.europa.eu/news/volatile-geopolitics-shake-the-trends-of-the-2022-cybersecurity-threat-landscape

El despliegue de redes 5G se percibe como un potencial amplificador a la exposición al riesgo cibernético. Específicamente, con 5G no es posible diferenciar claramente el núcleo del borde de la red; como resultado, es más difícil aislar ciertos componentes de la red en comparación con 4G. En términos más técnicos *"los **sistemas dinámicos basados en software de 5G** tienen muchos más puntos de enrutamiento de tráfico. Para estar completamente seguros, todos estos puntos deben ser monitorizados. Dado que esto podría resultar difícil de realizar, cualquier área no segura podría comprometer otras partes de la red creando nuevas vulnerabilidades" (*Nocetti, 2022).

En este ámbito la evolución de las tecnologías emergentes como sucede con las **comunicaciones cuánticas** puede alterar significativamente el terreno de juego puesto que tiene también un factor de disrupción muy relevante. La denominada **criptografía cuántica** es un ámbito de trascendencia para asegurar la seguridad de las comunicaciones digitales que, con

ordenadores cuánticos los cifrados habituales se ven comprometidos puesto que en cortos periodos de tiempo pueden romperse todos los códigos de cifrado. Una red con seguridad cuántica es inmune ante cualquier ataque computacional, independientemente de la potencia computacional de un atacante (aunque tuviese un ordenador cuántico, no podría romper una transmisión de claves cuántica)[98].

Estamos lejos de la madurez de la tecnología que permita la expansión del despliegue de sistemas de comunicaciones cuánticas, menos aún de computadores cuánticos, pero las experiencias piloto que se están llevando a cabo[99], las crecientes inversiones, el interés industrial, y su uso dual, auguran durante la presente década otro foco de disputa geopolítica entre grandes países. Es por esta razón por la que **es necesario un posicionamiento temprano de la UE en las tecnologías cuánticas**, no solo desde la coordinación de las actividades de I+D como se está haciendo desde el programa marco de investigación e innovación con el lanzamiento de un gran proyecto ***Quantum Technologies Flagship***[100], sino también en el aspecto regulatorio e industrial.

Desde junio de 2019, los 27 Estados miembros de la UE han firmado la *"Declaración EuroQCI"*, acordando trabajar juntos para el desarrollo de una infraestructura de comunicación cuántica que cubra toda la UE (**EuroQCI**) junto a la Comisión Europea y con el apoyo de la Agencia Espacial Europea (ESA)[101]. A ello tiene que seguir una **consolidación de la industria europea de tecnologías cuánticas**, proceso que, personalmente, lo veo más complicado.

98 La criptografía cuántica es la distribución de claves criptográficas (QKD) basada en la mecánica cuántica. Dado que entre el emisor y el receptor solo se envían fotones, el medio es seguro, porque al intentar capturar la información enviada los fotones se alteran, el resultado en el receptor es distinto, y eso permite conocer el intento de acceder a ella.

99 Por ejemplo, en Madrid la creación de la red Madrid Quantum Communications Infrastructure (MadQCI) implica un anillo de 30 Km basado en conexiones de fibra óptica que unirá el área metropolitana de Madrid con la futura red de comunicaciones cuánticas europea (EuroQCI) mediante estaciones satélite distribuidas. https://www.computerworld.es/empresas/madrid-quantum-toma-forma-como-el-proyecto-mas-ambicioso-de-comunicaciones-cuanticas-en-la-region

100 Fue aprobado por la Comisión Europea en 2018 para un periodo de 10 años con un presupuesto de 1.000 millones de euros. Agrupa la actividad de unos 5.000 investigadores. https://qt.eu/

101 https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

3

NECESIDAD DE UNA ESTRATEGIA FACTIBLE PARA LA UE

3.1. CONDICIONES PARA UNA ESTRATEGIA EUROPEA

La discusión previa sobre la autonomía estratégica digital de la Unión Europea y los puntos de fricción geopolítica devuelve la discusión a un punto de partida: **encontrar el equilibrio más adecuado entre lo deseable y lo posible.** La UE no está sola en el mundo por lo que su planteamiento debe realizarse, en mi opinión, desde una **visión realista**, aunque flexible, ambiciosa y prolongada en el tiempo.

Si la UE pudiese imponer al resto del mundo su visión de la regulación digital necesaria de acuerdo con sus principios y valores, nada que objetar, pero debe tener en cuenta que las empresas europeas no ocupan una posición relevante de poder en el mercado mundial como se ha visto en el caso de las plataformas digitales o de las comunicaciones 5G, y se repite en el caso de la microelectrónica o el de la inteligencia artificial. Sin ellas, **será difícil que lo consiga basándose únicamente en su poder regulatorio**.

Más aún, la hipótesis de partida es que el principal soporte de esa visión europea es la del atractivo de su **"gran mercado" potencial de más de 450 millones de usuarios** de relativamente alto valor adquisitivo de productos y servicios digitales a la que ninguna empresa global podría renunciar. Por consiguiente, todas ellas aceptarían el marco regulatorio europeo impuesto..., aunque no les satisfaga. ¿Es cierta esta afirmación a largo plazo?

La relevancia del volumen del mercado potencial de la UE evoluciona en el tiempo y está sometido a dos factores relevantes: el primero, es la **evolución de la demografía**, y el segundo, su **composición por estratos de edad**. Ambos influyen en el peso que la UE va a tener en el mundo en las próximas décadas.

Según datos de Statista[103] el **peso de la población europea en relación con la población mundial** en septiembre de 2022 era del 9,37% (comparada con el 59,73% de Asia y el 17,92% de África). Se estima que esta cifra[104] alcance los 449 millones en torno al año 2025, antes de descender, de 2030 en adelante, hasta los 424 millones de personas en 2070. Con los crecimientos estimados en otras partes del mundo, el porcentaje de **la población europea solo significará un 6%** de la mundial a mediados del presente siglo.

Más relevante es la **composición por edades de la población europea** dado que la reducción en términos absolutos vendrá acompañada de un envejecimiento importante: se prevé que la proporción de personas mayores de 65 años ascienda del 20 % en 2019 al 30 % en 2070. Al mismo tiempo, se espera que la población de entre 20 y 64 años (es decir, en edad laboral) disminuya de forma constante.

La relevancia de este segundo factor es crucial a la hora de pensar en los patrones de **penetración de productos y servicios digitales muy avanzados**. De hecho, es la población joven y no la mayor de 65 años la que asumirá un papel de "*adoptadores tempranos*" (*early adopters*) de los nuevos servicios digitales como ya ocurre actualmente[105]. El riesgo es que la evolución de muchos servicios digitales (véase el fenómeno de las redes sociales) está promovido por estratos de población muy jóvenes.

Es cierto que, desde un punto de vista político y dejando al margen la evolución demográfica, gran parte de la narrativa de la UE hacia la necesidad de reforzar su soberanía digital y la autonomía estratégica se ha utilizado para **reforzar su reputación internacional de la UE como innovadora en políticas públicas en defensa del ciudadano**. Dicho de otro modo, la UE espera convencer a los demás actores que los principios y valores que informan esas políticas se adoptarán por otros países porque son los que permiten construir una sociedad democrática y cohesionada en el que **el "principio de precaución" se aplica de forma sistemática apoyada por una regulación inteligente al entorno digital.** En mi opinión, se trata de un **modelo "eurocéntrico"** anclado en la percepción de *que "todo el mundo mira a Europa por lo que hace y cómo lo hace".* Me parece que esa presunción tendrá, progresivamente, menos fundamento.

103 https://es.statista.com/estadisticas/634787/distribucion-de-la-poblacion-mundial-en--por-continente/

104 https://www.eeas.europa.eu/eeas/la-demograf%C3%ADa-y-europa-en-el-mundo_es?s=248

105 Es cierto que la población de mayor edad va a hacer un uso creciente de servicios digitales de salud, pero lo va a hacer con tecnologías maduras y en el contexto de una relativamente lenta digitalización de los sistemas de salud domiciliaria y otros servicios de cuidado y entretenimiento. Aunque las nuevas generaciones de nativos digitales nacidos a finales del siglo XX o en el siglo XXI lleguen a tener una edad elevada y estén acostumbrados al uso de servicios digitales, serán superados continuamente por el impulso exploratorio hacia nuevos productos y servicios propio de las nuevas generaciones que se encontrarán continuamente con nuevas tecnologías disruptivas.

El programa político del ***Decenio Digital*** de la UE para 2030 (*"Path to the Digital Decade")*[106] establece un ciclo anual de cooperación para alcanzar los objetivos y metas comunes. Este marco de gobernanza se basa en un **mecanismo de cooperación anual** en el que participan la Comisión Europea y los Estados miembros (European Commission, 2021a).

La figura 25 presenta los **objetivos digitales planteados por la UE para 2030**. Obsérvese la ambición de los objetivos en relación con la situación en 2021 en los que la brecha supera el 50%. En el caso de las infraestructuras de telecomunicaciones, esta situación implica un **déficit de financiación de 174.000 millones de euros** para cubrir el objetivo de 2030. Adicionalmente, será cada vez más necesario aumentar el volumen, la velocidad y la capacidad de las infraestructuras de telecomunicaciones para permitir el creciente flujo de contenidos en toda la Unión. El informe de seguimiento presentado en septiembre de 2023 (European Commission, 2023d) presenta avances en todos ellos y un conjunto extenso de recomendaciones para acelerar el proceso de digitalización de la UE.

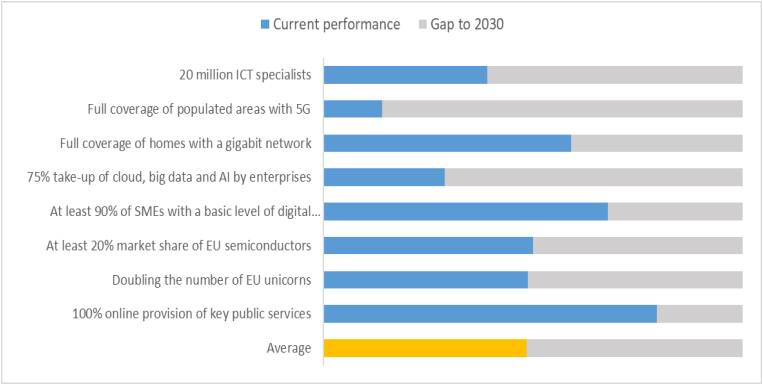


Figura 25. Objetivos del Decenio Digital Europeo. Fuente: European Commission, 2021

Para alcanzar los objetivos del ***Decenio Digital***, la Comisión Europea pretende facilitar la puesta en marcha de **proyectos multinacionales a gran escala** que ningún Estado miembro podría desarrollar por sí solo. Estos grandes proyectos podrían combinar inversiones del presupuesto de la UE, incluido el Mecanismo de Recuperación y Resiliencia, de los Estados miembros y del sector privado para cubrir los déficits identificados[107]. Cu-

106 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en#:~:text=various%20Member%20States.-,The%20Path%20to%20the%20Digital%20Decade,the%20Commission%20and%20Member%20States.

107 La Comisión ha identificado una lista inicial de proyectos multinacionales. Esta lista incluye áreas de inversión como infraestructura de datos, procesadores de baja potencia, comunicación 5G, computación de alto rendimiento, comunicación cuántica segura, administración pública, cadenas de bloques (blockchain), centros de innovación digital, y habilidades digitales. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

brir este gap implica **incrementar las inversiones en infraestructura** y mantener el ritmo de inversión durante toda la presente década para atender las necesidades de acceso a servicios proporcionados por plataformas digitales que, a comienzos de 2022, eran responsables del 70% del tráfico y con incrementos anuales cercanos al 50%.

Esta situación ha llevado a los máximos responsables de los operadores más relevantes de telecomunicaciones en la UE (*Telefónica, Deutsche Telekom, Vodaphone* y *Orange*) a solicitar mediante una carta conjunta[108] a las autoridades comunitarias en febrero de 2022 la necesidad de reflexionar sobre la **compartición de los costes del despliegue de infraestructuras con las grandes plataformas** digitales aludiendo a medidas similares tomadas en Corea del Sur. El riesgo para la UE es que no se cubran las necesidades de infraestructura al ritmo necesario.

Concretamente, la carta de los operadores decía: "*con las grandes plataformas de contenido digital presionando continuamente por una transmisión de mayor calidad, el cambio radical en el tráfico de datos que estamos experimentando aumentará constantemente sin límites. Si no solucionamos esta situación desequilibrada, Europa se quedará atrás de otras regiones del mundo, degradando en última instancia la calidad de la experiencia para todos los consumidores*".

La discusión sobre la propuesta de **"justa compartición de costes"** ("*fair share*") no ha alcanzado el consenso con agrios debates entre empresas, estados miembros y parlamentarios[109] y no parece fácil implementarlo[110]; la misma presión se ha producido también en Estados Unidos con un planteamiento similar por parte de Verizon y AT&T en 2022 (Condorelli et al., 2023). La Comisión Europea se ha mostrado comprensiva del problema en una *"Declaración sobre Derechos y Principios Digitales para la Década Digital"* en diciembre de 2022[111] en la que sugiere que toda la industria haga *"una **contribución justa y proporcionada** a los costos de los bienes, servicios e infraestructuras públicos".*

Las grandes empresas de contenidos dicen por su lado que el crecimiento del tráfico no se está saliendo de control y que ya están contribuyendo a la infraestructura. Obligarles a pagar una tarifa permitiría a los operadores

108 https://www.orange.com/en/newsroom/news/2022/acall-large-content-platforms-contribute-cost-european-digital-infrastructure

109 Grandes empresas de telecomunicaciones, Estados miembros del sur de Europa, algunos eurodiputados y miembros del mundo académico apoyan la idea, mientras que otras empresas de telecomunicaciones, grandes empresas tecnológicas propietarias de plataformas digitales, Estados miembros del norte de Europa y algunos eurodiputados se posicionaron en contra argumentando sobre los efectos perjudiciales que tal iniciativa podría conducir y favoreciendo un fondo especial, en caso de que se introduzca un mecanismo de compensación (Arnal y Ricard, 2023)

110 Una posible opción es forzar por el regulador una negociación obligatoria, respaldada por un arbitraje obligatorio cuando las partes no lleguen a un acuerdo sobre los términos.

111 https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7683

de telecomunicaciones cobrar tanto a los clientes como a los proveedores de contenido por el mismo servicio. (Pollet, 2023). Como resultado, la Comisión Europea lanzó una "*consulta pública*" para definir su postura[112].

La experiencia demuestra que implementar un modelo basado en el refuerzo de la autonomía estratégica digital de la UE no es solo resolver un problema de infraestructura de telecomunicaciones. Supone encontrar un **equilibrio entre el aumento de la independencia y la cooperación estratégica con otros países afines**. Este deseable equilibrio requiere una mayor coordinación de sus políticas digitales con sus relaciones globales con otros países, especialmente con los Estados Unidos. Aspecto que va más allá del ámbito digital.

Europa, para lograr un despegue efectivo de sus **políticas digitales, requiere incrementar el ritmo de inversión extranjera** procedente de grandes empresas y de fondos de inversión, tanto privados como soberanos, en los que compite por decisiones de inversión en otros países, entre ellos en Estados Unidos o en Asia. Si el marco legislativo, regulatorio, fiscal y de subvenciones europeo no es percibido como suficientemente atractivo, restrictivo o burocratizado en exceso, las inversiones se movilizarán hacia otros lugares.

El caso de la **atracción de potenciales inversiones** para la construcción en Europa de fábricas para la fabricación de semiconductores avanzados, o el despliegue de sistemas 5G nativo (SA), o para el desarrollo y lanzamiento de constelaciones de nanosatélites para el acceso a Internet son ejemplos muy claros de ello[113]. A ello, se suma la atracción de fondos de capital riesgo tecnológicos.

Desde mi punto de vista, instrumentalizar las políticas del mercado interior digital por razones geopolíticas es realmente muy difícil, en base a las estructuras jurídicas existentes en la UE[114]. Dada la **extraterritorialidad de muchas de las regulaciones adoptadas por los gobiernos sobre servicios digitales ofrecidos a usuarios en otros países**, este tema ha sido fuertemente controvertido por sus consecuencias sobre la soberanía de terceros países, sobre todo, en lo que concierne a la propiedad, acceso, y

112 https://digital-strategy.ec.europa.eu/en/consultations/future-electronic-communications-sector-and-its-infrastructure

113 Las grandes empresas capaces de fabricar circuitos integrados muy avanzados en el mundo son muy pocas (TSMC, Intel, Samsung) y muchos países están dispuestos a subvencionar la instalación de una de ellas en su país. En esta "batalla de subsidios industriales", tanto Estados Unidos como la UE (y muchos de sus estados miembros), y Japón han entrado en liza.

114 En este sentido, un tema que merece una reflexión es la dificultad creciente de que otros países avanzados se sumen al esfuerzo europeo en los programas marco de investigación e innovación (el actual denominado Horizonte Europa 2021-2027) debido, entre otros motivos, a la necesidad de asumir el marco jurídico impuesto por la UE en el programa marco, aunque deban financiarse su participación con sus propios recursos. El supuesto de que "correrían con los brazos abiertos a participar en el programa marco de cualquier manera", no es cierto. En mayo de 2023 muy pocos países avanzados han decidido participar.

explotación comercial de los datos que constituye el alimento fundamental para el sostenimiento de la economía digital.

En mi opinión, nos encontramos en un punto de inflexión en el que la futura gobernanza tecnológica, centrada en el control de las tecnologías emergentes, a la que me gustaría calificar de *"inteligente"* supone establecer **tres planos de discusión**, diferentes, pero entrelazados.

El primer plano es el que denomino **tecnológico** en el que se pretende establecer un **conjunto de reglas sobre una tecnología emergente** que delimite su marco de desarrollo, favorezca su correcto uso anticipándose a su completa madurez, asegure su interoperabilidad, reduzca los riesgos de seguridad inherentes a su desarrollo y uso, y permita su rápida adopción en la sociedad siguiendo unas pautas de evolución previsibles y limitando los efectos perjudiciales sobre el ciudadano y el medio ambiente que podrían derivarse de la aplicación de la tecnología. Es el plano de las **patentes** y los **estándares técnicos**.

El segundo plano, más difícil de implementar que el anterior, se focaliza en **establecer el marco de aplicación correcta de la tecnología en la sociedad.** En este plano se trata de establecer las reglas que permitan controlar cuándo y cómo debe utilizarse la tecnología por individuos e instituciones, buscando la máxima protección del individuo, tanto física como de su información personal, el establecimiento de responsabilidades derivadas del mal uso de la tecnología, y la satisfacción de un conjunto de principios y valores sociales y éticos asociados como pueden ser los medioambientales. Su implementación depende de la aplicación del denominado "**principio de precaución"** para evitar daños a personas o al medio ambiente.

Este es el nivel ligado al establecimiento de **legislaciones y regulaciones** con efectos jurídicos, generalmente, a nivel nacional o entre conjuntos de países como es el caso de la UE que no solo imponen reglas internas, sino que también afectan a proveedores externos. Rara vez este nivel alcanza una dimensión global mediante acuerdos internacionales más allá de declaraciones genéricas de principios[115].

Finalmente, el tercer plano de la gobernanza tecnológica, el **plano geopolítico**, nos adentra de manera directa en la batalla geopolítica ligada al control de la tecnología aludida repetidamente en las páginas anteriores. En este plano la tecnología emergente ya no es el objeto directo y único de

115 Su desarrollo está ligado a determinar el momento adecuado para hacerlo: si se hace prematuramente es posible que queda obsoleta por el propio desarrollo de la tecnología, si se hace de forma tardía para que la tecnología esté desarrollada puede que los efectos negativos por falta de una regulación apropiada ya se hayan producido y sean difíciles de eliminar. Esta situación se conoce como "dilema de Collingridge" (Collingridge, 1980).

discusión, sino que ésta se desplaza hacia la **forma en la que la tecnología es utilizada por países e instituciones multilaterales como un instrumento al servicio de una mejora relativa de su posicionamiento geopolítico.**

En el caso de **tecnologías emergentes con desarrollo multipolar** en el que intervengan varias potencias líderes, el establecimiento de una gobernanza tecnológica consensuada puede retrasarse buscando mejorar las posiciones relativas. Con, al menos, tres grandes actores constituidos en potencias tecnológicas, Estados Unidos, China, y la Unión Europea[116], junto a un conjunto de actores menores, pero relevantes en ciertas tecnologías como Japón, Taiwán, Corea del Sur, Singapur, Israel, Australia, India, Reino Unido, Canadá y Rusia, todos ellos con intereses propios, y coliderazgo en el desarrollo de algunas de ellas, **no es sencillo crear una gobernanza tecnológica estable e internacionalmente aceptada.**

En este contexto, una **política de sanciones prolongada en el tiempo** como la que Estados Unidos está imponiendo a China en el ámbito de los semiconductores tienen consecuencias sobre las empresas de Estados Unidos y sobre las de terceros países, como ocurre en el caso de la UE. No solo por el daño potencial a un mercado muy grande, sino también por las represalias sobre empresas de Estados Unidos[117], y la presión para acelerar la obtención de capacidades propias. Todo ello altera las estimaciones de fabricación de semiconductores y puede frenar inversiones[118].

Tal y como se ha planteado esta visión multinivel de la gobernanza, es aplicable a la gobernanza de todas las tecnologías. Interesa en este informe su potencial aplicación al caso de las **tecnologías digitales** que se aborda en la siguiente sección.

3.2. NIVELES DE AUTONOMÍA ESTRATÉGICA DIGITAL DE LA UE

3.2.1. Modelo conceptual

El desarrollo por un país concreto de un conjunto de actuaciones en los tres planos mencionados en la sección anterior para obtener un grado de autonomía estratégica digital suficiente presenta muchas perspectivas

116 En términos exclusivamente geopolíticos los actores tecnológicos mencionados se agrupan en grandes bloques. Uno de los bloques se ha configurado alrededor de Estados Unidos, y otro alrededor de China. He considerado en este informe a Rusia como "potencia menor" en lo que se refiere a tecnologías emergentes, a pesar de su relevancia militar, su peso en armamento nuclear y la buena posición relativa en algunas de ellas (p.ej. tecnología hipersónica o materiales).

117 Las autoridades chinas han anunciado en mayo de 2023 la prohibición de importación de chips de memoria Micron, empresa de Estados Unidos, en infraestructuras críticas, una medida considerada como la primera represalia significativa de China.

118 El consejero delegado de Nvidia, una de las grandes empresas de semiconductores ha advertido de que la industria tecnológica estadounidense corre el riesgo de sufrir "enormes daños" por la escalada de la batalla sobre los chips entre Washington y Pekín. Los controles a la exportación han hecho que sea incapaz de vender chips avanzados en uno de los mayores mercados de la compañía. Al mismo tiempo, las empresas chinas están empezando a fabricar sus propios chips para rivalizar con los procesadores para videojuegos, gráficos e inteligencia artificial de Nvidia, líderes del mercado (Murgia et al., 2023).

diferentes. Por este motivo es conveniente analizarlo mediante un **modelo conceptual multinivel** que permita abordar por separado la situación como se hace en los tres niveles presentados en la figura 26 (León, 2023a).

Figura 26. Modelo conceptual en niveles de autonomía estratégica. Fuente: León, 2023a

Para cada uno de los niveles el **grado de autosuficiencia tecnológica** obtenido por un país en un momento y para una tecnología determinada puede fluctuar entre el 0% (nula autonomía estratégica) y el 100% (autonomía estratégica total)[119]. Esta valoración cambia en el tiempo en función de las medidas adoptadas por el país en cuestión y también por las que adoptasen otros países con los que interacciona.

Como se ve en la figura 26 los niveles propuestos se han dividido en subniveles para abordar mejor el análisis. Debe tenerse en cuenta que los niveles no son totalmente disjuntos y pueden verse afectados, como ejemplo, por una determinada regulación que puede atraer o retraer inversiones extranjeras. Esas medidas tendrán como consecuencia que faciliten o impiden respectivamente la instalación de capacidades de fabricación de determinados productos.

El interés en esta sección es **aplicar el modelo genérico de la figura 26 al caso de la autonomía estratégica abierta digital de la UE**. Soy consciente de que el ámbito digital agrupa a un conjunto de tecnologías en los que la autonomía estratégica de la Unión puede ser diferente (p.ej. no es la misma situación la existente en el caso de semiconductores que en comunicaciones móviles o en inteligencia artificial); por este motivo, deberemos hacer un ejercicio de integración.

119 No trato de aplicar un análisis cuantitativo sino cualitativo. Una aproximación cuantitativa se ha hecho para el caso de 5G en da Ponte, León, y Álvarez (2022).

3.2.2. Nivel 1: Recursos naturales e infraestructuras de procesamiento y transporte

Sin disponer de las materias primas procesadas y de los componentes necesarios para disponer de productos digitales, o de las infraestructuras de comunicaciones para acceder a servicios digitales no es posible conseguir una autonomía estratégica real.

El subnivel de **acceso a recursos naturales** está condicionado en el ámbito digital a disponer de los materiales necesarios para el desarrollo de semiconductores empleados en todo tipo de productos electrónicos (tierras raras); también se pueden incluir los materiales necesarios para las baterías que emplean estos mismos productos (p.ej. litio)[120]. Concretamente, el acceso a las denominadas tierras raras se ha convertido en un elemento fundamental de la batalla geopolítica.

La UE tiene un nivel de dependencia elevado en el acceso a recursos naturales con una fuerte dependencia de China. Aunque pueden existir yacimientos en Europa los condicionantes medioambientales en la legislación y la opinión pública frenan su desarrollo (como sucede con la minería de litio en varios países). En el caso de componentes para la industria digital, la dependencia de la UE respeto a la fabricación de semiconductores es muy elevada. La mayor parte de ellos procede de fábricas *("foundries*") situadas en China, Taiwán, Corea del sur o Estados Unidos.

El subnivel de **infraestructuras de transporte** de materias primas componentes está muy condicionado por la estructura actual de las cadenas de valor y los lugares de origen de los productos, así como por la capacidad de procesamiento local en esos mismos países (al menos, para un primer nivel de tratamiento).

Las tensiones para la UE en **rutas de aprovisionamiento críticas** como las que proceden de Asia y la competencia con otras potencias en acceder a recursos naturales requeridos en terceros países (significativamente en el caso de África en el que la batalla geopolítica por los recursos naturales entre diversas potencias mundiales es muy visible) indican que la UE posee un nivel bajo de autonomía estratégica.

Por otro lado, a pesar de disponer de una **buena infraestructura de telecomunicaciones** intraeuropea como muestran los indicadores de DESI presentados anteriormente, Europa depende de la existencia de cables submarinos de comunicaciones digitales que son propiedad de diver-

120 El uso masivo de litio para baterías para el almacenamiento de electricidad a mayor escala (p.ej. baterías para el vehículo autónomo o procedente de energía solar fotovoltaica) deben considerarse parte de las tecnologías energéticas que pueden tener connotaciones de autonomía estratégica diferentes.

sas empresas privadas para el intercambio de datos y el acceso a servicios digitales cuyos servidores están situados fuera de la UE.

El problema para la UE es que su solución no depende en gran medida de ella sola, aunque **algunas acciones políticas en este nivel sí pueden aliviarlo**:

- Adaptar las regulaciones medioambientales específicas para la obtención de materias primas críticas para el desarrollo de productos digitales que aceleren y permitan su explotación en territorio europeo.
- Establecer acuerdos con terceros países para la explotación conjunta de yacimientos de materias primas, intentando mantener el control de la tecnología transferida, posiblemente dentro de una estrategia de poder blando más amplia.
- Facilitar mediante acuerdos públicos-privados la reestructuración de las cadenas de provisión de productos sensibles, cuando sea factible, a países amigos (*friend-shoring*) o cercanos (*near-shoring*) a la UE.

Parte de la solución a medio plazo puede venir de la **sustitución de algunos de los materiales críticos** por otros sintéticos o mucho más abundantes en la UE lo que nos conduce a la situación en el siguiente nivel.

Podría pensarse en que en el mundo digital estas consideraciones de materias primas y flujo de componentes y productos físicos no son relevantes cuando se trata de desarrollo de sistemas software que dan origen a la multitud de módulos software[121], aplicaciones y servicios que forman parte de la sociedad digitalizada. Hablamos de datos. Hay que tener en cuenta para este análisis que todo sistema software requiere para su ejecución de un sistema hardware basado en el cuso de semiconductores. Algunos de ellos son sistemas hardware ampliamente disponibles (ordenadores personales, teléfonos móviles inteligentes, etc.), pero otros poseen una alta sofisticación (por ejemplo, supercomputadores) que solo están al alcance de unas pocas empresas.

3.2.3. Nivel 2: Investigación, innovación, educación, y fabricación

No basta con disponer de materias primas o componentes si se desea mantener un nivel de autonomía estratégica. Se requiere también disponer de la **capacidad necesaria para el diseño y fabricación de sistemas digitales avanzados.**

En términos generales, la UE posee un nivel de autonomía estratégica en la investigación, incluyendo recursos humanos capacitados, alrededor

121 Muchos de ellos están disponibles en código abierto en repositorios públicos como GitHub que los desarrolladores de software pueden reutilizar para sus propios desarrollos.

de las tecnologías digitales que puede considerarse de bueno (en términos de recursos humanos formados, publicaciones o patentes), pero con recursos económicos insuficientes para mantener el ritmo competitivo exigido que hace difícil la retención en la UE de sus recursos humanos en algunas áreas como la IA en las que el déficit estimado sigue creciendo.

Adicionalmente, el problema de la UE estriba en seguir aportando recursos económicos suficientes para mantener este nivel en la I+D en un contexto internacional muy competitivo. El objetivo político acordado desde el año 2000 de que la UE alcance el 3% del PIB en I+D del que 2/3 proceda del sector privado, no se cumplió para 2010, tampoco para 2020, y veremos si en 2030 es posible (en 2022 fue del 2,22%).

El problema surge en el desarrollo de **tecnologías digitales disruptivas** como pueden ser la **tecnología cuántica**[122], las futuras **comunicaciones móviles celulares 6G**, los **sistemas autónomos**, la **computación neuromórfica**, o la **inteligencia artificial generativa** por citar las más relacionadas con las tecnologías digitales en la que los recursos que la UE está poniendo en juego son significativamente menores de los que se asignan a estas temáticas por otras grandes potencias tecnológicas. Todas estas tecnologías madurarán previsiblemente al final de la presente década (con la excepción de las tecnologías cuánticas que se retrasarán previsiblemente a la década de 2030) por lo que un retraso de tres o cuatro años para que la UE consiga una posición de liderazgo tecnológico, industrial y comercial puede situarla en una situación de **escasa autonomía estratégica difícil de revertir**.

Si nos fijamos en el **proceso de innovación** tampoco existe un condicionante que, *a priori*, haga que la UE no pueda obtener un nivel de innovación adecuado, pero se enfrenta a dos **problemas estructurales relevantes**:

- una dificultad en trasladar los resultados de su esfuerzo en I+D al mercado que haga que gran parte de su innovación dependa de productos y servicios digitales desarrollados en otros países, condicionado por el hecho de que la cooperación industria-academia-administraciones en ecosistemas digitales es aún débil.
- y una limitación en la financiación de capital riesgo para el crecimiento (escalado internacional) de sus start-ups digitales que, en muchos casos, acaban desarrollándose en Estados Unidos al encontrar mayores facilidades de financiación.

Europa tiene, por tanto, un reto colectivo para alinear su priorización política en el ámbito digital con los recursos disponibles para ello. Una

122 No es estrictamente hablando una tecnología digital, pero su desarrollo depende de la computación convencional y de la microelectrónica y se debe tener en cuenta de forma simultánea.

vez más la eficiencia de las medidas políticas está ligada a la existencia de presupuestos acordes con ella.

Para abordar ambos problemas la UE y la mayor parte de los estados miembros han puesto en marcha **múltiples programas y actuaciones** (p.ej. la creación del *European Innovation Council (EIC)*, creación del *Instituto Europeo de Innovación y Tecnología (EIT),* apoyo a los parques científicos y tecnológicos, fondos de capital riesgo apalancados públicamente, infraestructuras intraeuropeas, proyectos europeos de interés común) cuyos resultados son esperanzadores, pero insuficientes. En mi opinión, existe **demasiada fragmentación en pequeños programas y con dotaciones inferiores a la ambición de los objetivos planteados para que logren un efecto estructural real.**

El segundo subnivel, el de las **capacidades de fabricación de productos digitales**, se enfrenta a un problema estructural relevante dado que la UE dispone de capacidades limitadas y, en algún caso, como es el de los semiconductores avanzados (resoluciones inferiores a 10 nm) no posee capacidades de fabricación masiva lo que implica una dependencia elevada de otros países.

Las **decisiones tomadas años atrás por la industria europea de trasladar (descentralizar) gran parte de la producción de productos electrónicos a países como China**, e incluso la de desarrollo de sistemas software a otros países en búsqueda de costes salariales más bajos ha reducido la autonomía estratégica de la Unión. La recuperación de estas capacidades no es sencilla ni rápida, y, en todo caso, será muy costosa. En algunos sectores, como el de defensa poniendo en riesgo la seguridad colectiva.

En mi opinión, **es necesario actuar simultáneamente en los dos subniveles**. Pretender disponer de capacidades de fabricación orientando los recursos disponibles a ello (p.ej. primando la instalación en la UE de fábricas de empresas procedentes de otros países) sin la existencia de un ecosistema potente de investigación e innovación en las tecnologías asociadas, supone un riesgo enorme porque hace más sencilla su reubicación. Las capacidades de fabricación, como ha ocurrido otras veces[123], pueden reubicarse en otros países por múltiples razones sin dejar nada detrás de ello.

3.2.4. Nivel 3: Marco regulatorio, mercado y principios y valores compartidos

El tercer nivel considerado es el de establecer el **marco regulatorio y de principios y valores compartidos en el que se desarrolla el mercado**

123 España ha sufrido esta situación cuando disponía en los años ochenta de varias fábricas avanzadas de dispositivos semiconductores en Madrid (Tres Cantos), sin haber creado un ecosistema innovador potente, no quedó nada tras su cierre.

digital europeo, y sobre el que se configuran las relaciones internacionales de la UE con otros países. En este nivel la UE ha actuado desde hace años como **"potencia reguladora"** en base a la fortaleza de su mercado interior y del marco competencial para ello establecido en el Tratado de la Unión.

En el nivel 3 de la figura 26 se han establecido **tres subniveles** en los que la posición de la UE respecto a su autonomía estratégica digital puede ser diferente y que complementan los dos niveles anteriores:

- **Estructura del mercado**. Como ya se ha indicado previamente la UE tiene un principal problema derivado del tamaño de sus empresas digitales comparado con el de las grandes empresas de Estados Unidos o Asia. Al apoyo a las PYME se une la intervención, si fuera necesario, para evitar situaciones monopolísticas o de oligopolio, en fusiones y adquisiciones de empresas.
- **Marco regulatorio**. Establece condiciones que preservan la seguridad del ciudadano europeo, sus datos, y reglas de competencia. Concretamente, la protección de la privacidad en el acceso a servicios digitales se ha considerado un elemento clave para la implementación de una política proactiva de la Unión (véase anexo 2) asume una **visión proteccionista de los derechos de los ciudadanos europeos** forzando a los fabricantes y proveedores de servicios externos a aceptarlo para poder entrar en el mercado europeo.
- **Principios y valores compartidos.** La implementación de los dos subniveles anteriores y también el nivel regulatorio está condicionado por su relación con los principios éticos, la transparencia o el cumplimiento de los objetivos de desarrollo sostenible (ODS) que son considerados por la UE como elementos básicos de diferenciación en el concierto internacional. Será necesario evaluar el grado en el que pueden frenar el desarrollo de la UE en el ámbito digital o conseguir su aceptación por otros países.

Específicamente, en el **ámbito regulatorio** la UE ha sido muy activa poniendo en marcha un conjunto de regulaciones que afectan a diversos ámbitos. La tabla 4 resume seguidamente una visión general de la situación regulatoria digital que se detalla en el anexo. No se indican otras muchas regulaciones generales de la UE, no específicas del ámbito digital, que también afectan.

Instrumento legislativo	Fecha	Referencia
Reglamento General de Protección de Datos	2016	http://data.europa.eu/eli/reg/2016/679/oj
Directiva NIS	2016	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148
Directiva de protección de los consumidores	2019	https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-81968
Ley de ciberseguridad	2019	Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15
Directiva de Comercio electrónico	2020	https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295
Ley de servicios digitales	2022	https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81573
Ley de mercados digitales	2022	https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81470
Reglamento General de Seguridad de productos	2021	https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:346:FIN
Directiva de cargadores comunes	2022	https://data.consilium.europa.eu/doc/document/ST-10713-2022-INIT/x/pdf
Directiva NIS 2.0	2022	https://www.consilium.europa.eu/media/60338/st-10193-2022-init_x.pdf
Ley de gobernanza de datos	2022	http://data.europa.eu/eli/reg/2022/868/oj
Ley de chips	2023	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022AE1354&qid=1663948354673
Ley de Inteligencia artificial (EN TRAMITACIÓN acuerdo Político del Consejo en diciembre de 2023)	2021	https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206
Ley de Datos (EN TRAMITACIÓN adopción de la posición común del Consejo el 24 de marzo de 2023))	2022	https://data.consilium.europa.eu/doc/document/ST-6596-2022-INIT/es/pdf
Ley de materias primas críticas (EN TRAMITACIÓN Comunicación de la Comisión Europea en marzo de 2023)	2023	https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52023PC0160

Tabla 4. Resumen de la situación de la regulación digital en la UE, Fuente: elaboración propia

Muchas de estas regulaciones suponen un esfuerzo encomiable de la UE en adelantarse a otros países, aun a **riesgo de que se realicen sobre tecnologías en desarrollo cuyos impactos sociales no son bien conocidos**. Se ha optado por buscar un equilibrio para regular y forzar a otros países a adaptar sus productos y servicios al marco europeo si quieren comercializarlos en la UE dando (mucho) tiempo para su entrada en vigor[124].

Al mismo tiempo, la UE pretende buscar un mercado equilibrado entre grandes y pequeñas empresas distinguiendo entre grandes plataformas digitales que actúan como **puerta de entrada a servicios mayoritarios**

124 Como ejemplo, la Ley de Mercados Digitales afecta desde agosto de 2023 a las plataformas digitales cuyos usuarios en la UE supongan más del 10% de la población (45 millones de personas) y el resto tienen hasta 2024 para poder adaptarse.

(son las denominadas *"gatekeepers"*) y otras más pequeñas[125], asegurar un mejor control sobre contenidos ilícitos o nocivos[126], y dar facilidades para experimentar con los problemas de la regulación. La violación de las nuevas reglas antimonopolio del sector digital europeo puede suponer multas de hasta el 10% del volumen de negocio global de la compañía y de hasta un 20% en caso de reincidencia.

Las plataformas categorizadas como ***"guardianes de servicio"*** de acuerdo con la ley de mercados digitales son las que tienen una "repercusión significativa en el mercado interior", deben ser una "puerta de acceso importante" para que los profesionales lleguen a los usuarios finales y contar con una "posición afianzada y duradera" en el mercado[127]. En septiembre de 2023 la Comisión Europea ha declarado *Alphabet, Amazon, Apple, ByteDance, Meta* y *Microsoft* como empresas *"gatekeepers"* con servicios digitales que cumplen las condiciones establecidas en la Ley para que en un plazo de seis meses realicen las modificaciones necesarias; todas son de Estados Unidos menos *ByteDance* que es de China[128]. La figura 27 representa los servicios inicialmente afectados.

Por otro lado, en relación con la puesta en marcha de la **Ley de Servicios Digitales (DSA)** la Comision Europea ha identificado el 25 de abril de 2023 a 17 plataformas muy grandes (*Very Large Online Platforms, VLOP*) y dos motores de búsqueda[129] con más de 45 millones de usuarios mensuales activos como las primeras que tenían un plazo de cuatro meses para cumplir los requisitos establecidos por la DSA de control de contenidos,

125 La Ley de Mercados digitales (entró en vigor el 16 de noviembre de 2022) fuerza a que las plataformas digitales que controlan el acceso a servicios ya no podrán clasificar más favorablemente sus propios servicios y productos que otros similares ofrecidos por terceros en la misma página web. Tampoco podrán impedir que los usuarios desinstalen programas o aplicaciones preinstaladas si así lo desean. Además, los usuarios de pequeñas o grandes plataformas podrán intercambiar mensajes, enviar archivos o hacer videollamadas entre estas aplicaciones. En febrero de 2024 se aplicará ya a todas las plataformas https://www.europarl.europa.eu/news/es/headlines/society/20211209STO19124/la-ley-de-mercados-digitales-y-la-ley-de-servicios-digitales-explicadas

126 La Ley de Servicios Digitales (entró en vigor el 1 de noviembre de 2022) intenta abordar este problema bajo el lema de que "lo que es ilegal en el mundo real lo ha de ser también en el digital". Ello incluye la prohibición total de la publicidad dirigida a menores y de la publicidad específica según datos confidenciales (por ejemplo, basados en orientación sexual, religión, etnia). La adaptación a las nuevas normas deberá hacerse por parte de los proveedores de servicios (redes sociales o mercados electrónicos) antes de marzo de 2024. https://www.europarl.europa.eu/news/es/press-room/20220701IPR34364/dos-leyes-historicas-para-unos-servicios-digitales-mas-seguros-y-abiertos

127 En términos cualitativos deben ser empresas con una capitalización de al menos 75.000 millones de euros o que tengan un volumen de negocios en el espacio europeo igual o superior a 7.500 millones en los tres últimos años, y tengan al menos 45 millones de usuarios dentro de la UE con más de 10.000 usuarios profesionales activos al año en la UE o que cuenten con una capitalización bursátil de al menos 75.000 millones de euros o un volumen de negocio anual de 7,5 millones.

128 Otros como Gmail (de Alphabet) o Outlook (de Microsoft) no se han incluido. Hay reclamaciones por parte de algunas empresas afectadas sobre servicios concretos y el proceso continuará.

129 Las plataformas seleccionadas en base a los datos de usuarios comunicados en febrero de 2023 son: Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Googe Maps, Google Shopping, Instagram, Linkedin, Pinterest, Snapchat, Tik Tok, Twitter, Wikipedia, YouTube, y Zalando junto a dos motores de búsqueda muy grandes: Bing y Google Search. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413

sobre todo, para menores, mayor transparencia y asunción de responsabilidades, y mayor empoderamiento de usuarios para conocer mejor cómo actúa la plataforma (p.ej. sus algoritmos de recomendación).

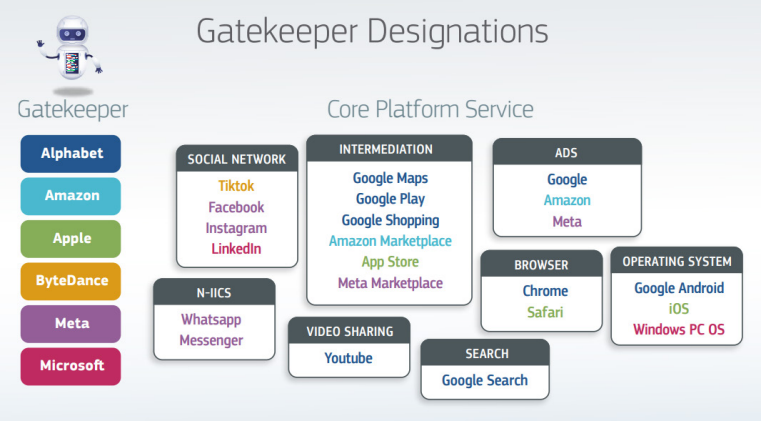


Figura 27. Servicios de plataforma digitales identificados afectados por la Ley DMA. Fuente: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

En este periodo las empresas propietarias de las plataformas conocidas han realizado el esfuerzo de modificar sus plataformas (como ejemplo, Meta indicó que tuvo a 1000 personas trabajando en ello)[130]. Tras el periodo de adaptación, el 25 de agosto de 2023 la DSA ha entrado totalmente en vigor.

Ahora, el reto para la comisión Europea es asegurar el cumplimiento de la Ley disponiendo de capacidades técnicas para ello. Para forzar el cumplimiento de las previsiones de la DSA la Comisión Europea ha puesto en marcha el *"European Centre for Algorithmic Transparency" (ECAT)*[131] que proporcionará apoyo técnico para conocer si los algoritmos empleados por las grandes plataformas cumplen con las condiciones establecidas en la Ley.

En este contexto, como opina Timmers (2022), **una cosa es legislar unilateralmente para todas las empresas que operan en la UE, y otra distinta es tratar de influir en las leyes y el comportamiento empresarial en todo el mundo**. Para Timmers, conseguirlo en función del tamaño de la economía de la UE a nivel mundial será poco eficaz. En mi opinión, tendrá que transcurrir un cierto tiempo para conocer si la legislación euro-

130 https://about.fb.com/news/2023/08/new-features-and-additional-transparency-measures-as-the-digital-services-act-comes-into-effect/

131 El ECAT se ha instalado en el IPTS en Sevilla del Centro Común de Investigación de la UE. Los investigadores de ECAT no solo se centrarán en identificar y abordar los riesgos sistémicos derivados de las plataformas en línea muy grandes y los motores de búsqueda en línea muy grandes, sino que también investigarán el impacto social a largo plazo de los algoritmos. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2186

pea, DSA y DMA, modifica el comportamiento de todos los actores a nivel mundial. En ello, influirá la evolución de la legislación en Estados Unidos y China como grandes actores.

El "efecto Bruselas", puede funcionar si la UE se anticipa a otros países como ocurrió con las normas de protección de datos, y hay pocas reglas internacionales con las que competir. Sin embargo, es menos probable que este enfoque funcione en temas como inteligencia artificial, en el que varios países han adoptado leyes diferentes a la (futura) ley de la UE, y, ésta no puede imponer su visión.

Conocer los efectos de una legislación digital muy novedosa no es sencillo cuando la evolución de la tecnología es muy rápida; el caso de la IA generativa es un ejemplo. Para paliar este problema es necesario **incrementar la capacidad de experimentación sobre los efectos regulatorios antes de extender su uso**. Uno de los instrumentos apropiados en este nivel para facilitar la experimentación es la creación de **entornos de prueba** *("sandboxes"*) **regulatorios en el ámbito digital** para acelerar el desarrollo de una regulación sobre una tecnología emergente que sea compatible con la protección al ciudadano e impulse el proceso innovador. Existen alrededor de cien iniciativas de *"sandboxes"* en todo el mundo hasta la fecha[132]

El objetivo con la puesta en marcha de "*sandboxes"* es **explorar el uso de una regulación en un ámbito tecnológico emergente mediante el desarrollo controlado de un conjunto de casos de uso**. Los *"sandboxes"* facilitan la creación de espacios donde los gobiernos involucran a las empresas para probar productos o servicios innovadores que permiten analizar la adecuación de los marcos legales existentes. Las empresas participantes obtienen una *"exención de aplicación de disposiciones legales específicas o de procesos de cumplimiento"* para permitirles innovar. Sus principales características (OCDE, 2023c) son: (1) tienen validez temporal; (2) utilizan un enfoque de prueba y error; y (3) involucran la colaboración y la iteración entre las partes interesadas.

También la UE ha impulsado el uso de esta herramienta en diversas tecnologías. Como ejemplo, la Comisión Europea ha lanzado en febrero de 2023 un entorno de pruebas reglamentario para casos de uso innovadores relacionados con **tecnologías de contabilidad distribuida** (*Distributed*

132 La Autoridad de Conducta Financiera del Reino Unido (FCA) fue pionera en el primer sandbox regulatorio fintech en 2015, y muchos países siguieron su ejemplo. El sandbox regulatorio FinTech de la Autoridad Monetaria de Singapur facilita la experimentación en vivo sobre productos y servicios de IA. La Oficina del Comisionado de Información del Reino Unido está probando el impacto de productos y servicios más amplios relacionados con la IA, particularmente en los marcos de privacidad (OCDE, 2023c).

Ledger Technologies, DLT)[133] en el que no existía una regulación ni el conocimiento preciso de cuál sería el enfoque más apropiado. También la OCDE ha propuesto su uso para Inteligencia Artificial (OCDE, 2023c).

La eficacia de la implementación de este nivel de actuación en relación con la autonomía estratégica digital está condicionada por la necesidad de disponer de **"aliados"** con los que la UE pueda poner en común visiones compartidas. Concretamente, el caso de Estados Unidos es especialmente relevante, pero lo es también alcanzarlo con otras potencias (digitales) avanzadas como Japón, Corea del Sur, Singapur, Australia, Canadá, Reino Unido, y otros.

El **debate entre la UE y los Estados Unidos** sobre el alineamiento en aspectos ligados a las tecnologías digitales (estándares, seguridad, sanciones a terceros y regulación) ha adquirido cierta virulencia. Primero con el Reglamento General de Protección de Datos, y más recientemente con las leyes de Mercados Digitales y de Servicios Digitales, ha sido interpretado en Estados Unidos como un **"ataque" de la UE a las grandes plataformas digitales de Estados Unidos** a lo que la UE ha respondido negando ese objetivo[134]**.**

Esta discusión de tipo político, técnico y regulatorio ha llevado a su inclusión en las discusiones en el **Comité conjunto** al más alto nivel creado en junio de 2021 ***TTC*** (*EU-US Trade and Technology Council*)[135]. Su objetivo es servir de foro para que los Estados Unidos y la UE coordinen enfoques sobre cuestiones comerciales y tecnológicas mundiales clave y para profundizar las relaciones comerciales y económicas transatlánticas basadas en estos valores compartidos[136]. Indirectamente, se persigue **evitar colisiones tecnológicas en un momento en el que las consecuencias geopolíticas son muy relevantes**.

133 https://digital-strategy.ec.europa.eu/en/news/launch-european-blockchain-regulatory-sandbox

134 El Comisario europeo Thierry Breton ha insistido en una reunión mantenida en junio de 2023 en el Silicon Valley ante presentantes de estas empresas que "el cumplimiento de las normas europeas no es un castigo", sino "una oportunidad para aprovechar el mercado único europeo", y ha afirmado que las empresas estadounidenses son "bienvenidas en Europa", siempre y cuando se acojan a sus "reglas" y sus "condiciones". https://elderecho.com/en-relacion-con-la-ley-de-servicios-digitales-o-ley-de-mercados-digitales-la-ue-rechaza-estar-en-contra-de-estados-unidos

135 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en

136 La Nota de Prensa publicada tras la tercera reunión mantenida el 5 de diciembre de 2022 muestra la relevancia de los temas (EU-US, 2022). La cuarta reunión se ha mantenido el 30-31 de mayo de 2023; uno de los puntos de la agenda fue el acercamiento de posturas ante la interpretación de la Ley de Servicios Digitales. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2922 ¡

3.3. RELEVANCIA DE LA TECNOLOGÍA DE SEMICONDUCTORES Y LA INTELIGENCIA ARTIFICIAL EN LA AUTONOMÍA ESTRATÉGICA EUROPEA

3.3.1. El papel de las tecnologías habilitadoras en la UE

Existen muchas áreas tecnológicas ligadas a la digitalización en las que se está produciendo un fenómeno de **confrontación geopolítica creciente** con impactos en los tres niveles presentados en la sección anterior. En algunos casos, se trata de **tecnologías habilitadoras** que se incorporan a múltiples productos y servicios comercializados, como es el caso de la **microelectrónica y semiconductores**, o la **inteligencia artificial (IA)** que, por este motivo, han suscitado mayor interés y provocado relevantes consecuencias geopolíticas.

En un contexto más académico el *concepto de tecnología habilitadora* puede incorporar también a otras tecnologías como la **nanotecnología** o la **biotecnología**. Para el presente informe circunscrito al ámbito digital no las voy a considerar, aunque la nanotecnología sí está presente implícitamente en los procesos de diseño y fabricación de dispositivos semiconductores (ahora a escalas nanométricas) y los aspectos geopolíticos asociados se tratarán en este contexto. También la IA emplea conceptos tomados de los seres vivos como es el de "red neuronal" y empiezan a aparecer los primeros experimentos en la convergencia nano-bio-electrónica que aún se encuentran en niveles de madurez muy bajos.

Asimismo, se han desarrollado **tecnologías específicas** integradas en tipos concretos de productos (sistemas) y servicios como pueden ser los *sistemas de navegación satelital* (p.ej. Galileo frente a GPS), las *comunicaciones móviles celulares* alrededor de 5G, las *constelaciones de nanosatélites*, o los *sistemas autónomos en robótica inteligente*.

Todas ellas emplean masivamente para su desarrollo la **tecnología de semiconductores** integrando en sus productos múltiples circuitos integrados, y, cada vez en mayor medida, hacen uso de **algoritmos de inteligencia artificial** para mejorar sus prestaciones haciendo uso de grandes conjuntos de datos. Las dos tecnologías habilitadoras mencionadas cumplen, por tanto, una función relevante.

No pretendo realizar en las siguientes secciones un análisis científico/técnico ni tampoco jurídico en relación con su uso, de las dos tecnologías habilitadoras indicadas, sino **exponer los problemas geopolíticos asociados y la forma en la que impacta a la UE y cómo los pretende abordar** en el contexto del objetivo político de mejora de su soberanía tecnológica y por ello, la de su autonomía estratégica digital.

Para ello, debe tenerse presente que **ambas tecnologías habilitado-**

ras tienen un carácter inherentemente dual con aplicaciones civiles y militares lo que incrementa aún más su valor estratégico y condiciona las decisiones políticas adoptadas en relación con el acceso a la información, propiedad intelectual, equipos de fabricación, algoritmos y dispositivos.

3.3.2. Factores geopolíticos de la tecnología de semiconductores en la UE

3.3.2.1. *Marco geopolítico del mercado y cadena de valor de los semiconductores*

La tecnología microelectrónica basada en el uso de dispositivos semiconductores se ha constituido en uno de los sectores clave de la sociedad actual. Para hacerse una idea de su relevancia, las ventas mundiales de semiconductores pasaron de 139.000 millones de dólares en 2001 a 574.000 millones de dólares en 2022, lo que supone una tasa de crecimiento anual compuesta de 6.67% anual.

El peso de la UE en el mercado mundial de semiconductores, sin embargo, es muy reducido. Está anclado en el 9-10% del total (SIA, 2023) a mucha distancia de Estados Unidos (48%) como indica la figura 28 tomada de la SIA (*Asociación de la industria de semiconductores de Estados Unidos*) de mayo de 2023.

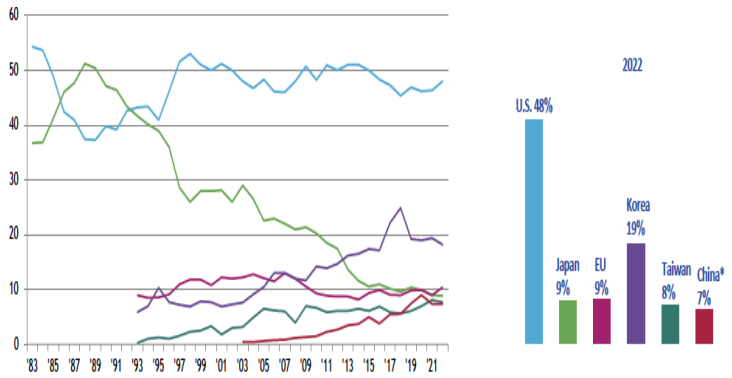


Figura 28. Evolución del mercado de semiconductores en el mundo. Fuente: SIA 2023

Esas ventas incluyen muchos tipos de dispositivos semiconductores adaptados a diferentes segmentos del mercado con características y procesos de diseño y fabricación diferentes. La figura 29, tomada del mismo informe de la SIA (2023) indica el **tipo de dispositivo semiconductor en el mercado** en relación con el volumen de ventas en 2022.

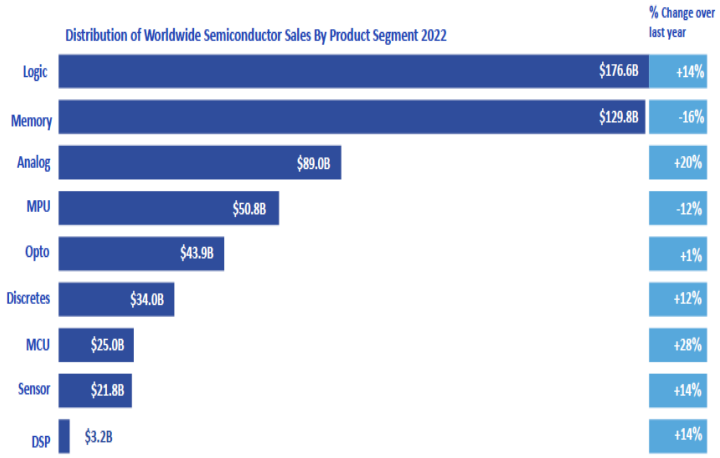


Figura 29. Distribución de las ventas de semiconductores por segmento del mercado. Fuente: SIA 2023

Obsérvese que los dispositivos **lógicos** (p.ej. microprocesadores) y los de **memoria** son los responsables de la mayor parte de las ventas puestos que se incorporan en un número enorme de productos, desde teléfonos móviles a juguetes, automóviles, lavadoras domésticas o misiles.

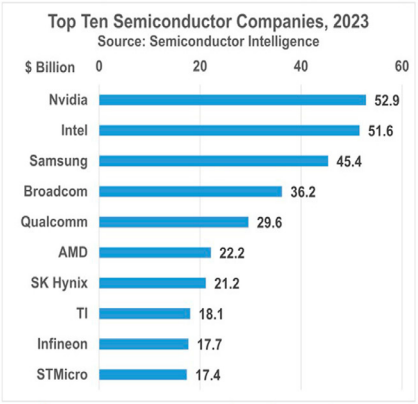
El posicionamiento de los países y sus fortalezas y debilidades varía fuertemente en función del eslabón de la cadena de valor de los semiconductores: desde la I+D, a la fabricación. En estos momentos, **ningún país del mundo domina todos los eslabones de la cadena para asegurar el acceso a los semiconductores en el volumen que requiere su sociedad**. Unos países no disponen de materias primas, otros no tienen capacidades de fabricación de semiconductores avanzados, y muchos otros, simplemente, asumen el papel de "compradores" o de usuarios finales de productos que los incorporan.

Hay pocas empresas capaces de cubrir todo el proceso, desde el diseño hasta la fabricación (una de ellas es Samsung), pero la mayor parte se especializa en una de las fases del proceso. Si atendemos a las **empresas más relevantes que fabrican semiconductores en términos de cuota de mercado** (véase la figura 30) ninguna de las principales es europea. Su evolución en los últimos años apenas ha variado.

Tras las cinco empresas indicadas en la figura 30 (TSMC, Samsung Foundry, GlobalFoundries, UMC, y SMIC) las cuotas de mercado de las siguientes cinco empresas importantes en la fabricación de semiconductores en 2022 son marginales, alrededor del 1%, y ninguna de ellas es europea.

Rank	Company	Country	Revenue (Q1 2023, USD)
1	TSMC	TW Taiwan	$16,735M
2	Samsung	KR South Korea	$3,446M
3	GlobalFoundries	US US	$1,841M
4	UMC	TW Taiwan	$1,784M
5	SMIC	CN China	$1,462M
6	HuaHong Group	CN China	$845M
7	Tower Semiconductor	IL Israel	$356M
8	PSMC	TW Taiwan	$332M
9	VIS	TW Taiwan	$269M
10	DB Hitek	KR South Korea	$234M
	Other		$556M
	Global Total		**$27,860M**

https://www.visualcapitalist.com/semiconductor-foundry-companies-ranked/



https://www.electronicsweekly.com/news/business/nvidia-to-be-no-1-rgis-yesr-says-si-2023-09/

Figura 30. Empresas más relevantes. Derecha: Empresas de semiconductores. Izquierda: empresas fabricantes de semiconductores

A este problema de "casi monopolio" (un oligopolio muy asimétrico) se suma la **concentración geográfica** dado que, con la excepción de Global Foundries en Estados Unidos y Tower Semiconductor (una de las marginales) en Israel, todas las demás se encuentran en una zona geográfica altamente conflictiva. Concretamente, la dependencia mundial de Taiwán y, especialmente, de TSMC es altísima.

Las máquinas necesarias para fabricar semiconductores avanzados también proceden de un puñado de empresas en todo el mundo. Algunas como ASML (en los Países Bajos) tiene casi el monopolio para los procesos de fotolitografía extrema (EUV) con la que se consiguen los semiconductores más avanzados de resoluciones inferiores a 2-3 nm. La figura 30 representa la última versión de uno de estos grandes equipos de ASML de tecnología EUV de gran apertura numérica[137] (obsérvese el tamaño del equipo en relación con las personas que aparecen) con un coste de centenares de millones de euros[138].

137 El objeto de menor tamaño posible que se puede imprimir con un determinado equipo de fotolitografía es proporcional a la longitud de onda de la luz dividida por la apertura numérica de la óptica. Por lo tanto, para lograr dimensiones más pequeñas deben emplearse longitudes de onda de luz más cortas o aperturas numéricas más grandes o una combinación de ambas. El valor de k1 se puede acercar a su límite inferior físico de 0.25 mejorando el control del proceso de fabricación. Esto es lo que ha conseguido ASML.

138 La inversión necesaria para la construcción de una fábrica avanzada de semiconductores puede oscilar entre 15.000 y 30.000 millones de euros en función de la tecnología y la capacidad de producción.

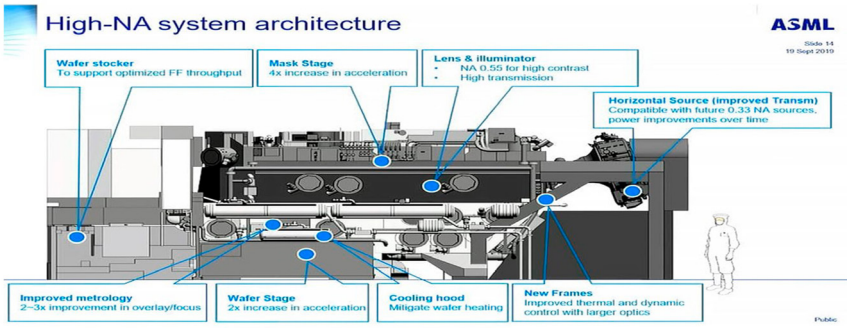


Figura 31. Esquema de un sistema de fotolitografía extrema EUV de gran apertura de ASML. Fuente: ASML 2019 https://elchapuzasinformatico.com/2023/12/intel-reserva-6-primeros-escaneres-euv-high-na-asml/

Otros países con capacidades relevantes en el desarrollo de equipos de fabricación de semiconductores son Estados Unidos y Japón. En Estados Unidos la empresa *Applied Materials* fabrica equipos que depositan finas películas de productos químicos sobre las obleas; *Lam Research* para el grabado de circuitos, y *KLA* para las herramientas que detectan errores nanométricos en obleas y máscaras litográficas. En Japón *Mitsubishi Gas Chemical* produce gases especiales para limpiar las obleas y fotorresistencias, y *Nikon* y *Tokyo Electron* equipos para fabricación (Ortega, 2023).

El tamaño del mercado mundial de equipos de fabricación de semiconductores se valoró en 2022 en 96,68 mil millones de dólares y se espera que crezca a una tasa de crecimiento anual compuesta (CAGR) del 7.7% de 2023 a 2030[139]. El crecimiento previsto de los equipos de fabricación de semiconductores se ve respaldado por las estimaciones de necesidades de evolución de la tecnología en la nube, el desarrollo de redes 5G y la creciente demanda de vehículos conectados.

Además, los ciudadanos de todos los países, salvo en crisis económicas severas, están dispuestos a gastar más en dispositivos avanzados como teléfonos móviles inteligentes o múltiples dispositivos ponibles (*wearables)* para mejorar sus niveles de vida.

3.3.2.2. Factores geopolíticos que condicionan la autonomía estratégica de la UE en la tecnología de semiconductores

El breve análisis del mercado global de los semiconductores efectuado en la sección anterior ha implicado la aparición o recrudecimiento de un **conjunto de puntos de fricción geopolítico** en torno a la microelectrónica y los semiconductores que agrupo seguidamente en **tres dimensiones**

139 https://www.grandviewresearch.com/industry-analysis/semiconductor-manufacturing-equipment-market-report#:~:text=The%20global%20semiconductor%20manufacturing%20equipment,7.7%25%20from%202023%20to%202030.

relevantes en las que se concentra la discusión geopolítica y las acciones emprendidas por muchos países: **tecnológica**, **defensa** y **comercial**.

La **dimensión tecnológica** está ligada a la confrontación entre países para dominar la evolución de las tecnologías avanzadas de semiconductores en los mercados mundiales en tres áreas principales:

- Empleo de **nuevos materiales** para el desarrollo de semiconductores de prestaciones elevadas. Concretamente, la exploración de materiales diferentes al silicio empleado actualmente en la mayor parte de los sistemas, y utilizar otros compuestos como el Nitruro de Galio (GaN), Nanotubos de carbono (CNT) o *cubic boron arsenide* (mejor conductor de calor y electricidad). Estos materiales permiten obtener dispositivos semiconductores más rápidos, aptos para altas frecuencias, o con características térmicas diferentes para un menor consumo, muy apropiados para aplicaciones espaciales o de defensa y, en el futuro, para todo tipo de sistemas[140].
  El empleo de estos materiales supone la necesidad de asegurar la provisión de las materias primas necesarias, disponibles en lugares concretos, y muy significativamente dominar los procesos de purificación y crecimiento en el desarrollo de dispositivos semiconductores, y, en el futuro, los componentes de sistemas cuánticos. Dominar los materiales semiconductores más allá del silicio empieza a ser un elemento de posicionamiento estratégico.
- Mejora de las **técnicas de fabricación con resoluciones de 2nm**. Conseguir estas resoluciones en chips de silicio implica el uso de maquinaria muy especializada únicamente al alcance de un grupo muy pequeño de empresas y capaces de usar tecnologías para arquitecturas de chip tridimensionales. Es obvio que el control del conocimiento necesario para fabricar o acceder al equipamiento necesario se ha convertido en un arma política muy relevante.
  En el contexto de la confrontación tecnológica entre grandes potencias se puede ver la relevancia de las medidas adoptadas para restringir la exportación aplicadas a estas empresas. Con ello, se impediría a otro país fabricar semiconductores avanzados de una resolución muy elevada a no ser que dispongan de capacidades de fabricación nacional de los mismos.
  El ejemplo más evidente es el derivado de las restricciones impuestas a China por Estados Unidos para obtener sistemas de fotolitografía extrema (EUV) que afectan a empresas no americanas, como ASML en los Países Bajos, a la que, junto a empresas de Japón, se les ha "forzado" a no vender sus equipos a China; en parte, por su

140 https://www.industryemea.com/news/64892-beyond-silicon-%E2%80%93-what-will-replace-the-wonder-material#:~:text=Gallium%20Nitride%20(GaN)%20chips%3A,ideal%20for%20high%20power%20applications.

posible utilidad militar y, en parte, para mantener el liderazgo tecnológico de Estados Unidos. Restricciones que se apoyan también, en que en el desarrollo de estos sistemas se utilizan componentes y propiedad intelectual procedente de Estados Unidos.

- Diseño basado **en hardware abierto** en el que los diseñadores puedan acceder a un *"conjunto reducido de instrucciones"* para diseñar sus propios circuitos integrados de procesamiento (como microprocesadores). Este es el caso de la iniciativa ***RISC V***[141] con un fuerte crecimiento desde su origen en 2015 cuyo objetivo es no depender de arquitecturas propietarias (como las de ARM, ahora mayoritarias) a la hora de diseñar un chip.
  Es interesante indicar que empresas chinas sometidas a sanciones de Estados Unidos como es el caso de Huawei han decidido apostar por *RISC V* para el diseño de sus circuitos integrados para evitar el uso de tecnología propietaria como es el caso de *ARM*[142] que es la más empleada en estos momentos.

La **dimensión de defensa** refleja el valor geopolítico adicional que adquiere la tecnología de semiconductores al tratarse de una **tecnología dual** cuyo uso quiere controlarse por parte de los países productores con el fin de evitar su uso militar por países potencialmente enemigos.

- Debe tenerse en cuenta que el uso de dispositivos semiconductores se encuentra en la base de todos los sistemas de armas actuales, desde los más simples (armamento ligero) a los más complejos (sistemas de misiles o vehículos autónomos) a los que se dota de capacidades de inteligencia en tiempo real al obtener información del entorno mediante múltiples sensores, y poder actuar en función del objetivo (p.ej. variando la trayectoria de un dron o misil).
- De hecho, el reconocimiento de esta situación ha conducido a regulaciones aprobadas por Estados Unidos, Australia, UE, Japón, etc. **limitando la exportación de dispositivos semiconductores o de los equipos que permitan fabricarlos** que puedan usarse en el desarrollo de sistemas de armas por parte de Rusia, China, Corea del Norte, Irán, etc., aunque esas restricciones supongan también una reducción del mercado potencial de las empresas de los países que

141 Actualmente RISC V International (https://riscv.org/) es una entidad sin ánimo de lucro que agrupa a 3.100 instituciones de 70 países que contribuyen y colaboran en el desarrollo de las especificaciones.

142 ARM es una empresa británica de semiconductores que diseña (no fabrica) chips utilizados en dispositivos móviles, como smartphones y tablets. La compañía fue adquirida en 2016 por el grupo japonés Softbank, que pagó 32.000 millones de dólares por ella. En septiembre de 2022, NVIDIA anunció que había llegado a un acuerdo para adquirir ARM por 40.000 millones de dólares. Sin embargo, la adquisición fue bloqueada por los reguladores de la competencia en varios países, incluyendo Estados Unidos, Reino Unido y China. Probablemente, cotizará en la bolsa de Nueva York. https://www.silicon.es/arm-comenzara-a-cotizar-en-la-bolsa-de-nueva-york-tras-frustrarse-su-compra-por-nvidia-2474285

las imponen, y de las dificultades objetivas en la monitorización del cumplimiento de las restricciones[143].

La **dimensión comercial** está asociada a obtener el máximo grado de **resiliencia de las cadenas de valor global** que impidan el estrangulamiento en la importación y exportación de semiconductores que frene el funcionamiento de sectores industriales como ha sucedido en los últimos años derivados de la COVID-19 y que todavía están presentes en sectores como el del automóvil.

- La consecuencia directa es la estrategia seguida por diversos países en establecer **incentivos** para disponer de capacidades de **fabricación de dispositivos semiconductores avanzados** en su propio territorio "invitando" a las empresas más relevantes con esas capacidades a instalar una fábrica ("foundry") subvencionando un porcentaje elevado de estos costes, y asegurar con ello el suministro a nivel nacional.
  La Ley de Estados Unidos de 2022 conocida como **CHIPS and Science Act** (*Creating Helpful Incentives to Produce Semiconductors and Science Act*) es un ejemplo en este sentido, "imitada" en sus incentivos económicos por decisiones similares de otros países y por la UE.

Para valorar la posición de la UE a nivel mundial teniendo en cuenta esos puntos de fricción geopolítica es necesario analizar el **peso que tiene la UE en cada uno de los eslabones** de la cadena de valor de los semiconductores[144].

- De manera cualitativa, si atendemos a las capacidades europeas, la UE ocupa una **posición relevante en la fase de investigación** en términos de publicaciones. Se nutre para ello de múltiples universidades y centros de investigación con capacidades de prototipado avanzado[145] bien situados a nivel mundial, aunque la investigación industrial no es tan potente.
  El mantenimiento de esta posición, en el futuro, seguirá dependiendo de la financiación pública, de la capacidad de retener el talento en la UE, y del fortalecimiento de un conjunto reducido de grandes empresas motoras con capacidad de investigación y dotadas de ecosistemas de investigación junto a start-ups, universidades y centros públicos.
- En la **fase de diseño**, aunque posee capacidades notables con em-

143 El hallazgo de circuitos integrados convencionales occidentales (como los empleados en electrodomésticos) en drones suicidas iraníes lanzados por Rusia en Ucrania indica la dificultad de establecer controles efectivos.

144 Wieringen (2022) ofrece un mapa de capacidades en Europa en el que las más relevantes se encuentran en Alemania, Países Bajos, Bélgica, Francia e Irlanda.

145 Uno de los más relevantes es IMEC situado en Bélgica. El gobierno español ha llegado a un acuerdo de intenciones para ubicar una segunda sede en España. https://www.imec-int.com/en

presas sólo de diseño (denominadas *fabless*), depende del uso de herramientas software y plataformas propietarias (p.ej. de ARM), así como el acceso a librerías de componentes de empresas no europeas. El movimiento del mercado hacia el diseño de chips basados en *hardware abierto* (p.ej. RISC V) mejorará su posicionamiento si su uso se extiende a nivel global y continúan mejorando sus prestaciones[146], a pesar de que también se incrementarán los competidores en otros países, incluyendo China.

- En la **fase de fabricación** la posición de la UE es débil, salvo en la provisión de equipos de **fotolitografía avanzada** empleados en la fabricación de semiconductores avanzados (sobre todo, a partir de la tecnología de la empresa ASML), aunque para ello requiere una larga y compleja red de proveedores[147].
  Especialmente, la UE no posee capacidades de fabricación de chips avanzados como los que se emplean en teléfonos móviles o para IA; sí de otros de menor complejidad, pero tampoco en volúmenes suficientes para otros sectores industriales en los que no se requieren resoluciones inferiores a 10nm (es el caso de la industria del automóvil, máquina herramienta, electrodomésticos, etc.), pero de los que depende un porcentaje significativo de la capacidad exportadora de la UE.
- Finalmente, tampoco tiene la Unión Europea una oposición destacada en el **ensamblado, prueba y empaquetado** que, fundamentalmente por razones de costes, proceden, sobre todo, de Asia. En relación con las cadenas logísticas, depende de suministros procedentes de zonas geográficas alejadas, fundamentalmente por rutas marítimas, aunque la distribución interna en la UE es razonable.

Como punto de partida, el problema geopolítico de la UE no estriba (sólo) en su escasa importancia relativa en el mercado mundial de los semiconductores con un peso inferior al 10%, como se ha indicado previamente[148], sino por lo que supone **depender de importaciones de dispositivos semiconductores de terceros países** dado que no es capaz de fabricar en Europa los chips que necesita para alimentar su propia estrategia de exportación de productos avanzados.

146 Debe tenerse en cuenta que, para un porcentaje muy elevado de dispositivos lógicos, las prestaciones logradas al emplear RISC V son suficientes.

147 Las máquinas de litografía más avanzadas (EUV) fabricadas por la empresa ASML, incorporan cientos de miles de componentes procedentes de casi 800 proveedores globales. Los módulos se construyen en 60 ubicaciones de ASML en todo el mundo y se envían a los Países Bajos para su ensamblaje. https://www.csis.org/analysis/opportunities-and-pitfalls-us-eu-collaboration-semiconductor-value-chain-resilience

148 Las cuotas de mercado europeas en la producción de chips para diferentes sectores son las siguientes: Automoción: 27%, Aeroespacial/Defensa/Seguridad: 22%, Industria: 20%, Salud y cuidado: 19%, Electrodomésticos: 17%, Audio y video: 11%, PC y procesamiento de datos: 5% y Telecomunicaciones: 4%. https://www.consilium.europa.eu/en/infographics/eu-chips-act/

Esta dependencia hace que, si no recibe chips, no puede fabricar automóviles y, por tanto, tampoco puede exportarlos que es un elemento clave de la balanza tecnológica europea. Esa misma dependencia aparece en otros sectores manufactureros como el de fabricación de robótica industrial, aeronáutica, espacio o defensa por citar algunos de los relevantes en la UE.

En el caso de la UE la necesidad de mejorar su posición en las fases de fabricación, ensamblado y prueba y empaquetado ha conducido a una estrategia que ha tomado forma en los dos últimos años con actuaciones e iniciativas presupuestarias tanto comunitarias como por parte de diversos estados miembros deseosos de **"convencer" a Intel, Samsung, TSMC, Global Foundries, etc. a instalar capacidades de fabricación avanzadas en un país europeo**. Esta estrategia tiene un límite derivado del volumen total del mercado nacional que justifique una inversión muy elevada y su amortización en plazos relativamente cortos (menores a cinco años) antes de que deba ser sustituida por otra tecnología de fabricación más avanzada.

En estos momentos, TSMC ha asegurado la decisión de instalar una fábrica de semiconductores avanzados en Alemania (Dresde) con una inversión de 10.000 millones de euros[149], e Intel otra también en Alemania (Magdeburgo) con una inversión de 17.000 millones de euros. En ambos casos con ayudas públicas de miles de millones de euros, y varios años por delante para hacer realidad estos proyectos. Disponer de capacidades de fabricación en la UE, aunque el coste final de los chips será más caro que los que procedan de China o Taiwán (extremo que ya ha valorado TSMC por los costes de mano de obra y energía, entre otros, en un 30% mayor) se compensa estratégicamente por una menor dependencia de suministros de semiconductores procedentes de Asia.

Es una estrategia similar a la seguida por **Estados Unidos**, impulsada por el mismo problema a pesar de disponer de plantas de Intel y Global Foundries, pero con inversiones muy superiores a las anunciadas en la UE. Como ejemplo, TSMC se ha comprometido a crear dos plantas de fabricación en Arizona por 40.000 millones de dólares (cuadruplicando la inversión prevista en Alemania), y la propia Intel ha comenzado la construcción de las nuevas foundries en Ohio con una inversión estimada de 20.000 millones de dólares[150].

India también ha entrado en la batalla global de los semiconductores acelerando la creación de un ecosistema nacional de semiconductores (Triphati, 2023). El gobierno de India lanzó en 2021 la denominada ***"India***

149 TSMC tendrá la propiedad del 70% de la planta y las empresas Infineon, NXP y Bosch tendrán una participación cada una del 10% sujeto a la aprobación de los reguladores.

150 https://www.intel.com/content/www/us/en/newsroom/news/intel-announces-next-us-site-landmark-investment-ohio.html

Semiconductor Mission" dotándola con 10.000 millones de dólares. En junio de 2023 los presidentes de Estados Unidos y de India firmaron un Memorando de Entendimiento (MoU) sobre la cadena de suministros de semiconductores y la coordinación de los programas de ambos países[151]. También India ha firmado otro acuerdo en 2023 con Japón. El interés estratégico es que India pueda convertirse a medio plazo en un proveedor alternativo a China en chips para aplicaciones no muy avanzadas.

El caso de **Rusia**, en el contexto de las sanciones impuestas sobre el acceso a semiconductores tras la invasión de Ucrania, merece una reflexión sobre la efectividad de las medidas. Las importaciones de semiconductores y circuitos integrados por Rusia de otros países ha crecido (datos de *Rusia Customs*) desde la invasión; sobre todo, los procedentes de China y Kong Kong.

Es evidente que **Rusia ha encontrado rutas alternativas**, principalmente a través de Turquía, Emiratos Árabes Unidos y China; pero también desde países de la UE como Chipre y Estonia (Intellinews, 2023). Encontrar una solución es una cuestión urgente, ya que cada vez hay más pruebas de cómo las fábricas rusas utilizan productos microelectrónicos comerciales occidentales en sus equipos de defensa (Yurchenko et al., 2023)[152].

3.3.2.3. Regulación de la tecnología de semiconductores en la UE

La relevancia de la tecnología de semiconductores y la necesidad de incrementar la autonomía estratégica está impulsando en varios países, como Estados Unidos, y también en la UE la aprobación de marcos legislativos específicos con un doble objetivo:

- Facilitar un marco regulatorio que incentive la I+D, formación y fabricación de semiconductores.

- Proporcionar cuantiosos recursos que atraigan inversiones privadas. De hecho, más importante que las reformas regulatorias que se establezcan en el mercado de semiconductores, incluyendo restricciones de exportación, se encuentra el volumen de recursos previstos y las condiciones de acceso al mismo.

El impacto de la Ley de semiconductores (*CHIPS and Science Act*) en

151 Tras la firma del acuerdo, el fabricante estadounidense de chips Micron Technology anunció que invertiría 825 millones de dólares para construir una instalación de ensamblaje y prueba de semiconductores en Gujarat aprovechando el apoyo económico concedido por el gobierno indio. También hay anuncios de AMD (400 millones de dólares) y de Applied Materials (400 millones de dólares). (Triphati, 2023).

152 En diciembre de 2022, RUSI (Reports, 2022) publicó un estudio que revela una red global de proveedores de electrónica a Rusia, indicando que 56 componentes únicos procedían de empresas europeas. En particular, el volumen más significativo de productos provino de NXP, con sede en los Países Bajos Semiconductors NV y STMicroelectronics, con sede en Suiza, la suiza u-blox, las alemanas EPCOS y Gumstix, y la francesa Thales Group.

Estados Unidos, aprobada en 2022, había generado un impulso del sector a finales de 2022 materializado en[153]:

- *Más de 50 nuevos proyectos de ecosistemas de semiconductores anunciados, incluida la construcción de nuevas instalaciones de fabricación de semiconductores (fabs), expansiones de sitios existentes e instalaciones que suministran los materiales y equipos utilizados en la fabricación de chips.*

- *Más de 210.000 millones de dólares en inversiones privadas anunciadas en 20 estados para aumentar la capacidad de fabricación nacional.*

- *44.000 nuevos empleos de alta calidad anunciados en el ecosistema de semiconductores como parte de los nuevos proyectos, que respaldarán cientos de miles de empleos adicionales en toda la economía de los Estados Unidos en general.*

La Ley europea equivalente "***Chips Act***" presentada por la Comisión Europea en febrero de 2022 (COM, 2022), tras un largo proceso negociador, ha sido finalmente adoptada por el Consejo Europeo el 25 de julio de 2023[154]. Para mejorar la posición de la UE la **Estrategia Europea de Chips** se articula en torno a cinco objetivos estratégicos:

- *Europa deberá reforzar su liderazgo en materia de investigación y tecnología;*

- *Europa deberá desarrollar y reforzar su capacidad propia para innovar en el diseño, la fabricación y el empaquetado de chips avanzados y convertirlos en productos comerciales;*

- *Europa deberá establecer un marco adecuado para aumentar sustancialmente su capacidad efectiva de producción de aquí a 2030;*

- *Europa deberá hacer frente a la grave escasez de capacidades, atraer nuevos talentos y apoyar la aparición de trabajadores cualificados;*

- *Europa deberá desarrollar una comprensión profunda de las cadenas mundiales de suministro de semiconductores.*

Con esos objetivos en mente la Ley de Chips europea tiene una estructura en tres pilares: 1) **pilar 1** para reforzar el desarrollo de capacidades tecnológicas a gran escala y la innovación en el ecosistema de chips de la

153 https://www.semiconductors.org/the-chips-act-has-already-sparked-200-billion-in-private-investments-for-u-s-semiconductor-production/

154 Tras ser firmada por el Presidente del Parlamento Europeo y el Presidente del Consejo, el Reglamento se publicará en el Diario Oficial de la Unión Europea y entrará en vigor el tercer día siguiente al de su publicación. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

UE; 2) **pilar 2** para mejorar la seguridad del suministro de la UE; 3) y el **pilar 3** para establecer un mecanismo de seguimiento y respuesta a las crisis.

Desde el punto de vista económico el programa tiene previsto movilizar **43.000 millones de euros en inversión pública y privada** (3.300 millones de euros del presupuesto de la UE), con el objetivo de duplicar la cuota de mercado mundial de semiconductores de la UE, del 10 % actual a, al menos, el 20 % para 2030. Será necesario esperar dos años para ver si los incentivos son suficientes para impulsar la inversión privada.

En paralelo, varios estados miembros de la UE han puesto en marcha programas nacionales con objetivos alineados a los europeos y aprovechando los recursos procedentes de los *Fondos de Recuperación y Resiliencia*. En el caso español, se ha concretado en un PERTE (*Proyectos Específicos para la Recuperación y Transformación Económica*) específico (*PERTE de Microelectrónica y Semiconductores*[155]) aprobado en mayo de 2022 con una asignación inicial de 12.600 millones de euros hasta 2026.

En todo caso, l**as economías de sectores tecnológicos de los países desarrollados están muy acopladas** y eso le sucede a la UE en la tecnología de semiconductores con respecto a Estados Unidos[156] o China[157]. Como indica la presidenta de la Comisión Europea debe pensarse más en un proceso de *reducción de riesgos* que de *desacoplamiento*. Téngase en cuenta que con la instalación en la UE de fábricas avanzadas de TSMC o de Intel como se ha indicado mejora la autonomía estratégica europea, al reducir la dependencia de importaciones de zonas tensionadas, **pero no necesariamente su soberanía tecnológica**. La tecnología de TSMC e Intel está protegida y será necesario comprobar hasta qué punto se puede crear un **ecosistema europeo alrededor de estas fábricas** que genere un salto cualitativo frente a la situación actual.

A pesar de los esfuerzos con la Ley de Chip europea, la **seguridad de suministros de semiconductores** para la UE en los próximos años puede evolucionar en escenarios diferentes de los deseados puesto que existen muchas variables que no están bajo el control de la UE. Wieringen (2022) propone **cuatro escenarios posibles** de mejor a peor posicionamiento de la UE (véase la figura 32). Los dos últimos escenarios (DECLINE y COLLAPSE) no son imposibles. El futuro no está escrito.

155 https://planderecuperacion.gob.es/como-acceder-a-los-fondos/pertes/perte-de-microelectronica-y-semiconductores

156 Las empresas europeas han participado en proyectos de investigación de fabricación de chips en Estados Unidos, las empresas estadounidenses participan en organizaciones de investigación europeas, como IMEC en Bélgica, Fraunhofer en Alemania y CNET-Leti en Francia. Las empresas europeas tienen instalaciones de producción de chips en los Estados Unidos (Infineon, X-Fab, BAE Systems) y las empresas estadounidenses fabrican chips en Europa (Intel, GlobalFoundries, ON Semiconductor, IXYS, Analog Devices) https://www.csis.org/analysis/opportunities-and-pitfalls-us-eu-collaboration-semiconductor-value-chain-resilience

157 China ha aumentado su cuota en chips menos avanzados (no ligados a restricciones de importación al no considerarse críticos) con costes muy bajos con los que la UE no puede competir.

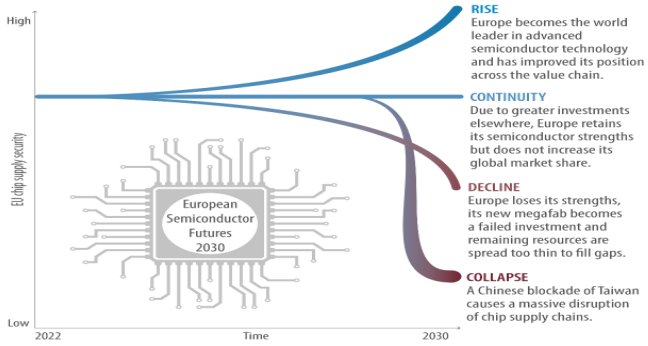


Figura 32. Escenarios 2030 de la UE en semiconductores. Fuente: Wieringen, 2022

La valoración personal del modelo multinivel presentado con anterioridad a la tecnología de semiconductores puede verse en la figura 33. La UE tendrá que actuar en todos los niveles. Desde un replanteamiento flexible de los requisitos medioambientales para poder explotar yacimientos de litio o tierras raras en el territorio de la UE, hasta crear ecosistemas potentes ligados a sectores estratégicos dependientes de chips con materiales distintos al silicio, el **aprovechamiento de las oportunidades de la UE** implicará una voluntad política sostenida, fuertemente alineada con la que pongan en marcha los estados miembros.

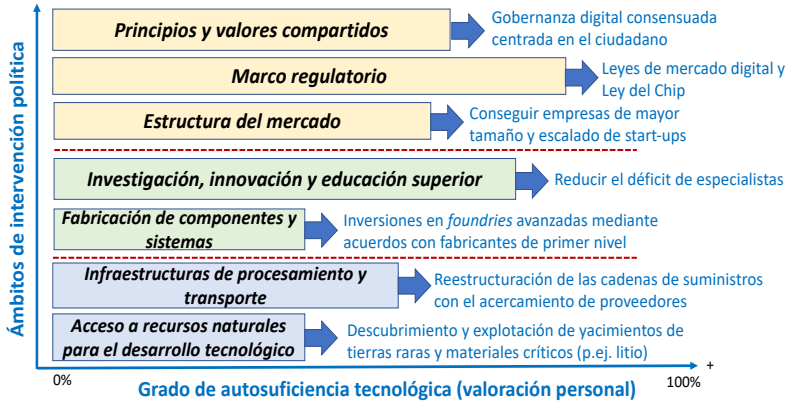


Figura 33. Valoración personal del grado de autosuficiencia tecnológica de la UE en la tecnología de semiconductores. Fuente: León, 2023.

Esta valoración puede verse perturbada por las subvenciones que pueden concederse a empresas a ambos lados del Atlántico. No puede perderse de vista que tanto la Ley Europea (EU CHIPS Act) como la de Esta-

dos Unidos (US CHIPS Act) son leyes básicamente económicas que afectan a las decisiones de las empresas y pueden conducir a una **"batalla por las subvenciones".** En la reunión de 30-31 de mayo de 2023 del órgano creado para la coordinación tecnológica y comercial entre la UE y Estados Unidos (Trade and Technology Council, TTC) se acordó en relación con este tema en la ***Declaración Conjunta***[158] (European Commission, 2023):

"La Unión Europea y los Estados Unidos se han comprometido a evitar una carrera en el apoyo público a los semiconductores. Por lo tanto, se ha establecido un mecanismo recíproco de consulta a nivel de los directores para facilitar la comunicación para evitar y prevenir las carreras de subsidios.... Compartimos el compromiso con la buena administración de los fondos públicos y, a través de nuestra cooperación, apuntamos a hacer que cada uno de nuestros respectivos programas de apoyo público sea más eficiente y efectivo".

Un factor esencial que está tomando una relevancia técnica y geopolítica decisiva es la **relación cada vez más estrecha de la tecnología de semiconductores con otra tecnología habilitadora de uso dual como es la "inteligencia artificial" (IA)** cuyo desarrollo en los últimos años y sus perspectivas de crecimiento en los próximos es muy elevada**.** Esta relación se analiza en la siguiente sección.

3.3.3.Factores geopolíticos de la inteligencia artificial en la UE

3.3.3.1. Un marco geopolítico condicionado por un proceso de innovación acelerado

Aunque se hable de inteligencia artificial como una tecnología, en realidad, debe considerarse como un conjunto relacionado de tecnologías con múltiples aplicaciones en un número creciente de sectores. De hecho, **muchas de las tecnologías enmarcadas en la IA se complementan con la tecnología de semiconductores** indicada anteriormente.

No es extraño en estas circunstancias que las aplicaciones de la IA en todos los sectores hayan también sufrido un crecimiento exponencial. El **mercado de la IA es gigantesco** con un tamaño estimado en 87.000 millones de dólares en 2021, y que crecerá previsiblemente hasta los 1.597.000 millones de dólares en 2030 con un CAGR del 38,1 % de 2022 a 2030[159].

158 https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2992

159 https://www.precedenceresearch.com/artificial-intelligence-market#:~:text=The%20global%20artificial%20intelligence%20(AI,38.1%25%20from%202022%20to%202030.&text=The%20advertising%20%26%20media%20segment%20accounted,the%20market%20share%20in%202021. También https://es.statista.com/estadisticas/1139768/inteligencia-artificial-valor-de-mercado/

El vertiginoso desarrollo de la(s) tecnología(s) relacionada(s) con la IA en estos últimos años, tras unas décadas de cierto estancamiento, y una aceleración en la última década (Gómez, 2023) se ha basado en la conjunción de factores tecnológicos, por un lado, y en haber encontrado amplios dominios de aplicación muy relevantes. De hecho, ha sido esta utilidad real en múltiples áreas la que le ha conferido su calificación como *"tecnología habilitadora"* y, por consiguiente, le ha dotado de una relevancia estratégica mayor.

También es cierto que ha crecido la preocupación por su potencial mal uso pidiendo una reacción rápida; en algunos casos en tonos alarmistas. Como ejemplo, los responsables de casi todos los principales laboratorios de investigación en IA advirtieron en una carta hecha pública en mayo de 2023 que *"mitigar el riesgo de extinción provocado por la IA debería ser una prioridad global, junto con otros riesgos a escala social, como pandemias y guerras nucleares".*

Como ejemplo de malos usos de la IA, a medida que los modelos grandes de lenguaje (*Large Language Model, LLM*) mejoren sus prestaciones en la producción de texto que parezca auténticamente humano, se volverán mejores tanto en la creación de contenido adaptado a las necesidades individuales de cada persona como en la **escritura de correos electrónicos de "phishing"[160] convincentes**. Será más difícil detectarlos.

Las mejoras se suceden sin pausa: el modelo de IA de Meta, ***"Cicerón",*** demostró un rendimiento similar al humano en *Diplomacy*, un juego que implica negociar con otras personas en un conflicto geopolítico simulado. Otro ejemplo procede de un experimento realizado en mayo de 2022. Un grupo de investigación en química desarrolló un sistema de IA para identificar 40.000 compuestos químicos tóxicos en seis horas, muchos de los cuales eran completamente nuevos. Predijo que **algunas de estas creaciones serían más tóxicas que cualquier arma química conocida**.

Un tercer ejemplo, ayuda a comprender el potencial impacto. Los avances obtenidos en los modelos de generación de código con IA podrían hacer posible producir *malware* con una experiencia de codificación mínima. En este momento, solo los profesionales capacitados pueden crear armas biológicas y químicas. Pero gracias a la IA, en lugar de requerir experiencia científica, **todo lo que un futuro terrorista podría necesitar para hacer un patógeno mortal es una conexión a Internet**.

Hacer frente a estos retos exigirá una gran **creatividad regulatoria**

160 Es uno de los ciberdelitos más conocidos basado en el robo de datos sensibles haciéndose pasar digitalmente por otra persona o entidad.

tanto de los responsables políticos como de los científicos. También requerirá que ambos grupos trabajen rápido y conjuntamente. Es solo cuestión de tiempo hasta que sistemas de IA muy potentes y potencialmente peligrosos como los mencionados comiencen a extenderse, cuando la sociedad aún no esté preparada (Anderljung y Scharre, 2023).

El interés de abordar la relevancia geopolítica de la IA en esta sección es porque, más allá de la capacidad de incremento de prestaciones en multitud de productos y servicios como corresponde a una tecnología habilitadora, ha entrado también en la **discusión geopolítica global desde tres dimensiones complementarias:**

La **dimensión tecnológica** en la que el desarrollo y penetración en la sociedad de la IA está ligado a otros dos ámbitos tecnológicos con interés geoestratégico que influyen y se ven influidos por la IA: la tecnología de microelectrónica y semiconductores, la captura y análisis de grandes volúmenes de datos. Son ellos los que permiten la existencia de sistemas autónomos.

En las dos tecnologías citadas, en cierta medida, independientes en su concepción de la IA, existe una clara sinergia en el desarrollo de productos y servicios que está ligado al condicionamiento procedente de tensiones geopolíticas. En el caso de la **tecnología de microelectrónica y semiconductores** esta relación se ve potenciada por la necesidad de ejecutar más rápidamente algoritmos de IA para aplicaciones en tiempo real como puede ser las necesarias para el vehículo autónomo. En estos casos, la mejor forma es emplear circuitos integrados específicos para ejecutar algoritmos de IA de forma paralela (p.ej. para análisis de imágenes) lo que hace a la IA dependiente de los semiconductores y ligado geopolíticamente a ellos.

Para el **manejo de grandes volúmenes de datos necesario para mejorar los algoritmos de aprendizaje** surgen dos necesidades técnicas: la necesidad de almacenar un número ingente de datos accedidos y comparados para la búsqueda de patrones, obligando a disponer de servidores con arquitecturas muy especializadas (de hecho, empleando también procesadores de IA), y a determinar cómo y en qué condiciones se pueden obtener estos datos de los usuarios. Es, sobre todo, este segundo aspecto el que implica atender a condicionantes geopolíticos y en los que se centra la regulación nacional.

Esta relevancia se ve en la evolución de algunas **empresas de diseño de circuitos integrados cuyo crecimiento está basado en el diseño de chips específicos para IA**. Es el caso de ***Nvidia*** cuyo valor en bolsa, debido al auge de la lA generativa y la necesidad de entrenar modelos de lenguaje muy grandes ya ha superado los 930.000 millones de dólares (23 de

mayo de 2023) y la coloca ya cerca de Amazon, Apple, Microsoft, y Alphabet que superan los 1.000 billones de dólares.

La **dimensión social** en el que, posiblemente, sea difícil encontrar un ámbito tecnológico en los últimos treinta años que supere el potencial de disrupción social de la IA en la vida de las personas en su ámbito personal (salud, entretenimiento), relaciones sociales (comunicación entre personas), o en la configuración de las relaciones laborales.

Si bien la microelectrónica desde los años setenta del siglo pasado, ha pasado de ser una tecnología "de nicho" para sistemas tecnológicos especializados a una tecnología de penetración masiva en la que todos los usuarios poseen en su entorno multitud de dispositivos que utilizan circuitos integrados (el principal producto de la microelectrónica), el grado de disrupción social es significativamente menor. Ahora le toca el turno a la IA, apoyada en la microelectrónica y la gestión de grandes volúmenes de datos, en adquirir una **dimensión social de carácter disruptivo** cuyo planteamiento estratégico por parte de las grandes potencias tecnológicas tendrá ganadores y vencedores durante el primer tercio de este siglo.

Estamos aún lejos de entender las consecuencias de la penetración de la IA en todas las capas de la sociedad a medio plazo, pero el incremento de la atención de los desarrolladores y la inversión en lo que se ha venido en denominar ***"inteligencia artificial generativa"***[161] es enorme y se ha producido en un tiempo muy corto[162].

Este tendencia se manifiesta en la forma en la que el fenómeno de ***ChatGPT***[163] de la empresa *Open AI* y otras similares han puesto de manifiesto en 2022 y que las grandes empresas han empezado a incorporar a sus herramientas más conocidas, como ha hecho Google en su buscador (y anuncia hacerlo sobre Gmail) al incorporar la herramienta ***Google Bard*** (todavía restringida al mercado de Estados Unidos) que permite acceder a

161 La IA generativa se refiere a la inteligencia artificial que puede generar contenido novedoso. Los modelos generativos de IA producen texto, imágenes o música: publicaciones de blog, código de programa, poesía y obras de arte. El software utiliza modelos complejos de aprendizaje automático para predecir la siguiente palabra basada en secuencias de palabras anteriores, o la siguiente imagen basada en palabras que describen imágenes anteriores. https://www.fastcompany.com/90826178/generative-ai

162 ChatGPT ha alcanzado los 100 millones de usuarios en solo dos meses. Ha supuesto el ritmo de crecimiento de una aplicación más rápido de la historia de la tecnología. Como ejemplo, TikTok tardó nueve meses en alcanzar los 100 millones de usuarios, Instagram 26, Facebook 54 meses y Twiter 65. https://www.xataka.com/empresas-y-economia/instagram-tiktok-chatgpt-plataforma-que-rapido-ha-crecido-toda-historia-internet#:~:text=100%20millones%20en%20dos%20meses.&text=Ese%20estudio%20est%C3%A1%20basado%20en,hab%C3%ADa%20en%20diciembre%20de%202022.

163 Todavía con imperfecciones, ChatGPT https://openai.com/blog/chatgpt/ o Google Bard mejorarán y resolverán algunos problemas como conocer cuáles han sido las fuentes de su resultado y, sobre todo, abordar la calidad y confianza en sus fuentes; al fin y al cabo, se trata de información tomada de Internet. Entre otras razones, la regulación de la UE sobre IA va a exigir conocer las fuentes de la información que generen estas herramientas de IA generativa. Ello va a permitir comercializar estas herramientas como servicios "premium" o no.

Internet para mejorar sus respuestas,[164] seguido del anuncio de su propio modelo, Gemini, en diciembre de 2023 y, un poco antes, lo había hecho Microsoft al incorporar **ChatGPT** a la última versión de su buscador ***Bing***.

La **dimensión de defensa** ha adquirido gran relevancia dado que la inteligencia artificial es inherentemente una tecnología de uso dual, en la que el uso de la tecnología de IA está condicionando una carrera armamentística para conseguir la superioridad potencial en el campo de batalla[165]. De manera muy rápida se ha incorporado la IA, junto a sistemas microelectrónicos, sensores y actuadores, en múltiples sistemas de armas inteligentes en una carrera entre grandes potencias.

El desarrollo de los conflictos armados actuales concede a la tecnología de la IA un papel esencial, para múltiples **sistemas de armas de precisión inteligente** en las que se delega en ellos la toma de decisiones[166]. No es extraño, por tanto, que los gobiernos hayan incluido a los productos y servicios basados en el uso de la IA normativas restrictivas para su exportación e importación, a pesar de las dificultades existente para monitorizar su uso y hacer cumplir las restricciones.

En un tipo de uso diferente también ha alcanzado notoriedad la capacidad de **inducir comportamientos favorables a una determinada idea ya sea a nivel individual como colectivo**. El posible uso para ello de la difusión de **noticias falsas** (generadas junto a texto, voz, imágenes, etc., creadas artificialmente) genera un problema geopolítico de primer orden que está obligando a repensar el tipo de controles a realizar,

Asociada con esta dimensión se encuentra la **discusión ética** sobre lo que debe permitirse o no en estos sistemas que pueden implicar **decisiones que afecten a la vida humana**. Un tratamiento consensuado entre todos los países es muy necesario, aunque no se esté cerca de ello[167].

Para gestionar los peligros, algunos expertos han pedido una **pausa (moratoria) en el desarrollo de los sistemas de IA más avanzados**. Personalmente, dudo que se lleve a cabo puesto que estos modelos son simplemente demasiado valiosos para que las entidades que invierten miles de

164 https://bard.google.com/

165 Algunos autores (Lee, 2021) argumentan que la IA provocará una tercera revolución en la conducción de la guerra, después de la primera revolución impulsada por la pólvora y la segunda por el armamento nuclear.

166 La actual guerra en Ucrania ha visto cómo se ha roto la sutil barrera preexistente en el uso de drones autónomos armados que ahora, son empleados por ambos bandos con la máxima capacidad que permite la tecnología de la IA.

167 En abril de 2023, se consiguió que ChatGPT proporcionara instrucciones detalladas sobre cómo fabricar napalm, una tarea que normalmente rechazaría, pidiéndole que simulara a la abuela de la persona, que solía contar historias antes de dormir sobre cómo hacer napalm. (Anderljung y Scharre, 2023)

millones de dólares en ellos congelen el progreso. Además, las moratorias propuestas para que de tiempo a pensar sobre el uso de la IA (p.ej. la solicitada de seis meses apoyada por múltiples expertos en Estados Unidos) han causado preocupación porque puede ocurrir que no todos los competidores globales vayan a aplicarla, y supondría darles una ventaja decisiva[168].

Sin embargo, los **responsables de la formulación de políticas** pueden y deben ayudar a guiar el desarrollo del sector y preparar a los ciudadanos para sus efectos. Pueden comenzar controlando quién puede acceder a los chips avanzados que entrenan a los principales modelos de IA, asegurando que los actores indeseados no puedan desarrollar los sistemas de IA más poderosos. Los gobiernos también deben establecer regulaciones para garantizar que los sistemas de IA se desarrollen y utilicen de manera responsable. Si se hace bien, estas reglas no limitarían la innovación de la IA. Pero *"comprarían tiempo antes de que los sistemas de IA con mayores riesgos sean ampliamente accesibles"* (Anderljung y Scharre, 2023).

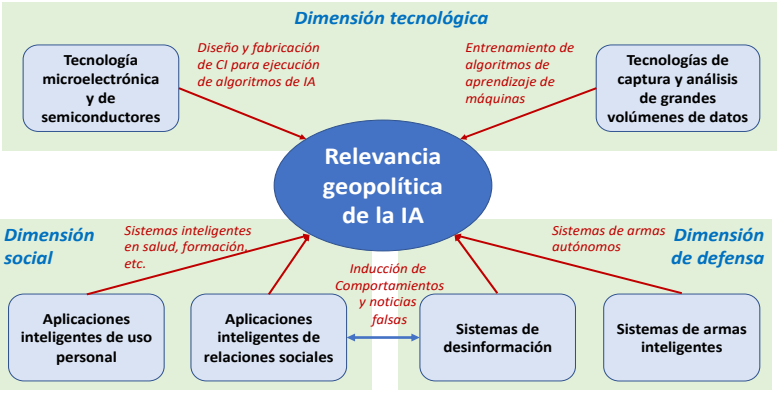


Figura 34. Relación entre las dimensiones coadyuvantes de la relevancia estratégica de la IA. Fuente: elaboración propia

La relevancia geopolítica que se concede a la IA no surge del análisis independiente de cada una de estas dimensiones, sino de su **estrecha relación que potencia su impacto y acelera su desarrollo.** He querido representarlo gráficamente en la figura 34.

3.3.3.2 Hacia un modelo de gobernanza de la IA

No es extraño, por tanto, que se desee **buscar un consenso entre todas las partes interesadas** para desarrollar un modelo de gobernanza de

168 No veo sencillo que se implemente en el ámbito de la defensa ninguna moratoria, sino, al contrario, seguirá en un proceso de aceleración si los conflictos militares continúan. Su verificación, al modo de lo establecido en los acuerdos de uso de armas nucleares o químicas, no es directamente aplicable.

la IA que sea, a la vez, efectivo y eficiente. *"Los creadores de la IA son ellos mismos actores geopolíticos, y su soberanía sobre la IA afianza aún más el orden "tecnopolar" emergente, uno en el que las empresas de tecnología ejercen el tipo de poder en sus dominios que alguna vez estuvieron reservados para los estados-nación"* (Bremmer y Soleyman, 2023).

El cambio de actitud a favor de una regulación de la IA empieza a calar. En 2023 se han realizado muchos esfuerzos diferentes para buscar una gobernanza global de la IA que permita establecer las reglas de uso más allá de lo que un país pueda acordar. Tres ejemplos muestran los intentos iniciados recientemente por **organizaciones multilaterales**:

- En mayo de 2023, el **G-7** lanzó el ***"Proceso de IA de Hiroshima"*** (G7, 2023) un foro dedicado a armonizar la gobernanza de la IA.
- En junio de 2023, la **OCDE** publica el informe sobre la IA en relación con la investigación (OCDE, 2023a) adoptando una **posición positiva al desarrollo abierto de la IA** y en julio de 2023, su informe sobre el impacto de la IA sobre el empleo (OECD, 2023b)**.**
- En julio de 2023, la **ONU**, a través del Secretario General, Antonio Guterres, pidió el establecimiento de un **organismo de control regulador global de la IA**.

En relación con el Proceso de IA de Hiroshima la visión de los siete países queda reflejada en el siguiente párrafo del comunicado final (G7, 2023) aludiendo a que **la gobernanza de la economía digital debe alinearse con los valores democráticos compartidos.**

"Reconocemos que, si bien el rápido cambio tecnológico ha fortalecido a las sociedades y las economías, la gobernanza internacional de las nuevas tecnologías digitales no necesariamente ha seguido el ritmo. A medida que se acelera el ritmo de la evolución tecnológica, afirmamos la importancia de abordar los desafíos comunes de gobernanza e identificar posibles brechas y fragmentación en la gobernanza tecnológica global. En áreas como la IA, las tecnologías inmersivas como los metaversos y la ciencia y la tecnología de la información cuántica y otras tecnologías emergentes, la gobernanza de la economía digital debe seguir actualizándose en línea con nuestros valores democráticos compartidos".

La primera recomendación del Consejo de la OCDE sobre IA data de mayo de 2019; desde entonces, ha mantenido un interés creciente[169]. En

169 La OCDE también actúa como secretariado para el GPAI (Global Partnership for AI). Concretamente, la OCDE facilitará las sinergias entre el trabajo científico y técnico de GPAI y el liderazgo internacional en políticas de IA proporcionado por la OCDE, fortaleciendo la base de evidencia para políticas dirigidas a una IA responsable. https://www.gpai.ai/about/

julio de 2023 ha analizado el impacto de la IA como parte del informe sobre la evolución del empleo (OCED, 2023b) **instando a los gobiernos a adoptar políticas que garanticen el uso confiable de la IA y la capacitación adecuada de los trabajadores durante la transición.** Todo ello, a pesar de que, según el informe, hasta ahora no hay datos concluyentes de que realmente la IA esté afectando al empleo.

"Si bien la adopción de la IA por parte de las empresas sigue siendo relativamente baja, el rápido progreso, incluso con la IA generativa (por ejemplo, ChatGPT), la caída de los costos y la creciente disponibilidad de trabajadores con habilidades de IA sugieren que los países de la OCDE pueden estar al borde de una revolución de la IA. Es vital recopilar datos nuevos y mejores sobre la adopción y el uso de la IA en el lugar de trabajo, incluidos los puestos de trabajo que cambiarán, se crearán o desaparecerán, y cómo están cambiando las necesidades de habilidades. Al considerar todas las tecnologías de automatización, incluida la IA, el 27% de los trabajos se encuentran en ocupaciones con alto riesgo de automatización. Los hallazgos iniciales de una nueva encuesta de la OCDE sobre el impacto de la IA en los sectores manufacturero y financiero de siete países destacan tanto las oportunidades como los riesgos que conlleva la IA".

Por parte de las Naciones Unidas se ha comenzado a analizar el papel que debe jugar, comenzando con trasladar el debate a las labores de la ONU. En palabras del Secretario General Antonio Guterres en julio de 2023 ante la Asamblea General (ONU, 2023) refuerzan la **necesidad de intervenir**:

"El debate de hoy es una oportunidad para considerar el impacto de la inteligencia artificial en la paz y la seguridad, donde ya está planteando preocupaciones políticas, legales, éticas y humanitarias. Insto al Consejo a que aborde esta tecnología con un sentido de urgencia, una lente global y una mentalidad de alumno. Porque lo que hemos visto es solo el comienzo. Nunca más la innovación tecnológica se moverá tan lentamente como lo está haciendo hoy… Y las cuestiones de gobernanza serán complejas por varias razones. En primer lugar, los potentes modelos de IA ya están ampliamente disponibles para el público en general. En segundo lugar, a diferencia del material nuclear y los agentes químicos y biológicos, las herramientas de IA se pueden mover por todo el mundo dejando muy poco rastro. Y tercero, el papel de liderazgo del sector privado en IA tiene pocos paralelos en otras tecnologías estratégicas".

A pesar de estos **esfuerzos multilaterales** que tienen la virtud de reconocer el problema y elevar el debate por encima de los intereses particulares de países o empresas, **la responsabilidad actual sobre la gober-**

nanza de la IA recae en los gobiernos de los países y en las empresas multinacionales que controlan su desarrollo.

En mi opinión, dudo que los **esfuerzos voluntaristas** del G7, de la OCDE o de la ONU por mencionar los tres organismos citados previamente sean capaces de poner en marcha una gobernanza efectiva de la IA a tiempo en un momento en el que el desarrollo de aplicaciones se ha acelerado en todos los dominios. Ninguno de ellos tiene capacidad operativa real.

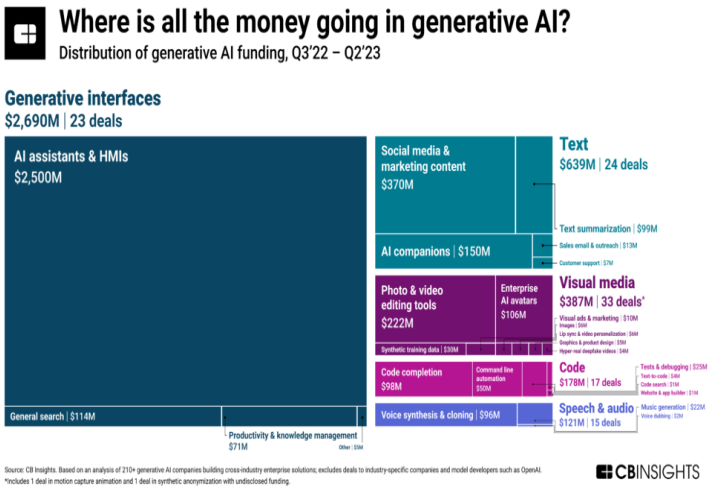


Figura 35. Inversiones en IA generativa. Fuente: CB Insights 2023

El ejemplo del desarrollo acelerado de la **IA generativa**, su incursión en múltiples **dominios duales**, las **enormes inversiones** que está concentrando, y los **nuevos actores** que intervienen demuestran la necesidad de una **gobernanza sincronizada con el desarrollo de la tecnología**. El riesgo es que estos esfuerzos de gobernanza global no lleguen a tiempo y la maldición del *"dilema de Collingridge"* se cebe en los esfuerzos de alcanzar una gobernanza efectiva antes de que la tecnología vuelva a mutar y los esfuerzos regulatorios iniciados sean vanos. No hay más que observar las **inversiones de capital riesgo alcanzadas por la IA generativa** que ascendieron a 2.690 millones de dólares en un año (véase la figura 35) y su distribución en la que los asistentes desarrollados con IA generativa supusieron 2.600 millones de dólares para darse cuenta de la relevancia que está alcanzando cuando los países aún discuten como regularla.

A pesar de que los Estados Unidos y la Unión Europea, con ocasión de la primera reunión del "*Trade and Technology Council (TTC)"* mantenida

en septiembre de 2021 acordaron en su declaración conjunta una postura firme frente a los "peligros" de la IA en manos de gobiernos autoritarios (Larsen, 2022) sus caminos han seguido rumbos diferentes.

3.3.3.3. Enfoque regulatorio de la IA por Estados Unidos y China

Estados Unidos comenzó el proceso regulatorio sobre la IA en 2018 con el establecimiento de **nuevos controles comerciales**. Las dos razones aducidas eran: 1) razón geopolítica motivada por el deseo de impedir que China y Rusia se aprovecharan de la tecnología de IA desarrollada en los Estados Unidos, y 2) asegurar que los controles comerciales establecidos promuevan y mantengan las ventajas comerciales a las empresas estadounidenses que desarrollan sistemas de IA.

Concretamente, las **tecnologías de IA que han sido sometidos a control comercial** son[170]:

- *Redes neuronales y aprendizaje profundo (p.ej., modelado del cerebro, predicción de series temporales, clasificación);*
- *Computación evolutiva y genética (p.ej., algoritmos genéticos, programación genética);*
- *Aprendizaje por reforzamiento;*
- *Visión por computador (p.ej., reconocimiento de objetos, comprensión de imágenes);*
- *Sistemas expertos (p.ej., sistemas de apoyo a la decisión, sistemas de enseñanza);*
- *Procesamiento de audio y voz (p.ej., reconocimiento y generación de voz);*
- *Procesamiento de lenguaje natural (p.ej., traducción automática);*
- *Planificación (p.ej., juegos, planes);*
- *Tecnologías de manipulación de audio y video (p.ej., clonado de voz, información falsa);*
- *Tecnologías de nube de AI;*
- *Chips de IA.*

El intento de controlar el desarrollo de la inteligencia artificial en China se hizo evidente cuando en agosto de 2022, el gobierno de Estados Unidos ha **prohibido la exportación de chips de IA a China**, específicamente los chips avanzados de *Nvidia Corp* y *Advanced Micro Devices Inc.* (AMD).

La industria de IA de China actualmente depende de *Nvidia* y *AMD* por

170 Obsérvese que la lista es más amplia de lo indicado en la figura sobre la taxonomía de la IA. Este control se hizo con la IA junto a otras 14 tecnologías y productos relacionadas con el desarrollo de armamento: navegación y posicionamiento; microprocesadores; tecnología de computación avanzada; analítica de datos; tecnología de computación y sensores cuánticos; interfaces cerebro-ordenador; y tecnologías de vigilancia avanzada.

lo que la industria de semiconductores de China, especialmente su industria de IA se ve indudablemente afectada[171]. De todas formas, **la aplicación de los controles a bienes intangibles como es el software es más difícil** y, en noviembre de 2021, únicamente se había añadido una aplicación software de IA al régimen de control de exportaciones.

En la actualidad, la regulación de la IA en los Estados Unidos todavía se encuentra en sus primeras etapas, y **no existe una legislación federal integral dedicada exclusivamente a la regulación de la IA.** Sin embargo, existen leyes y regulaciones que afectan a ciertos aspectos de la IA, como la privacidad, la seguridad y la lucha contra la discriminación. En relación con un esfuerzo legislativo específico, en 2023 han comenzado discusiones preliminares tanto por parte del gobierno de Estados Unidos como por parte del Senado.

La administración Biden (vicepresidenta Kamala Harris) se reunió en la Casa Blanca en mayo de 2023 con los directores ejecutivos de *Microsoft, Google, OpenAI y Anthropic* y presionó a la industria tecnológica para que tomara la seguridad más en serio. El esfuerzo continuó en julio de 2023, cuando representantes de siete compañías tecnológicas anunciaron en la Casa Blanca un conjunto de principios para hacer que sus tecnologías de IA sean más seguras, incluidos controles de seguridad de terceros y marcas de agua de contenido generado por IA para ayudar a detener la propagación de información errónea. No se trata de nuevas regulaciones.

Los legisladores también comenzaron a interesarse en mayo de 2023 con una audiencia con Sam Altman, el director ejecutivo de la empresa *OpenAI*. Los proyectos de ley están en sus primeras etapas y hasta el momento no cuentan con el apoyo necesario para avanzar. En junio de 2023, el líder demócrata del Senado, Chuck Schumer, anunció un proceso para la creación de una legislación de IA que incluía "sesiones educativas" para los legisladores en el otoño[172].

En el caso de los Estados Unidos la discusión sobre la eficiencia de estas medidas está sobre la mesa, y ya se levantan voces argumentando que un modelo de gobernanza de la IA mediante controles de exportación complementado con la autorregulación voluntaria de las empresas no será suficiente. Sobre todo, cuando la credibilidad de algunas de estas empresas está dañada. Como ejemplo[173]:

171 En un paso más Estados Unidos también está diseñando planes para extender la prohibición a los semiconductores utilizados en herramientas de IA y fabricación de chips con KLA, Lam Research y Applied Materials como las tres compañías objetivo. https://daxueconsulting.com/china-semiconductor-industry/ (accedido el 8 de enero de 2023).

172 https://www.nytimes.com/2023/07/21/technology/ai-united-states-regulation.html#:~:text=RT%2D2%20Robot-,In%20U.S.%2C%20Regulating%20A.I.,distant%2C%20lawmakers%20and%20experts%20said.

173 Sarah Myers West, directora del AI Now Institute, https://www.theguardian.com/technology/2023/jun/13/artificial-intelligence-us-regulation

"Las empresas que están liderando el rápido desarrollo de sistemas de IA son las mismas empresas tecnológicas que han sido llamadas ante el Congreso por violaciones antimonopolio, por violaciones de la ley existente o por daños relativos a la información en la última década. Básicamente, se les está dando una vía para experimentar con sistemas que ya sabemos que son capaces de causar un daño generalizado al público".

En varios foros de Estados Unidos se ha propuesto la creación de un **nuevo organismo regulador** focalizado en los modelos de IA más avanzados ("de frontera").

"Washington debería establecer un régimen de licencias para los modelos de IA de frontera, los que están cerca o más allá de las capacidades de los sistemas más avanzados de la actualidad, entrenados en supercomputadoras de IA a escala industrial. Para hacerlo, los formuladores de políticas podrían crear un ***nuevo organismo regulador*** *ubicado en el Departamento de Comercio o el Departamento de Energía. Este organismo debería exigir que antes de entrenar sus modelos, los desarrolladores de IA de frontera realicen evaluaciones de riesgos e informen sus hallazgos. Las evaluaciones proporcionarían una mejor visibilidad del desarrollo y brindarían a los reguladores la oportunidad de exigir que las empresas ajusten sus planes, como reforzar las medidas de ciberseguridad para evitar el robo de modelos".*

El paso más relevante tomado por el gobierno de Estados Unidos ha sido la "Orden Ejecutiva" de la Casa Blanca de octubre de 2023 sobre Inteligencia Artificial orientada a reducir los riesgos[174]. No es, por tanto, una legislación aprobada en las cámaras parlamentarias.

La Orden obliga a los fabricantes de sistemas de IA compartir con el gobierno de Estados Unidos la información de las pruebas efectuadas, así como desarrollar sistemas y herramientas para conseguir sistemas de IA seguros y confiables.

Adopta el objetivo de limitar riesgos para el ciudadano americano, y afirmar los valores de apoyo a la innovación con acciones que deben tomar todas las empresas en determinados plazos. Es pronto para conocer los efectos de un enfoque voluntarista[175] cuando otros grandes bloques como China y la UE adoptan una postura más asertiva basada en la regulación.

El caso de **China** es diferente (Sheehan, 2023) y no se puede decir que no haya adoptado una visión de que la regulación de la IA no sea relevante; independientemente de que Occidente, y Estados Unidos en par-

174 https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

175 Aunque el análisis efectuado por Naciones Unidas resalta que su puesta en marcha requiere la firme voluntad de las empresas para lograr su efectividad https://unu.edu/cpr/blog-post/us-executive-order-ai-takeaways-global-ai-governance

ticular, la haya criticado. El origen de su esfuerzo regulatorio procede de la aprobación en 2017 de la estrategia de IA. En 2021 China aprobó una regulación sobre los datos personales más amplio que la IA. La ley denominada *"Personal Information Protection Law" (IPPL)* estaba inspirada en el RGPD (Reglamento General de Protección de Datos) de la UE. El objetivo primordial era asegurar que las empresas que operan en China clasifiquen y almacenen sus datos en China como parte de la estrategia de soberanía digital (Larsen, 2022).

Desde la perspectiva regulatoria, China se ha adelantado en el tiempo a la UE y a Estados Unidos. Las regulaciones más relevantes aprobadas hasta la fecha tienen un **eje central en el control de la información**. Estas son: la regulación sobre "*Algoritmos de recomendación de IA*" en 2021, la regulación sobre *"Síntesis profunda de servicios de información de Internet"* (focalizado en el contenido generado sintéticamente) de 2022, y las reglas sobre "*IA generativa"* de 2023 (aún en modo borrador).

Como se indica en la figura 36, las regulaciones siguen un doble y simultáneo proceso de desarrollo: un **marco político** (a la izquierda de la figura) que conduce a la aprobación por el Partido Comunista de China, y un **marco de impacto tecno-económico** (a la derecha de la figura) no limitado exclusivamente a China, sino también a su impacto en otros países en desarrollo influidos por China.

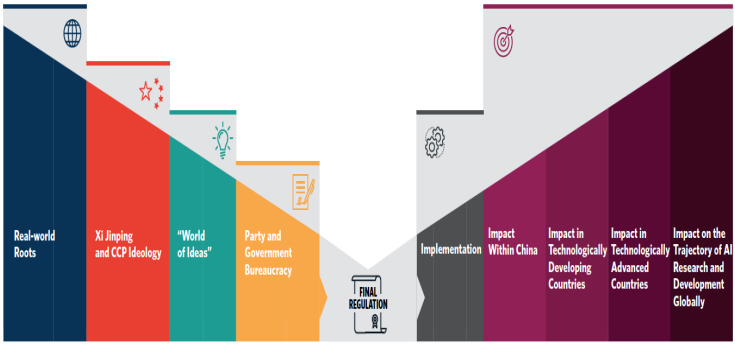


Figura 36. Modelo regulatorio de China. Fuente: Sheehan, 2023

La **regulación sobre algoritmos de recomendación** no solo da derechos a los usuarios, y mayor transparencia de los criterios de recomendación, anticipándose a otros países, sino que también instruye a las empresas privadas a realizar una labor de auto-moderación de contenidos para asegurar que sean "positivos" y que estén alineados con los objetivos del gobierno chino (p.ej. contenido patriótico o a favor de la familia).

La **regulación de la "síntesis profunda"** de los servicios de información de Internet requiere colocar etiquetas visibles en el contenido generado sintéticamente. Y la **regulación sobre IA generativa** requiere que tanto los datos de entrenamiento como los resultados del modelo sean "verdaderos y precisos" (un obstáculo difícil de superar para los *chatbots* de IA).

Otro documento relevante es el de las **normas éticas para la nueva generación de IA** (*Ethical Norms for New Generation AI)* aprobadas en septiembre de 2021. Estas normas incluyen que los humanos deben mantener el control sobre la IA y asumir la responsabilidad final de los sistemas.

El gobierno chino es consciente de que la innovación tecnológica en IA es crucial y presta su apoyo a grandes empresas chinas del sector como **"campeones nacionales"** (*Baidu, Alibaba, Huewei, SenseTime*, etc.) a las que les fuerza a colaborar en la creación de un **ecosistema nacional de IA potente y con proyección internacional**[176]. Evidentemente, el mercado chino es muy grande y muchas empresas de otros países siguen teniendo interés en operar allí, aunque eso suponga la adaptación de sus sistemas para cumplir con el marco regulatorio de China.

Es interesante señalar que el gobierno chino ha intentado también poner trabas al uso de software de código abierto basado en repositorios como *GitHub*, liderado por empresas de Estados Unidos, promoviendo el uso de *Gitee* como alternativa nacional. Conocer en qué medida se trata de una práctica de apoyo a la innovación nacional o de expulsión progresiva de empresas de Estados Unidos no es sencillo de determinar; la frontera es sutil.

Posiblemente, sean las **restricciones impuestas a la importación de circuitos integrados avanzados por Estados Unidos** la que puede parcialmente frenar el desarrollo de la IA por parte de empresas chinas. El entrenamiento de sistemas basados en grandes modelos de lenguaje (LLM) como se requiere en aplicaciones de IA generativa consume enormes capacidades de cálculo y requieren emplear **chips específicos para ejecución de algoritmos de IA** que no van a poder obtener fácilmente. Todavía su sector microelectrónico no es capaz de producirlos.

Parte de esta postura procede del carácter dual de la inteligencia artificial. En el **Plan de Desarrollo de la Nueva Generación de la Inteligencia Artificial** (*AIDP*) aprobado por China en 2017 se ha establecido el siguiente objetivo: *"fortalecer el uso de una nueva generación de tecnología de IA para la toma de decisiones militares y equipamiento de defensa nacional".* Las

176 El esfuerzo de China en obtener datos para el reconocimiento facial y poder entrenar a algoritmos en un grado difícil de alcanzar por otros países se apoya en la instalación desde 2020 de más de 620 millones de cámaras. El objetivo perseguido es doble: el control de la información del ciudadano para preservar la seguridad nacional, y apoyar la competitividad de estos campeones nacionales en los mercados internacionales (Larsen, 2022).

consideraciones de defensa se apoyan en un amplio conjunto de leyes y regulaciones de control de importaciones y exportaciones de productos con IA (Carrozza et al., 2022).

En ese mismo documento se refuerza la **visión estratégica de China de participar en la gobernanza multilateral de la IA**[177]. La gobernanza mundial de la IA es considerada como un área nueva y emergente donde las normas y las instituciones están por crear y China ha llegado a tiempo para ser un actor clave:

"*China participará activamente en la gobernanza global de la IA, fortalecerá el estudio de los principales problemas comunes internacionales, como la alienación de robots y la supervisión de la seguridad, profundizará la cooperación internacional en leyes y regulaciones de IA, reglas internacionales, etc., y enfrentará conjuntamente los desafíos globales".*

Más recientemente, la postura de China ante la **necesidad de un acuerdo multilateral** se ha manifestado por el embajador chino en las Naciones Unidas Zhang Jun en el Consejo de Seguridad el 18 de julio de 2023 (MFA, 2023b) en apoyo al Secretario General Antonio Guterres. Concretamente, su postura inicial fue:

"En la actualidad, como tecnología de vanguardia, la IA todavía se encuentra en su etapa inicial de desarrollo. Como arma de doble filo, si es buena o mala, depende de cómo la humanidad la utilizó, la reguló y cómo equilibramos el desarrollo y la seguridad. La comunidad internacional debe defender el espíritu del verdadero multilateralismo, entablar un diálogo amplio, buscar constantemente el consenso y explorar el desarrollo de principios rectores para la gobernanza de la IA. Apoyamos el papel central de coordinación de las Naciones Unidas en este sentido, y apoyamos los esfuerzos del Secretario General Guterres para mantener discusiones en profundidad entre todas las partes, así como la plena participación de todos los países, especialmente los países en desarrollo, en participar en esta causa y hacer sus propias contribuciones".

El diablo se esconde en los detalles de la diplomacia porque esa visión es seguida por otra sobre la ética de la IA en la que se indica que **la gobernanza de la IA debe alinearse con las condiciones nacionales y características sociales y culturales**. Ello permite una interpretación que puede ser muy distinta de la que ofrezcan otros países con condiciones sociales y culturales diferentes. Reproduzco seguidamente el párrafo aludido.

177 Hasta 2010 China no estuvo dispuesta a tomar ninguna responsabilidad ni a cambiar su enfoque principal orientado a problemas nacionales frentes a los internacionales, especialmente cuando los internacionales se consideraban como un problema creado por Occidente. Posteriormente, su progresiva dependencia de otros países derivada de su integración en cadenas globales de producción hizo cambiar su posición (Cheng y Zhen, 2023a).

"En primer lugar, debemos adherirnos al principio de poner la ética en primer lugar. Los impactos potenciales de la IA pueden exceder los límites cognitivos humanos. Para garantizar que esta tecnología siempre beneficie a la humanidad, es necesario tomar la IA orientada a las personas y la IA para siempre como los principios básicos para regular el desarrollo de la IA y evitar que esta tecnología se convierta en un caballo salvaje desbocado. Sobre la base de estas dos directrices, se deben realizar esfuerzos para establecer y mejorar gradualmente las normas éticas, las leyes, los reglamentos y los sistemas de políticas para la IA, al tiempo que se permite a los países establecer sistemas de gobernanza de la IA que estén en línea con sus propias condiciones nacionales en función de sus propias etapas de desarrollo y características sociales y culturales".

Obviamente, el gobierno de China se opone a todo tipo de restricciones al desarrollo y uso de la tecnología más avanzada de IA procedente de otros países; en realidad, de Estados Unidos sin nombrarlo, y busca un apoyo a una visión de seguridad publicada en febrero de 2023 (MFA, 2023a). Concretamente:

"El desarrollo de la ciencia y la tecnología debe lograr un equilibrio relativo entre el progreso tecnológico y las aplicaciones seguras. El mejor camino es mantener una cooperación abierta, fomentar intercambios y diálogos interdisciplinarios, interindustriales, interregionales y transfronterizos, y oponerse a diversas formas de clubes exclusivos, desacoplamiento y desconexión".

La referencia al *"desacoplamiento"* buscado por Estados Unidos y, parcialmente, por la UE, es claro. En mi opinión, **no será sencillo establecer una gobernanza global de la IA duradera** si persiste un clima de confrontación geopolítica como el actual.

3.3.3.4. Enfoque regulatorio de la IA por la Unión Europea

Desde la perspectiva de la regulación de la IA presentada en las páginas anteriores por Estados Unidos y China, la UE tiene que adoptar una posición que le permita conciliar un **papel activo en el desarrollo de las tecnologías de IA** que fortalezca a las empresas europeas del sector y las haga más competitivas internacionalmente, con una **adecuada protección del consumidor europeo**, al mismo tiempo que ayude a preservar su anhelada **autonomía estratégica**[178].

Se trata de un equilibrio difícil de lograr por la UE y cuya primera piedra se pretende abordar con la ley sobre IA en discusión en los órganos

178 Recuérdese que uno de los objetivos del Decenio Europeo propone que más del 75% de las empresas de la UE adopten tecnologías de nube, IA y big data en 2030.

comunitarios[179] (European Commission, 2021b). Sin entrar en excesivos detalles, es relevante comentar los elementos claves de la regulación de IA impulsada por la UE.

El interés partió en abril de 2018 con una *"Comunicación"* de la Comisión Europea titulada ***"Inteligencia Artificial para Europa"*** a la que siguió otra en diciembre del mismo año sobre un ***"Plan coordinado para la Inteligencia Artificial"***. Ese mismo año, en abril de 2018, 24 estados miembros y Noruega firmaron una *"**Declaración de Cooperación en Inteligencia Artificial"*** para formalizar su intención de responder colectivamente a los retos y oportunidades de la IA. Con ello, el debate político sobre la IA estaba abierto.

El siguiente año, en abril de 2019, la Comisión Europea quiso focalizar el esfuerzo en lo que denominaba *"la construcción de confianza en una inteligencia centrada en el ser humano",* seguida por otra comunicación en 2020 denominada ***"Inteligencia Artificial: Un enfoque europeo para la excelencia y la confianza"*** apoyada por un grupo de expertos que, en 2019, publicó un documento titulado *"**Directrices éticas para una IA confiable**"* (European Commission, 2019) que enmarcaba un problema básico para el despegue de la IA en la sociedad: incrementar la confianza en los algoritmos empleados en las aplicaciones.

El impulso a la IA desde la Unión en el periodo 2018-2020, además de un incremento de la financiación de proyectos de I+D en IA a través del programa marco de investigación e innovación de la UE H2020, se ha orientado al **establecimiento de normas éticas** con un enfoque *"centrado en la persona*" aprovechando el potencial regulatorio y el mercado único europeo como una ventaja competitiva. Esto es lo que la UE denomina **IA confiable** ("*trustworthy AI*") una visión que se centra en la transparencia, diversidad y equidad que podría incrementar la soberanía digital de la Unión.

En octubre de 2020, la preocupación por el desarrollo de la IA alcanzó al Parlamento Europeo que adoptó un texto titulado "***Marco de aspectos éticos de la inteligencia artificial, robótica y tecnologías relacionadas"***. Es interesante que el Parlamento reconoce el papel dual de la IA incorporando una sección sobre seguridad y defensa; concretamente, señala que "*las tecnologías de IA son, en esencia, de uso dual, y el desarrollo de la IA en actividades relacionadas con la defensa se beneficia de intercambios entre tecnologías militares y civiles"*. Asimismo, el Parlamento remarca que se trata de una tecnología disruptiva transversal que *"puede proporcionar oportunidades para la competitividad y la autonomía estratégica de la Unión".*

179 Se pretende introducir una modificación en la Ley por la que las empresas que implementen herramientas generativas de IA, como ChatGPT o el generador de imágenes Midjourney, también tendrán que revelar cualquier material con derechos de autor utilizado para desarrollar sus sistemas.

En esos años, algunos países europeos empiezan a discutir el desarrollo de normativas nacionales y a compartir la **necesidad de atajar riesgos**. Al igual que en los Estados Unidos, también la UE ha dado pasos para incrementar la coordinación y convergencia con los estados miembros para disponer de una regulación sobre la IA incluyéndola en 2021 en el **control de exportación de tecnologías sensibles de doble uso.**

Finalmente, la Comisión Europea en abril de 2021 publicó su **"Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen Normas Armonizadas en Materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se Modifican Determinados Actos Legislativos de la Unión**".[180] Como se indica en el texto a debate: *"La propuesta se basa en los valores y derechos fundamentales de la UE y tiene por objeto inspirar confianza en los ciudadanos y otros usuarios para que adopten soluciones basadas en la IA, al tiempo que trata de animar a las empresas a que desarrollen este tipo de soluciones".*

El texto de la Comisión propone un **marco reglamentario sobre inteligencia artificial** con los siguientes objetivos específicos:

- *garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión;*
- *garantizar la seguridad jurídica para facilitar la inversión e innovación en IA,*
- *mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA;*
- *facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado.*

La UE asume y aplica el "principio de precaución" de las administraciones públicas en relación con la IA mediante un numeroso **grupo de prohibiciones a diferentes niveles** para proteger al usuario. La propuesta clasifica el uso en función de los **niveles de riesgo para el usuario: inaceptable, alto, limitado, y mínimo**[181]**.** Como ejemplo, se limitan aquellas prácticas que tienen un gran "*potencial para manipular a las personas mediante técnicas subliminales que trasciendan su consciencia o que aprovechan las vulnerabilidades de grupos vulnerables concretos, como los menores o las personas con discapacidad, para alterar de manera sustancial su comportamiento de un modo que es probable que les provoque perjuicios físicos o psicológicos a ellos o a otras personas".*

180 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0206 (accedido el 8 de enero de 2023).

181 Se utiliza un enfoque de riesgos similar al empleado para la regulación de los dispositivos médicos.

La propuesta prohíbe igualmente que las autoridades *"realicen calificación social basada en IA con fines generales"*. Por último, también se prohíbe, salvo excepciones limitadas, el *"uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley"*.

El proceso de negociación es lento e implica, tras la propuesta realizada por la Comisión Europea, al Consejo y al Parlamento Europeo. El **Consejo de la Unión Europea** adoptó su **posición común** sobre la Ley de IA en diciembre de 2022. En su posición el Consejo redujo la definición de "sistema de IA" cubierta por la Ley de IA para centrarse en una medida de autonomía, es decir, para garantizar que los sistemas de software más simples no se capturaran inadvertidamente. El 14 de junio de 2023, el **Parlamento Europeo** votó a favor de adoptar su propia posición de negociación sobre la Ley de IA, lo que abrió el proceso de discusión ("Diálogo Tripartito") entre la Comisión Europea, el Consejo y el Parlamento para conciliar las tres versiones y llegar a una aprobación final de la Ley de IA.

Con el acuerdo político alcanzado en el Diálogo Tripartito a finales del año 2023 sobre una versión de consenso para convertirse en ley en los primeros meses de 2024, la Ley de IA estará sujeta a un **período de implementación de dos años** durante el cual deberán establecerse sus estructuras de gobernanza, por ejemplo, la *Oficina Europea de Inteligencia Artificial*, antes de ser finalmente aplicables a todos los proveedores de IA a finales de 2025 o comienzos de 2026 como pronto.

Los últimos problemas que han retrasado el acuerdo alzanzado en el Diálogo Tripartito[182] sobre temas como los siguientes:

- Uso de IA para la vigilancia biométrica en espacios públicos. El Parlamento introdujo prohibiciones que limitan el uso de la aplicación de la ley, que probablemente serán objetadas por los gobiernos de los Estados miembros en el consejo.
- Definición de IA de alto riesgo. El Parlamento permite una definición más amplia de los casos de uso para la IA de alto riesgo, mientras que el Consejo preferiría reducir esa definición.
- Gobernanza. Discusión sobre los silos nacionales en términos de implementación y cumplimiento, así como los niveles de coordinación.
- Regulación de la IA generativa. Si bien la Ley considera los usos posteriores de los modelos, no considera otros aspectos cruciales de la cadena de suministro (construcción de conjuntos de datos y método de entrenamiento).

182 https://hai.stanford.edu/news/analyzing-european-union-ai-act-what-works-what-needs-improvement

- Evaluaciones de las aplicaciones de alto riesgo después de la entrada en vigor.

Teniendo en cuenta que la Ley de IA comenzó a prepararse en 2020 y entrará plenamente en vigor en 2026, supondrá **seis años de elaboración e implementación** completa en los que la tecnología de la IA cambiará profundamente (piénsese simplemente en la IA generativa). **La pregunta es si la Ley será capaz de cubrir esta evolución tecnológica tan rápida en un marco legislativo sólido y estable** que proporcione garantías jurídicas a las empresas.

Como ejemplo de estos desajustes en base a la rápida evolución de la tecnología, la regulación en discusión se estructura alrededor de la idea de que **cada aplicación de IA se asigne a una categoría de riesgo basada en su uso previsto**. Este enfoque refleja el tradicional de la UE basado en que cada producto tiene un fin único y bien definido. Sin embargo, el uso de modelos fundacionales (MLL) en la IA generativa puede permitir personalizarse a muchos usos potenciales por los usuarios finales, algunos de alto riesgo y otros no. ¿Qué se quiere hacer? Una opción sería asumir que la tecnología basada en MLL es de alto riesgo, independientemente de lo que se haga con ella, y otra sería ir caso a caso (inviable). Si los mecanismos que se implementen para otorgar las "licencias" en la UE son muy complejos, beneficiará a las grandes empresas que ya se han posicionado y tienen los medios para hacerlo, en contra de la PYMES; no creo que se quiera eso.

En resumen, será necesario, en mi opinión, que la UE sepa **encontrar un equilibrio** en la redacción final y disponga de los medios adecuados y suficientes para monitorizar de forma continua su **cumplimiento** en todos los estados miembros.

La pregunta, sin contestación todavía, es si este enfoque regulatorio de la UE será el seguido por terceros países como Estados Unidos y China, con procesos regulatorios diferentes, y si una aplicación muy estricta de la misma puede hacer que la UE quede fuera del proceso de innovación en IA ampliándose la brecha ya existente. Intentar llegar, mientras tanto, a **acuerdos voluntarios**, al menos entre la UE y Estados Unidos, parece un camino útil teniendo en cuenta el peso de las empresas de IA de Estados Unidos en la UE[183].

183 Margrethe Vestager, vicepresidenta ejecutiva de la Comisión Europea en la reunión de mayo de 2023 del Consejo de Comercio y Tecnología (TTC) entre Estados Unidos y la UE promovió la elaboración de un "código de conducta" voluntario para productos de IA generativa y generó expectativas de que dicho código podría redactarse "en cuestión de semanas". https://www.reuters.com/technology/eu-tech-chief-calls-voluntary-ai-code-conduct-within-months-2023-05-31/

Este proceso deberá tener en cuenta también cómo se produce la entrada en vigor de otros instrumentos legislativos complementarios como son la Ley de mercados digitales y la Ley de servicios digitales aprobadas recientemente. Todo ello configura el **marco legislativo digital de la UE cuyo impacto deberá analizarse de forma conjunta.**

La valoración de la **situación de soberanía tecnológica europea en el caso de la inteligencia artificial en base al modelo multinivel** presentado anteriormente se representa en la figura 37.

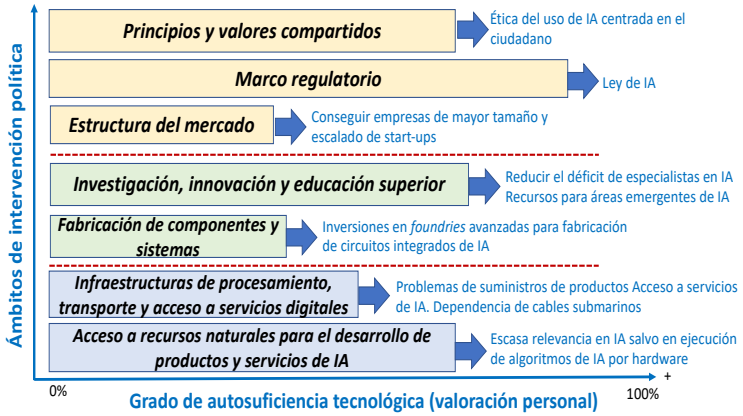


Figura 37. Valoración personal del grado de autosuficiencia tecnológica de la UE en la tecnología de inteligencia artificial. Fuente: elaboración personal

Tampoco puede la UE estar ajena a la posición de Estados Unidos en torno a la IA; su enorme relevancia en el mercado impide prescindir de un enfoque autárquico y refleja la necesidad de acometer un proceso de acercamiento. El órgano básico para ello es el denominado ***"Trade and Technology Council (TTC)"***. En la última reunión del TTC mantenida en Suecia el 30 y 31 de mayo de 2023 se acordó respecto a la IA en la *Declaración conjunta*[184] (subrayados personales):

"La Unión Europea y los Estados Unidos reafirman su ***compromiso con un enfoque de la IA basado en el riesgo para promover tecnologías de IA fiables y responsables****. Cooperar en nuestros enfoques es clave para promover la innovación responsable de la IA que respete los derechos y la seguridad y garantice que la IA proporcione beneficios en línea con nuestros valores democráticos compartidos.* ***Los desarrollos recientes en IA generativa resaltan la escala de las oportunidades y la necesidad de abordar los riesgos asociados****.... Tenemos la intención de ampliar*

184 https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2992

los términos compartidos de IA, continuar nuestro progreso hacia el avance de los estándares y herramientas de IA para la gestión de riesgos de IA, y desarrollar un catálogo de riesgos existentes y emergentes, incluida una comprensión de los desafíos planteados por la IA generativa.".

Veremos si este compromiso se refleja en futuras **regulaciones de IA compatibles** en las que, por ahora, la UE ha tomado la delantera en el proceso legislativo.

3.4. ¿AUTONOMÍA ESTRATÉGICA O INTERDEPENDENCIA DIGITAL INTELIGENTE?

3.4.1. Visión desde el Sur Global

Aunque el periodo transcurrido desde el arranque del proceso iniciado hacia una mayor autonomía estratégica europea es aún corto, sí puede extraerse una consecuencia inicial: **la UE no puede aspirar a conseguir una autonomía estratégica, aunque la califique de "abierta", con el beneplácito y aplauso de sus competidores y sin incrementar los riesgos globales para la misma UE en su relación con otros países.**

En definitiva, apostar por una autonomía estratégica excluyente tiene un **coste geopolítico para la UE si quiere jugar un papel "equilibrador" a nivel global** que es necesario valorar.

Esta situación se manifiesta no solo porque en el interior de la UE surgen **posiciones divergentes entre estados miembros** en función de su posición de partida e intereses nacionales ante la autonomía estratégica que dificultan y ralentizan la creación de un marco regulatorio común, sino, y más relevante, en sus relaciones con otros países del grupo (muy heterogéneo) denominado **Sur Global**[185]. Empleando la visión de Torreblanca (2023): "*muchos países del Sur Global ya no ven a la UE como un actor que defiende un sistema abierto y basado en reglas, sino como uno que los empuja a unirse a los esfuerzos de Estados Unidos y Europa para derrotar a Rusia y contener a China. Consideran que un mundo de sanciones, controles de exportación, control de inversiones y medidas proteccionistas es perjudicial para su crecimiento e intereses".*

La visión de *"vuelta a la escena geopolítica del Sur Global"*, latente desde hace años, pero acelerada recientemente por las presiones realizadas a mu-

185 El término "Sur global" tiene sus orígenes en el siglo XX. Fue utilizado en un conocido informe de 1980, Norte-Sur: Un Programa para la Supervivencia, publicado por un comité independiente dirigido por el excanciller alemán Willy Brandt, y en un informe de 1990, El desafío al Sur: El informe de la Comisión del Sur, emitido por un panel de la ONU dirigido por Julius Nyerere, entonces presidente de Tanzania. El prefijo "global" se agregó en la década de 1990 después del final de la Guerra Fría, posiblemente un subproducto de la creciente popularidad de otro término, "globalización", que se puso de moda en ese momento (Shidore, 2023).

chos países para sumarse a las sanciones impuestas a Rusia tras la guerra de Ucrania, tiene una relevancia creciente para la UE. De hecho, algunos de estos países han aumentado en 2022 sus relaciones comerciales con Moscú, reduciendo la eficacia de las sanciones occidentales[186] (Shidore, 2023).

Si bien **el concepto de autonomía estratégica abierta se aplica a todos los ámbitos y sistemas tecnológicos**, es en el **sector digital** en el que se manifiesta con mayor impacto por el doble hecho de su carácter habilitador y de una tasa de evolución tecnológica muy rápida. No es extraño observar que, en este contexto, **muchos países ajenos a la UE perciben la implementación de la autonomía estratégica digital de la UE desde una óptica defensiva,** como una forma moderna de apuntalar el viejo proteccionismo europeo como, según ellos, demuestra la voluntad política europea de establecer un marco regulatorio digital defensivo no consensuado en órganos multilaterales, sino "impuesto unilateralmente" a empresas de otros países para poder operar en el mercado digital de la Unión.

En la dimensión económica digital el esfuerzo de la UE en atraer inversiones a sus estados miembros de fábricas de semiconductores, de grandes centros de datos, o de centros de desarrollo de IA, contribuye aún más a esta percepción porque estos recursos no van a permitir inversiones avanzadas en otros países por las limitaciones de los recursos humanos (sometidos también a una presión para desplazarse a la UE) y materiales, y por las condiciones impuestas en tecnologías digitales concretas. Los datos de las inversiones privadas complementadas por las subvenciones procedentes de la *Chips and Science Act* en Estados Unidos o la equivalente en la UE corroboran este desplazamiento.

Es cierto que, en la medida en la que el **tamaño y nivel innovador del mercado europeo** siga siendo esencial para las grandes empresas digitales, esta estrategia podría seguir siendo válida porque las grandes corporaciones estarán dispuestas a realizar las **adaptaciones técnicas y comerciales necesarias de sus productos o servicios** para asegurar su lanzamiento prioritario en la UE, pero no tiene por qué seguir siendo así en el futuro. En algunos casos, ya empieza a observarse que la UE está siendo relegada en el lanzamiento mundial de algunos productos y aplicaciones digitales muy innovadoras por la inseguridad jurídica de una legislación europea cuyo alcance aún no está totalmente definido.

De hecho, las **tensiones entre gobiernos y grandes empresas digitales sobre el alcance legal de las normativas europeas** en la responsabilidad de los operadores de plataformas en ciberseguridad o en los

186 En 2022, el comercio de Rusia aumentó en un 87% con Turquía, en un 68% con los Emiratos Árabes Unidos y en un enorme 205% con la India.

límites impuestos a la privacidad de los datos, o en el contenido capturado, almacenado y distribuido, reflejan la tensión geopolítica con efectos sobre el proceso innovador desde posiciones ideológicas muy diferentes.

Debe señalarse que, a diferencia de otras grandes potencias tecnológicas, **Europa no puede basar su estrategia en defender los supuestos intereses de grandes empresas digitales porque no las tiene con un tamaño comparable**. Su apelación a que los cambios normativos tienen un efecto positivo para proteger a las PYME digitales europeas o por atraer o retener talento digital está por demostrar, pero sí ha quedado claro que asume la protección al *"ciudadano"* como eje de su actuación.

Para otros gobiernos con grandes empresas digitales surgidas en su territorio, pero operando en todo el mundo con centenares de millones de usuarios como es el caso de Estados Unidos y, en cierta medida, de China, **la tentación es "contraatacar" aprobando un conjunto de normas proteccionistas similares, lo que contribuirá a fragmentar aún más el mercado**. Es evidente que la entrada en otros mercados de los productos y servicios digitales europeos implica la necesidad de aceptar recíprocamente las regulaciones digitales aprobadas en los mismos.

3.4.2. Interdependencia digital y el calificativo de "abierto" aplicado a la autonomía estratégica

Ya se ha comentado previamente que la UE ha calificado su concepción de autonomía estratégica con el término ***"abierta"*** pretendiendo con ello preservar la cooperación con otros países, cuando sea posible. También se ha mencionado que su potencial contradicción y ambigüedad en el proceso de implementarla que liga cualitativamente el **grado de apertura** a factores histórico-culturales, económicos y políticos de la UE combinados en dosis coyunturales cambiantes en cada caso hacía difícil su aceptación por terceros países. Este problema se ha manifestado, sobre todo, en aquellos países que forman parte de ese conglomerado heterogéneo conocido como ***Sur Global*** que desean adquirir un mayor protagonismo.

Algunos autores han propugnado recientemente, no solo en el ámbito digital, que la UE debería focalizarse más en **desarrollar el concepto de *"interdependencia"*** reduciendo el énfasis en la defensa de la autonomía estratégica para reducir la carga negativa asociada en terceros países y favorecer un papel global equilibrador que la Unión está perdiendo. Concretamente, Torreblanca (2023) lo expresaba en agosto de 2023 de la siguiente forma (el énfasis es mío): *"La UE debe adoptar esta interdependencia estratégica* ***aumentando las interdependencias con aliados y socios clave, y reduciéndolas al mismo tiempo con sus rivales****. La autonomía*

estratégica es una estrategia reactiva para abordar los desafíos actuales; La interdependencia estratégica es una forma proactiva de satisfacer las necesidades de Europa y superar las limitaciones de la autonomía estratégica" (Torreblanca, 2033).

El problema es que **la adjetivación de los países externos a la Unión como "aliados", "socios clave" y "rivales" es ambigua y evoluciona con el tiempo** en función de la evolución de sectores y tecnologías; no se trata, por tanto, de un concepto legal, aunque se plasme en determinados acuerdos. Como consecuencia, no permite dotar a las relaciones tecnológicas internacionales de la UE de la suficiente estabilidad temporal como para mantener interdependencias estratégicas fructíferas.

Además, **no vale cualquier tipo de interdependencia**. Deberá ser (muy) ***inteligente*** para que rompa la visión negativa existente con la *autonomía estratégica abierta* y sea capaz de generar una cascada de adhesiones o aproximaciones similares en otros países que promueva una **colaboración activa en la definición del marco futuro de colaboración**. Más concretamente, centrada la discusión en el ámbito digital, el concepto de **interdependencia digital inteligente** tiene, en mi opinión, **tres dimensiones básicas** que deberán servir de guía para su fructífera implementación. Estas son:

- **Cooperación internacional digital estable** basada en la contribución en diversos eslabones de la cadena de valor del desarrollo de productos y servicios digitales. Se concretaría en reducir las barreras artificiales existentes que impiden lograr una interdependencia del tipo *"ganar-ganar"*.
  Para conseguirlo, es necesario romper la tendencia a fortalecer cadenas de valor fuertemente asimétricas en muchos de los eslabones con ganadores y perdedores alimentadas por enfoques como *"friend-shoring"* y aranceles discriminatorios porque eso genera una reacción proteccionista con diversas herramientas que se potencian entre sí: condiciones restrictivas de entrada al mercado en función del origen, restricciones al movimiento de capitales, barreras al acceso y circulación del talento, ventajas arancelarias derivadas de la pertenencia a bloques, etc.
- **Interdependencia especializada**. Se trataría de aceptar la especialización tecnológica de zonas geográficas y sectores empresariales asumiendo la existencia de cadenas de valor resilientes tanto físicas como virtuales ligadas al intercambio de datos en determinados eslabones de la cadena de valor que genere confianza entre los actores. La confianza está ligada a la seguridad (tanto ciber como física) lo

que implica una cooperación a largo plazo no solo entre empresas sino también entre gobiernos. El ejemplo de los cables de datos submarinos es un ejemplo.
En la situación actual, la percepción por parte de terceros países de que la autonomía estratégica europea implica la (promoción de la) reubicación de capacidades de un país a otro (basado en la implementación de los conceptos de *re-shoring o friend-shoring*) no contribuye a generar el clima de confianza necesario.

- **Desarrollo de un marco regulatorio digital.** Para ello, deberá estar consensuado y basado en un triple acuerdo: a) favorecer la experimentación para promover la innovación, b) aplicar el principio de precaución para el consumidor final, y 3) adoptar una visión de la normativa centrada en el usuario y no en el desarrollador.
No se trata con ello de reducir la regulación digital para hacerla más laxa, sino abordar el conocido *dilema de Collingridge* anticipando los problemas regulatorios con datos procedentes de espacios de prueba regulatorios (sandboxes) en todo el mundo, asegurar el desarrollo de productos con datos que asuman la diversidad de usuarios y países[187], con un esfuerzo mayor en la formación digital de los usuarios en diferentes niveles de especialización.

Para que una interdependencia digital inteligente sea eficaz será necesario **modificar las estructuras de gobernanza digital actuales**. En mi opinión, no basta con mantener una discusión bilateral sobre normativas o estándares en ciberseguridad o IA como el TTC hace entre la UE y Estados Unidos, ni tampoco basta con abordarlo en foros multilaterales restrictivos como el G7 o estructuras similares. No es suficiente. Articularlo en el contexto de organizaciones surgidas desde el concepto del Sur Global o la expansión de los países BRICS (si sus disensiones internas no la hacen inoperativa) puede ser relevante cara a una gobernanza digital global

En este contexto, las Naciones Unidas pueden desempeñar un papel fundamental en la promoción de esta gobernanza digital. Ya en 2020, las Naciones Unidas, anticipando algunos de los problemas que ahora se han hecho evidentes, abogaba por una **"cooperación digital"** que incorporase a todos los actores: *"La cooperación digital es un esfuerzo de múltiples actores y, si bien los gobiernos siguen ocupando un lugar central, es esencial la participación del sector privado, las empresas de tecnología, la sociedad civil y otras partes interesadas. Es vital comprometerse con el sector privado, la comunidad técnica y la sociedad civil desde el principio si se quieren tomar decisiones y políticas realistas y efectivas".* (UN, 2020). Como es ha-

187 Evitando con ello los sesgos derivados, por ejemplo, del entrenamiento de algoritmos de IA con conjuntos de datos procedentes de un solo país, aunque sus usuarios estén en todos los países.

bitual en el marco de las Naciones Unidas, **su capacidad para imponer acuerdos es muy limitada** y se quedan en reflexiones conceptuales y en programas de actuación voluntaria muy limitados.

En resumen, en el ámbito digital, **la UE deberá reinterpretar el calificativo de "abierta" aplicado a la autonomía estratégica en el contexto de una interdependencia inteligente** que se implemente de forma proactiva con terceros países, aceptando un mayor protagonismo de algunos países y regiones en su relación con la UE.

4

DIGITALIZACIÓN EN DEFENSA: RETO DE LA UE

4.1. CONTEXTO

Las **capacidades comunes de defensa europeas**, base del poder duro, son limitadas. El fracaso de la constitución de la *Comunidad Europea de Defensa* en los años cincuenta del siglo XX hizo que, en la práctica, y durante todo el periodo de la Guerra Fría, fuese Estados Unidos directamente, o a través de la OTAN, quien tomase esa responsabilidad. Europa aceptó ceder esa capacidad lo que, desde un punto de vista positivo, permitió centrarse en su propio desarrollo económico como gran baza política hacia sus ciudadanos, asegurando que las tropas de Estados Unidos permanecerían en Europa; hecho que sigue ocurriendo en la actualidad, aunque en menor cuantía.

La **ambición política de la UE en alcanzar una autonomía estratégica en defensa** aparece ya a finales del siglo pasado (Burni et al., 2023) (Biscop, 2021). En diciembre de 1999, las conclusiones del Consejo Europeo de Helsinki establecieron el alcance de la autonomía como objetivo de la **Política Común de Seguridad y Defensa (PCSD)** de la UE, especificando los objetivos principales, que establecían en ese Consejo que la UE debería poder desplegar hasta un cuerpo de ejército (50-60.000 soldados) en un plazo de 60 días y mantener el despliegue durante al menos un año.

Nada de eso se hizo realidad, a pesar de la creación de instrumentos específicos; la ambición chocó con la realidad de presupuestos de defensa menguantes en los estados miembros y la visión de que el mundo era suficientemente estable y el paraguas de la OTAN, en manos de Estados Unidos, suficiente. La creciente **emergencia de conflictos político-militares** en los que la UE se siente más amenazada ha hecho cambiar esta percepción.

En junio de 2016, la Vicepresidenta de la Comisión y Alta Representante de la Unión en ese momento Federica Mogherini presentó al Consejo

Europeo la denominada "**Estrategia Global sobre Política Exterior y de Seguridad de la Unión Europea"** (Estrategia Global de la UE), en la que se definía la estrategia para la puesta en marcha de la PCSD[186] [187].

El objetivo de autonomía estratégica en defensa ha vuelto a relanzarse recientemente con la creación de ***PeSCO*** (*Permanent Structured Cooperation*). Se debe mencionar que la creación del **Fondo Europeo de Defensa** (**FED)**[188] con la adjudicación de proyectos y publicación de convocatorias[189], o el **Fondo Europeo de Apoyo a la Paz (FEAP)** aprobado en 2021, empleado en el apoyo a Ucrania[190], incrementan la visibilidad de la defensa común y alientan un mayor compromiso político en su implementación.

La aprobación en febrero de 2022, al iniciarse la guerra en Ucrania, de la denominada ***"Brújula estratégica para la seguridad y la defensa de la UE"***[191] (Unión Europea, 2022) supuso un cambio de paradigma en defensa y seguridad al poner encima de la mesa de los Jefes de Estado y de Gobierno europeos la necesidad de progresar en una **defensa común compatible y complementaria a la pertenencia a la OTAN** de muchos de sus estados miembros. Su adopción en marzo de 2022 confirmó la voluntad de los Estados miembros en reforzar su compromiso militar para construir una Europa de la defensa, especialmente tras la invasión rusa de Ucrania.

Decisiones recientes de hondo significado político como supone la creación de la **Capacidad de Despliegue Rápido de la UE** que el Parlamento Europeo ha ratificado en abril de 2023[192], y que permitirá la creación de una fuerza de intervención de 5.000 soldados más todo el personal

186 Se determinaron cinco prioridades: la seguridad de la Unión; la resiliencia estatal y social de los vecinos orientales y meridionales de la Unión; la concepción de un enfoque integrado en relación con los conflictos; los órdenes regionales de cooperación; y una gobernanza mundial para el siglo XXI. https://www.europarl.europa.eu/factsheets/es/sheet/159/la-politica-comun-de-seguridad-y-defensa#:~:text=La%20PCSD%20es%20el%20principal,paz%20y%20la%20seguridad%20internacionales.

187 La UE ha llevado a cabo treinta y siete operaciones y misiones en tres continentes. Desde marzo de 2022, hay dieciocho misiones y operaciones PCSD en curso (once misiones civiles y siete operaciones militares, incluidas dos en el ámbito marítimo). Alrededor de 4.000 miembros del personal militar y civil de la Unión están actualmente desplegados en el extranjero.

188 El Reglamento del Fondo Europeo de Defensa fue presentado por la Comisión Europea en 2018 y aprobado por el Consejo Europeo en 2021.

189 https://defence-industry-space.ec.europa.eu/european-defence-fund-eu12-billion-boost-eu-defence-capabilities-and-new-measures-defence-innovation-2023-03-30_en

190 El 26 de junio de 2023, el Consejo adoptó una Decisión para aumentar el límite financiero global del Fondo Europeo de Apoyo a la Paz (FEAP) en 3.500 millones de euros. El límite financiero global asciende ahora a más de 12.000 millones de euros (a precios corrientes). https://www.consilium.europa.eu/es/policies/european-peace-facility/

191 Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales, aprobado por el Consejo el 21 de marzo de 2022 y refrendado por el Consejo Europeo el 25 de marzo de 2022. El objetivo principal de la Brújula Estratégica es proporcionar orientación política para la puesta en práctica de la "autonomía estratégica" en cuatro áreas notables: gestión de crisis, resiliencia, capacidades y asociaciones.

192 Resolución del Parlamento Europeo, de 19 de abril de 2023, sobre la Capacidad de Despliegue Rápido de la UE, grupos de combate de la UE y artículo 44 del TUE: próximas etapas (2022/2145(INI)). Parlamento Europeo. P9 TA (2023)0113.

y medios de apoyo necesarios al mando del *Vicepresidente de la Comisión y Alto Representante de la UE*, con recursos puestos en juego de forma independiente a los de la OTAN, demuestran una incipiente voluntad de **construcción progresiva del "poder duro" de la UE que reafirme su papel en el mundo**.

4.2. LA DIGITALIZACIÓN DE LA DEFENSA

La problemática de la autonomía estratégica digital de la UE presentada en las secciones anteriores concentra en el **sector de la defensa** un interés y repercusiones aún mayores al sumarse a su dependencia en el uso de tecnología avanzada otros **condicionantes de seguridad adicionales** que obliga a considerar los elementos de autonomía estratégica y soberanía tecnológica en términos diferentes ligados a compromisos internacionales.

Parto del reconocimiento de que existe un amplio acuerdo de que la **digitalización**[193] **del campo de batalla es imparable**, y se ha convertido en una condición necesaria para *asegurar la superioridad* en los conflictos. Se asume que el éxito en el proceso de digitalización militar marcará diferencias sustanciales entre países. Reproduzco el párrafo de Pérez-Martínez (2023) con el que estoy de acuerdo, aunque no solo ligado a la IA.

"En los próximos años se producirá una brecha digital en la IA entre los países que dispongan de una "Defensa Nacional Inteligente" potente -con unos sistemas militares dotados de IA, personal capacitado para diseñarlos, producirlos y operarlos, y recursos invertidos en su despliegue- y otros que no. Las decisiones que se tomen ahora definirán a que grupo se pertenecerá en el futuro… y también el peso de cada país en la nueva economía digital globalizada"

Este proceso de transformación tecnológica se inició durante la última década del siglo pasado en lo que se denominó la **"Revolución de los Asuntos Militares"** (*Revolution in Military Affairs*): un concepto que recogía la necesidad de utilizar las *nuevas tecnologías* para mantener la eficacia de las Fuerzas Armadas de Estados Unidos (Cordesman, 2014). Pronto la experiencia demostró en Estados Unidos y en otros países que la dimensión tecnológica militar no era suficiente y debía ir acompañada de una **transformación profunda de las organizaciones militares y de las operaciones** en el campo de batalla para que las tecnologías digitales en las operaciones militares tuvieran el impacto deseado.

La **confluencia de múltiples tecnologías en el campo de batalla** está haciendo que no solo la obtención de datos en tiempo real de múl-

193 En castellano se entiende por digitalización tanto al proceso de convertir algo no digital en una representación digital, como al uso de tecnologías y datos digitales para optimizar una actividad haciéndola más eficiente, productiva y/o rentable. En inglés hay una distinción entre los términos "digitization" y "digitalization".

tiples sensores y su integración en sistemas de armas haya adquirido una relevancia fundamental, sino que también lo es la incorporación de la inteligencia artificial en la toma de decisiones. De esta manera, se está produciendo una **transición desde un campo de batalla digital a otro "inteligente"** en el que la superioridad militar depende de la capacidad de integrar tecnologías digitales emergentes y acelerar el proceso de toma de decisiones desde el nivel del soldado individual al del planeamiento de operaciones del estado mayor.

La **guerra provocada por la invasión rusa de Ucrania** también ha reforzado la importancia de trasladar al terreno operativo lo antes posible muchos desarrollos recientes de hardware y software que puedan suponer una ventaja estratégica. Los notables desarrollos recientes en la optimización en el uso integrado de datos procedentes de múltiples sensores en apoyo de la toma de decisiones, o la emergencia en IA de los *Grandes Modelos de Lenguaje (LLM*), están intensificando la competencia estratégica relacionada con la IA. **Acceder a datos de alta calidad y a la capacidad de análisis de estos se ha convertido en un componente crítico de la capacidad de combate.**

El documento preparado por el gobierno del RU (UK, 2023) **resume las lecciones extraídas de la guerra de Ucrania** desde un punto de vista de innovación estratégica: *"La guerra en Ucrania también nos ha proporcionado un claro recordatorio de la necesidad de adaptarse rápidamente e innovar constantemente en la guerra, ya sea creando nuevas capacidades o adaptando las existentes. La combinación dinámica de nuevas capacidades, la creciente interconexión y un entorno de datos en expansión exige un enfoque digital en el corazón de la defensa y la disuasión*".

Actualmente, no es posible disociar el proceso de digitalización en Europa de las **relaciones entre la UE y la OTAN** a la que pertenecen la mayor parte de los estados miembros de la Unión. Desde ambas perspectivas, conseguir el mayor nivel de digitalización de forma integrada e interoperable es necesario; no es extraño por ello que la OTAN y la UE se hayan embarcado simultáneamente en un **proceso de transformación digital del sector de la Defensa acelerado** por un recrudecimiento de conflictos en las fronteras de Europa que han incrementado simultáneamente la preocupación colectiva y los presupuestos de defensa.

En este contexto, entre los años 2022 y 2023, la OTAN adoptó su primera **visión de transformación digital** y una estrategia de implementación de transformación digital. En paralelo, la UE respaldó un plan estratégico de implementación para *la "digitalización de las fuerzas de la UE, efectos cibernéticos integrados en las operaciones militares de la UE y capacidades digitales prioritarias"* como parte del cuarto pilar (inversión) de su estrategia

denominada "***Brújula Estratégica***" (*Strategic Compass*) (Soare, 2023).

El alcance de la transformación digital es **ambicioso** tanto en la OTAN como en la UE y dada la complejidad se realizará de forma progresiva durante la presente década, aunque **de forma acelerada en función de la necesidad de incorporación operativa ante la persistencia de conflictos activos**. La transformación digital de la defensa incluye pilares tecnológicos, organizativos-procedimentales y de adaptación de los recursos humanos, priorizando actuaciones sobre los datos, la nube y un enfoque actualizado de la ciberseguridad.

Obviamente, no se parte de cero. En la situación actual, todas las fuerzas armadas europeas utilizan al menos algunas tecnologías digitales y sistemas de planificación de recursos empresariales de defensa (EPR). También las empresas y organismos de defensa se han parcialmente digitalizado, con ritmos diferentes. En todo caso, las restricciones presupuestarias y la necesidad de integración han hecho que el modelo de digitalización haya sido el de una **innovación incremental**. La figura 38 destaca los **niveles comparativos genéricos de digitalización de la defensa en toda Europa** de acuerdo con datos de Soare (2023).

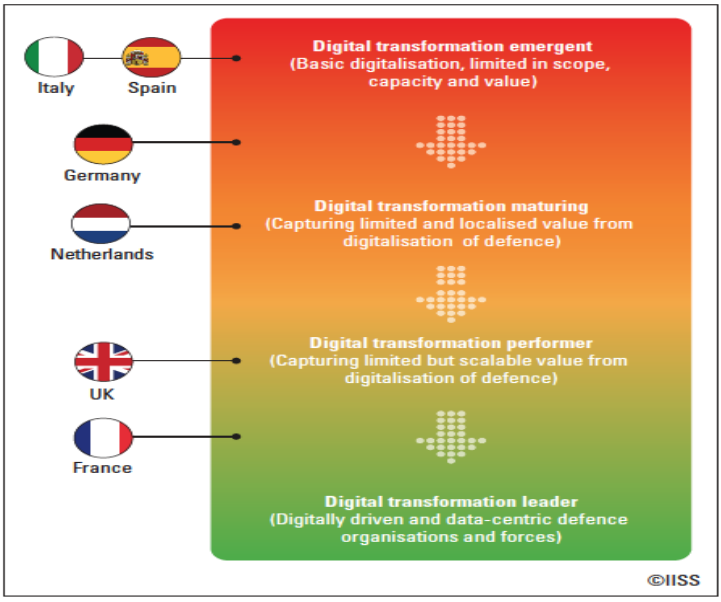


Figura 38. Situación del proceso de digitalización de la defensa en varios países. Fuente: Soare, 2023

Soare (2023) indica que, a pesar de la decisión política, la implementación efectiva se ve limitada por *"los largos plazos temporales exigidos por la adquisición y despliegue de nuevos sistemas de armas, la falta de progreso*

en componentes de procedimiento cruciales (en particular la contratación pública y la alineación presupuestaria), los desafíos en torno a la soberanía y accesibilidad de los datos, y la persistente falta de inversión en capacidades digitales para la defensa en toda Europa".

Todo ello hacía difícil que la OTAN y la UE consiguieran cumplir sus objetivos de transformación digital al final de la presente década. Sin embargo, ante un **recrudecimiento de los conflictos militares convencionales** como demuestra la guerra en Ucrania, y como ha sucedido en la historia en otros grandes conflictos militares, el proceso de digitalización se va a acelerar con la incorporación de **múltiples innovaciones disruptivas** en las operaciones militares de la mano del uso masivo de sistemas autónomos, de algoritmos de inteligencia artificial, de generación sofisticada de noticias falsas, de ciberataques, o del empleo de comunicaciones basadas en constelaciones de satélites de órbita baja por citar algunas de ellas. **Sin el dominio de estas tecnologías en el campo de batalla no será posible obtener la superioridad deseada** y ello acelerará el proceso de innovación.

Como ejemplo, el documento de 2023 publicado por el **Ministerio de Defensa del Reino Unido** considera como objetivo la aceleración de la transformación digital de sus fuerzas armadas y lo eleva al 8,3% del presupuesto de defensa, superior al de Estados Unidos, cuando el estimado para Alemania está entre el 2-2,6% y el de España solo alcanza el 0,4% (véase figura 39).

Table 1: **Estimated annual expenditure of individual allies in NATO and the EU on digital capabilities for defence (2022–23)**

Country	Nominal defence budget (billions, national currency)	Nominal defence budget (billions, USD)	Estimated annual spending on digital capabilities (billions, national currency)	Estimated annual spending on digital capabilities (billions, USD)	Estimated digital capabilities investment as % of defence budget *
France	43.9	46.7	2.6–3.0	2.8–3.2	6.0–6.8
United Kingdom	53.1	64.5	4.4	5.3	8.3
Netherlands	15.8	16.8	0.6–1.0	0.6–1.1	3.6–6.0
Germany	50.1**	53.2	1.0–1.3	1.1–1.4	2.0–2.6
Italy	26.0	27.6	0.2–0.5	0.2–0.5	0.9–1.8
Spain	12.8	13.6	0.0557	0.0592	0.4
United States	816.7	N/A	55.2	N/A	6.8

Note: all figures have been rounded to one decimal place, with the exception of Spain's estimated annual spending on digital capabilities.
* Percentages were calculated using unrounded, national-currency values for nominal defence budgets and estimated annual spending on digital capabilities.
** Core defence budget only, does not include funding reserved for digital capabilities under the off-budget Defence Investment Fund (*Sondervermögen*)
Source: Compiled by author from multiple official sources (national, NATO and EU), 2023

Figura 39. Gasto anual estimado en capacidades digitales para la defensa. Fuente: IISS, 2023

Es interesante señalar que el propio ministerio de Defensa británico en su informe a la Cámara de los Comunes de febrero de 2023 reconozca que **todavía no se ha transformado digitalmente para enfrentarse a los retos de la guerra moderna**. En una de sus conclusiones dice expresamente que "*la tecnología digital está cambiando rápidamente el carácter*

de la guerra, pero que aún no es capaz de explotar las nuevas tecnologías a ritmo y escala. Esto se debe a que no entiende completamente qué datos tiene; Los viejos sistemas "heredados" complican tareas tan rutinarias como pedir un par de botas; sus procesos están configurados para adquirir equipo militar convencional en lugar de software; y carece de todas las habilidades digitales que necesita"[194]

Presento, seguidamente, algunos elementos clave del **proceso de transformación digital en defensa en el contexto de la OTAN y en el de la UE.**

4.3. ACTUACIONES DE LA OTAN

La digitalización acelerada de la defensa está empezando a ganar terreno dentro de la OTAN. En octubre de 2022, los líderes de los Estados miembros respaldaron la visión de la Alianza para la transformación digital y adoptaron una ***Política Marco de Explotación de Datos*** (DEFP) de la OTAN. Posteriormente, en julio de 2023, los miembros de la OTAN adoptaron la ***Estrategia de Implementación de la Transformación Digital***, vinculando los hitos de la transformación digital con los objetivos de desarrollo de capacidades y los requisitos de interoperabilidad.

La figura 40 organiza el objetivo básico de la **Estrategia de Transformación Digital** (en naranja en el centro de la figura) en función de tres pilares básicos: **procesos**, **tecnologías** y **personas**. Sobre ellos se establecen cinco bloques fundamentales: 1) Adopción de nuevas capacidades, 2) Gestión de riesgos y aseguramiento de la misión digital, 3) Agregación de datos, 4) Orquestación de efectos operativos y 5) Mejora de la consciencia situacional mediante entornos sintéticos.

194 https://publications.parliament.uk/pa/cm5803/cmselect/cmpubacc/727/report.html

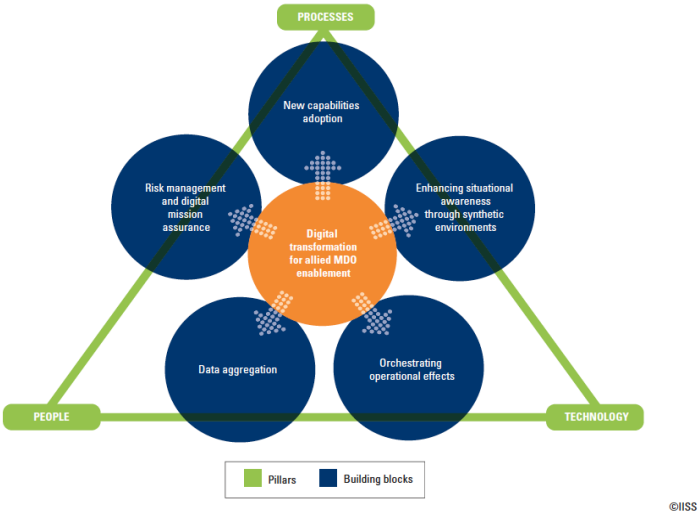


Figura 40. Pilares y elementos de la transformación digital de la OTAN. Fuente: Soare, 2023

El compromiso de llevar a cabo esta transformación digital se ha reforzado en la última **cumbre de la OTAN** mantenida en Vilnius durante el mes de julio de 2023. En el **comunicado final** (NATO, 2023), se presta atención a la digitalización desde una implicación mayor de la industria de defensa, la implementación de la Estrategia de Implementación de la Transformación Digital, y una mayor preocupación sobre la ciberseguridad. Concretamente:

- El **párrafo 30 del comunicado** indica (subrayado propio) que *"la Alianza requiere una **industria de defensa fuerte y capaz**, con cadenas de suministro resistentes. Una industria de defensa fuerte en toda la Alianza, incluida una industria de defensa más fuerte en Europa y una mayor cooperación industrial de defensa dentro de Europa y a través del Atlántico, sigue siendo esencial para ofrecer las capacidades requeridas".*
- Explícitamente, en relación con la transformación digital, el párrafo 60 del comunicado final expresa (subrayado propio) que: "*La capacidad de la Alianza para cumplir sus tareas principales depende cada vez más de la **adopción de tecnologías digitales**. Reconociendo la urgencia de una Alianza transformada digitalmente, hemos respaldado una **Estrategia de Implementación de Transformación Digital** para respaldar nuestra capacidad de llevar a cabo Operaciones Multidominio, impulsar la interoperabilidad en todos los dominios, mejorar la conciencia situacional, la consulta política y emplear la toma de decisiones basada en datos".*

- Finalmente, se reconoce la relevancia alcanzada por el riesgo de **ciberseguridad** y, extraído del párrafo 66 (subrayados propios), se puede leer: "*Respaldamos un nuevo concepto para mejorar la contribución de la defensa cibernética a nuestra disuasión general y postura de defensa. Integrará aún más los* ***tres niveles de ciberdefensa de la OTAN*** *(político, militar y técnico), asegurando la cooperación civil-militar en todo momento en tiempos de paz, crisis y conflicto, así como el compromiso con el sector privado, según corresponda… Hemos lanzado la nueva* ***Capacidad Virtual de Apoyo a Incidentes Cibernéticos*** *(VCISC) de la OTAN para apoyar los esfuerzos nacionales de mitigación en respuesta a importantes actividades cibernéticas maliciosas".*

Dada la **importancia creciente de mejorar la situación de seguridad en Europa**, y la necesidad de optimizar los recursos disponibles cuando muchos estados miembros de la UE son miembros de la OTAN (más aún con la incorporación de Finlandia y Suecia[195] en 2023) el párrafo 73 del comunicado (subrayados propios) expresa la relevancia de la relación entre ambas organizaciones:

"La ***Unión Europea sigue siendo un socio único y esencial para la OTAN****. Nuestra asociación estratégica es esencial para la seguridad y la prosperidad de nuestras naciones y de la zona euroatlántica. Se basa en nuestros valores compartidos, nuestra determinación de hacer frente a los desafíos comunes y nuestro compromiso inequívoco de promover y salvaguardar la paz, la libertad y la prosperidad. La OTAN reconoce el valor de una* ***defensa europea más fuerte y capaz*** *que contribuya positivamente a la seguridad transatlántica y global y* ***que sea complementaria e interoperable con la OTAN****. El desarrollo de capacidades de defensa coherentes, complementarias e interoperables,* ***evitando duplicaciones innecesarias****, es clave en nuestros esfuerzos conjuntos para hacer que la zona euroatlántica sea más segura."*

En el ámbito nacional, el conflicto con Rusia ha acelerado el proceso de digitalización en defensa. Como ejemplo, un país europeo clave de la OTAN, el Reino Unido, aunque no perteneciente a la UE, ha extraído las lecciones de la invasión de Ucrania en el ámbito digital (UK, 2023): "*Aprovecharemos las oportunidades de cambio de juego que ofrecen los avances digitales de los últimos años para mantener una ventaja decisiva contra nuestros adversarios".*

En este contexto de **complementariedad** e **interoperabilidad**, el proceso de digitalización de la defensa en la UE es un elemento esencial cuyas líneas maestras políticas y presupuestarias se presentan en la siguiente subsección.

195 Suecia se encuentra en proceso de ratificación por los estados miembros de la OTAN, habiéndose sorteado el veto inicial de Turquía.

4.4. ACTUACIONES DE LA UE

4.4.1. Programas de la UE de interés para la defensa

Como se ha indicado en el conjunto de la presente monografía, el proceso de digitalización ha sido un objetivo político prioritario de la UE. A ello se han dedicado esfuerzos en el ámbito tecnológico con crecientes presupuestos en los programas marco de investigación e innovación (actualmente *Horizon Europe* 2021-2027), el programa *Digital Europe*, la relevancia que han adquirido las infraestructuras digitales, la adopción de servicios innovadores y la obtención de habilidades digitales en la política de cohesión o en los fondos de recuperación y resiliencia. Todo ello, acompañado del esfuerzo legislativo y regulatorio que se ha presentado en otras secciones de la monografía.

Era lógico que en la acción intergubernamental de la UE en el que se inserta el esfuerzo en defensa y seguridad también se hayan puesto en marcha **actuaciones concretas de interés para la defensa** teniendo en cuenta que muchas de las tecnologías en desarrollo (p.ej. en el pilar II de *Horizon Europe*) o las infraestructuras digitales desplegadas (p.ej. *Galileo, Copérnico* o *5G*) tienen o pueden tener un carácter dual.

Es destacable que el ***Comité Militar de la UE (EUMC)*** ha estado desarrollando una agenda para la digitalización de la defensa desde 2019[196]. La Comisión Europea (CE), el EUMC y la **Agencia Europea de Defensa** (AED) están trabajando activamente en diferentes aspectos de la digitalización de la defensa europea, ya sea a través del **Fondo Europeo de Defensa (FED)** u otros instrumentos a nivel de la UE. Este proceso culminó con la aprobación del ***Plan Estratégico de Implementación para la Digitalización de las Fuerzas de la UE*** en 2021, que proporcionó un análisis de las brechas existentes y estableció un nivel de ambición y objetivos e hitos específicos para la digitalización e interoperabilidad de las fuerzas armadas europeas.

Desde el punto de vista político, la aprobación de la ***"Brújula estratégica"*** de la UE ha sido esencial al hacer hincapié en la modernización y la inversión en tecnologías digitales y nuevas como uno de los cuatro pilares prioritarios para la acción en la defensa europea. Por lo tanto, un desafío importante para las transformaciones digitales en la OTAN y la UE será alinear las iniciativas nacionales y garantizar la compatibilidad de los datos, y la interoperabilidad digital, por defecto entre los Estados miembros y dentro de sus propias empresas organizativas (IISS, 2022).

196 En 2019, un documento de reflexión sobre «Digitalización e inteligencia artificial en defensa», publicado conjuntamente por Finlandia, Estonia, Francia, Alemania y los Países Bajos, hizo hincapié en la importancia de la digitalización de la defensa en toda Europa como precursora de la modernización a través de la adopción de la IA.

4.4.2. Reflexión sobre la autonomía estratégica y la soberanía tecnológica digital europea en el ámbito de la defensa

El estallido en febrero de 2022 de un conflicto militar en las fronteras de la UE ha producido un **claro incremento de los presupuestos de defensa** y un reforzamiento de los compromisos de inversiones ya adquiridos previamente por diversos países**.** Aunque la experiencia de los últimos años indica que **será difícil cumplir con los objetivos de inversión** en las fechas previstas por todos los estados miembros, tanto los comprometidos con la OTAN (superar el 2% del PIB en gastos de defensa) como los establecidos por los gobiernos a nivel nacional, la UE tiene una **oportunidad real de mejorar su autonomía estratégica y la soberanía tecnológica** en un conjunto de tecnologías y sistemas duales. Pero no tiene por qué ser así, ni está claro que lo desee por las connotaciones geopolíticas que implica.

Debe distinguirse en el ámbito de la defensa el objetivo de **mejora de la autonomía estratégica**, entendida como la capacidad de tomar decisiones que afecten a la defensa europea sin necesidad de depender de otros países, del objetivo de **soberanía tecnológica**, con la que se pretende no depender de tecnologías procedentes de otros países en el desarrollo de sistemas de armas que se consideren claves para la UE.

La valoración de la **autonomía estratégica** implica analizar un triple condicionamiento para hacerla realidad: **querer** ejercerla, **poder** ejercerla, y **saber** ejercerla. Analizo seguidamente mi visión personal sobre cada una de estas condiciones.

El primero de ellos, ***"querer"***, implica la existencia de una voluntad política conjunta en el ámbito de la UE sostenida en el tiempo para obtener la autonomía estratégica en defensa sin condicionamientos excesivos de terceros países que permita tomar decisiones. La UE ha decidido dar pasos en esa dirección, pero de forma cautelosa, siguiendo la estela de la *"Brújula Estratégica"*. Un proceso rápido en esta dirección chocaría con una visión de intereses nacionales contrapuestos, y se encontraría con la dificultad de asumir los riesgos de intervención colectiva en otros países o regiones como demuestra el caso del Sahel. Veo difícil a corto plazo avanzar de forma conjunta por parte de la UE en otras partes del mundo como ha sucedido en el caso de Ucrania en el que el papel de la OTAN ha sido decisivo.

En el **ámbito digital** la dimensión de ***"querer"*** en el contexto de la UE ha estado ligado al acuerdo político conjunto para la **puesta en marcha de programas espaciales ambiciosos para el desarrollo de sistemas digitales duales dotados de servicios** en el ámbito de la defensa y seguridad como son:

- la señal protegida del sistema de navegación **Galileo** denominado *"Servicio Público Regulado (PRS)"*[197], restringido a las Fuerzas Armadas, policía, Guardia Civil, bomberos, sistemas de emergencia y usuarios autorizados,
- la **constelación de nanosatélites** para acceso a Internet denominada "*Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²)"*[198] cuyo Reglamento fue aprobado en marzo de 2023 (European Union, 2023) cuya capacidad operativa total se alcanzará en 2027 con servicios restringidos a usuarios gubernamentales dotados de una infraestructura gubernamental que requieran un alto nivel de seguridad sin depender de operadores civiles[199].
- la creación de un **Centro de Coordinación de la Ciberdefensa de la UE (EUCDCC)** propuesto en noviembre de 2022 como parte de la política de UE en ciberdefensa, que apoye una mayor conciencia situacional dentro de la comunidad de defensa, incluidos todos los comandantes militares de la PCSD de la UE basándose en el proyecto del *Centro de Coordinación del Ciberespacio y del Dominio de la Información* (CIDCC). Su objetivo será proporcionar un análisis holístico del ciberespacio, el entorno electromagnético y el dominio cognitivo al reunir diferentes fuentes de información a los niveles estratégicos y operativos militares[200].

En referencia a ***"poder"***, la UE es consciente de su debilidad en el ámbito de la defensa. Ha asumido la dependencia en la práctica de la OTAN, con una presencia reforzada en la frontera este de Europa tras el desencadenamiento de la guerra en Ucrania, para poder ejercer su acción en el territorio cubierto por la Alianza. Fuera de este ámbito geográfico, no es evidente que la UE pueda ejercerlo sin recursos propios. Un cambio sustancial requeriría modificar el Tratado de Funcionamiento de la Unión, y nos retrotrae al *"querer"* indicado anteriormente reforzando las capacidades que ya tiene el Alto Representante de la Unión.

Finalmente ***"saber"*** implicaría no solo reforzar las capacidades operativas conjuntas de mando y control, la integración de unidades operativas de diferentes estados miembros, el despliegue rápido de unidades de varios países donde sea necesario, asegurar la movilidad en el transporte

197 Con el servicio PRS se pretende proporcionar una señal cifrada con una protección mayor, y con requisitos de operatividad en todo momento que haga más difícil y costoso un ciberataque a la señal, tanto con señales falsas que suplanten la señal de Galileo como por defenderse de interferencias. https://www.inta.es/CPA/es/que-es-el-prs/

198 https://defence-industry-space.ec.europa.eu/eu-space-policy/iris2_en

199 El caso del papel jugado por Startlink en Ucrania fue una clara señal a la UE para acelerar la disponibilidad de un sistema propio para defensa y seguridad.

200 https://www.eeas.europa.eu/eeas/joint-communication-european-parliament-and-council-eu-policy-cyber-defence_en

europeo, disponer efectivamente del servicio PRS de Galileo o la efectiva operación de IRIS², etc., sino también de acuerdos a largo plazo para una **profunda integración de la industria europea de defensa** que permita disponer de sistemas avanzados con una masa crítica suficiente en tiempos razonables por encima de los intereses nacionales.

En relación con la **soberanía tecnológica** es cierto que, en los últimos años, se han puesto en marcha algunos proyectos para el desarrollo de capacidades financiados por el **Fondo Europeo de Defensa (FED)**[201] (tanto en investigación como en desarrollo de sistemas) que siguen procesos tradicionales de desarrollo de prototipos con plazos de entrega dilatados hasta la próxima década. Aún más, el uso para defensa de muchos de los resultados generados en los proyectos financiados por los programas marco de investigación e innovación de la UE requiere un largo proceso de adaptación.

Hasta 2023 el FED había asignado en las dos primeras convocatorias unos 2.000 millones de euros en 101 proyectos con la distribución temática que se indica en la figura 41 (Fiott, 2023). El peso de la I+D digital es muy elevado en todas las áreas.

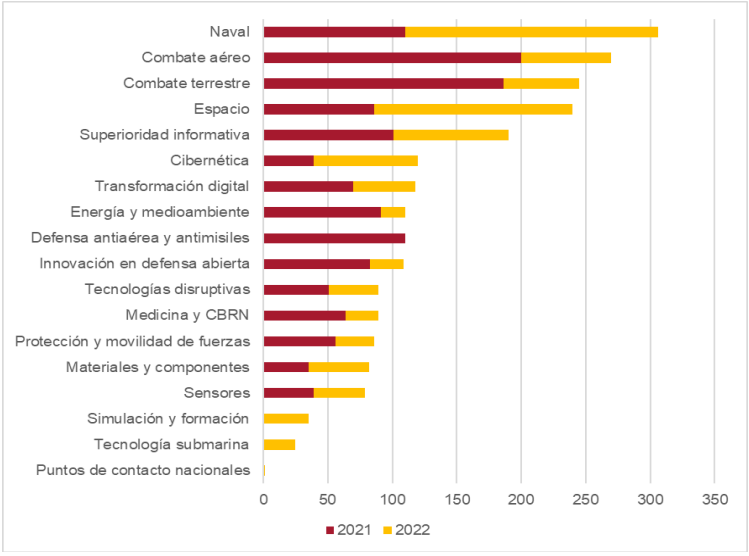


Figura 41. Distribución de los recursos del Fondo Europeo de Defensa. Fuente: Fiott, 2023

A pesar de los esfuerzos realizados en EDF y en otros programas na-

201 https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en

cionales similares, los resultados de estos proyectos de I+D, incluso en el caso de que tuvieran éxito, se dilatarán en el tiempo para que puedan incorporarse en esta década en sistemas de armas. A ello se suma que existe una **simultaneidad en el uso de sistemas de armas de diferentes generaciones de tecnología** (en muchos casos coexisten equipos que tienen más de cuarenta años de distancia en su proceso de diseño) lo que puede dificultar su interoperabilidad.

Puede parecer chocante, pero las tecnologías digitales se introducen más lentamente en el campo militar que en el campo civil al tener que asegurar esa interoperabilidad, y cuando proceden de desarrollos civiles, tener que adaptarse a entornos de operación mucho más exigentes.

La consecuencia es que, dada la obsolescencia de sus sistemas actuales, **muchos países europeos deben tomar decisiones de adquisición de sistemas de armas disponibles actualmente proporcionados por otros países**, sobre todo de Estados Unidos, antes de que otros equivalentes europeos estén disponibles. La consecuencia de disponer de mayores presupuestos ha sido la aceleración de la adquisición de aviones, misiles, sistemas de defensa aérea, drones, helicópteros, múltiples tipos de munición, etc. Debe tenerse en cuenta que todos ellos incorporan **subsistemas digitales avanzados**, y dependen de redes digitales avanzadas para su funcionamiento.

El ejemplo de la **aviación de combate** ejemplifica la situación estratégica de la UE. El **futuro sistema de combate aéreo europeo (ECFAS)** de 6ª generación que Francia, Alemania y España han decidido iniciar no estará operativo hasta comienzos de la década de 2040, si todo fuera bien. Esta fecha tan lejana impide a muchos estados miembros de la UE poder esperar hasta entonces para renovar sus plataformas aéreas.

Tampoco se puede considerar el **ECFAS** como "*el avión de combate europeo*" en el que la UE apuesta, puesto que su desarrollo no incluye a todos los estados miembros, no se financia con presupuestos comunitarios, y compite con otros aviones desarrollados en Europa como el *Gripen* de Suecia. Nada obliga, además, a otros países distintos a los tres firmantes a adquirirlo como ya ha sucedido previamente con el *Eurofighter* o el *A-400M* de transporte, salvo acuerdos industriales en el proceso de diseño y fabricación que, en todo caso, dependen de las empresas integradoras de los sistemas.

En resumen, diversos estados miembros deberán adquirir sistemas avanzados ahora, adquiriendo aviones de 5ª generación como el **F-35** de

Estados Unidos[202], y desplegarlos en la década de 2030[203]. Esto implica también condicionamientos en los sistemas de armas implicados, en la aviónica embarcada, en los sistemas de comunicaciones, en la nube de combate, etc. y el mantenimiento y mejoras durante muchos años de vida operativa. Europa dependerá más de Estados Unidos al final de la década de 2030 que en la actualidad.

Los procesos de negociación para la adquisición de sistemas pueden implicar la firma de acuerdos industriales con los países compradores en la provisión de determinados subsistemas, pero la experiencia demuestra que **en sistemas avanzados como el F-35 la transferencia de tecnología es muy limitada**. En mi opinión, la UE no va a mejorar su soberanía tecnológica por estas adquisiciones, aunque sí lo haga su autonomía estratégica en el supuesto de que el uso de los sistemas adquiridos no esté muy condicionado en las cláusulas de adquisición.

Este análisis se puede trasladar de forma similar a otros sistemas de defensa diferentes al aéreo en varios dominios (p.ej. sistemas de defensa de misiles en los que la disponibilidad del sistema *Patriot* es relevante en muchos países europeos[204]) que, además, deben asegurar su interoperabilidad con sistemas ya empleados por la OTAN.

Finalmente, reproduzco las tendencias en el proceso de **transformación al campo de batalla inteligente** procedente de Pérez-Martínez (2023a, 2023b). La combinación de todas ellas supone un cambio disruptivo durante la presente década.

- ***Sensorización y "datificación"****: Estamos "datificando" la realidad y no solo con sensores electromagnéticos y electroópticos cada vez más eficaces, en términos de alcance, precisión y capacidad de identificación y de menor coste. 7.000 millones de teléfonos inteligentes, 5.000 millones de usuarios de internet, despliegue del IoT que permitirá configurar centenares de miles de redes con millones de millones de conexiones fiables y seguras.*

202 Entre sus sensores digitales muy avanzados destacan el radar "Active Electronically Scanned Arrays" (AESA), el Sistema de Apertura Distribuida (DAS), el Sistema de Apuntamiento electroóptico (EOTS) y el Sistema de visión integrado en el casco.

203 Esta decisión ya ha sido adoptada por algunos como Alemania, Finlandia, Suiza, Rumanía y República Checa, aunque su entrega durará años. Esto supone, alrededor de 600 aviones. Y otros países que ya poseen F-35 como Bélgica, Italia, Países Bajos, Noruega, Polonia y Reino Unido están pensando en incrementar su número.

204 Existen proyectos europeos lanzado por Francia y Alemania, pero los plazos de disponibilidad son excesivos. Alemania prefiere comprar equipamiento militar disponible, aunque no sea de producción europea. La iniciativa alemana "European Sky Shield" consiste en coordinar la logística y compra de capacidades de defensa antiaérea con misiles Iris T de fabricación alemana junto a los Patriot estadounidenses y al sistema de defensa israelí Arrow 3, lo que ha generado tensiones con Francia que posee los denominados Mamba (SAP/T) desarrollados juntamente con Italia. https://www.elconfidencial.com/mundo/europa/2023-07-27/choque-misiles-francia-alemania-defensa-europea_3704631/

- ***Conectividad e hiperconectividad****: La información se modificará mientras recorre las redes para adaptarla a las necesidades del combatiente. Las redes serán inteligentes y jugarán un papel esencial en la consecución de la superioridad de la información La tecnología 5G y 6G se impondrá, habrá un estándar 5G/ 6G militar que se desplegará en los campos de operaciones junto a otras redes redundantes de menores prestaciones.*
- ***Inteligencia, automatización y autonomía****: Se pasará de la IA estrecha (la IA supera al humano en tareas específicas trabajando con un conjunto de datos grande pero limitado) a la IA general (varias tareas simultáneas con un conjunto ilimitado de datos).*
- ***Procesado distribuido y procesado cognitivo****: Se pasará de un procesado que permite optimizar la interpretación de los datos por los usuarios (los actuales procesados en la nube, en el borde, en la niebla…) a un procesado que interpreta los datos y toma decisiones.*
- ***Agilidad e inmediatez****. Pasaremos de respuestas rápidas a respuestas en tiempo real. El futuro desarrollo de los sistemas hipersónicos y las armas de energía dirigida implicarán una radical disminución en los tiempos de respuesta, acelerando los combates hasta límites en los que el operador humano puede ser superado en su capacidad de reacción. La solución es sacarlo del combate o, en el mejor de los casos, convertirlo en mero supervisor*

En conjunto, el panorama expuesto describe una situación en la que **la UE tendrá que alinear sus esfuerzos para incrementar su capacidad con tecnologías avanzadas propias incrementando sustancialmente en los próximos años los recursos disponibles para defensa y seguridad** y ligarlo todo con una política ambiciosa de la industria de defensa europea. Todo ello, con un reforzamiento de la política exterior común que debe conducir a un replanteamiento del Tratado de la UE.

5

OPCIONES DE LA UE PARA MEJORAR SU AUTONOMÍA ESTRATÉGICA DIGITAL ABIERTA

5.1. OPCIONES PARA LA UE

Las páginas anteriores de la presente monografía han expuesto una situación en la que la UE presenta un conjunto de **debilidades para reafirmar su autonomía estratégica digital abierta** que, en caso de prolongarse, puede conducir a una situación irreversible de **pérdida de relevancia** frente a otras potencias.

En mi opinión, para contrarrestar las debilidades existentes, la UE debe actuar muy rápidamente con decisión política, asignando recursos suficientes para ello en tecnologías clave, con una regulación inteligente, y asegurando el alineamiento entre las instituciones comunitarias y los estados miembros para mantener una postura común en política exterior, y poder así revertir la situación.

Algunas de estas actuaciones obligarán a conceder un peso mayor a las instituciones comunitarias en sus relaciones con terceros países. Por eso, **sería necesario reforzar las posiciones geopolíticas de la UE** mediante un reequilibrio competencial entre la UE y los estados miembros lo que puede llevar a largo plazo a cambios en el Tratado de la UE. Soy consciente de la dificultad que eso implica e, incluso en el caso de éxito, los plazos dilatados que supondría por lo que será necesario buscar actuaciones más factibles a corto y medio plazo.

Cuenta a favor de la UE la existencia de una **base científica y tecnológica en el ámbito digital muy potente**, con un **despliegue de tecnologías digitales avanzadas** que abarca la mayor parte del territorio y la población europea, con sistemas digitales desarrollados en la UE en los que posee una excelente proyección internacional (como son los sistemas de navegación satelital) y con **una experiencia en el proceso regulatorio digital** que la convierte en una potencia reguladora mundial. El anexo proporciona una visión actualizada en diciembre de 2023 del esfuerzo regulatorio realizado (no completado todavía).

A ello se añade una visión política aceptada por todas las instituciones comunitarias y estados miembros de la UE de **actuar en beneficio del usuario protegiendo sus datos y proporcionándole la mayor confianza en el uso de la tecnología**, limitando en lo posible sus efectos perniciosos, a través de una regulación digital avanzada. En contra de la UE juega la existencia de un **tejido industrial relativamente débil** con pocas grandes empresas con impacto sistémico generador de nuevas tecnologías digitales en el que el peso de las grandes empresas europeas del sector es limitado para imponer sus productos y criterios de mercado[205].

Es verdad que, en la última década, se ha producido un cambio positivo con la **multiplicación de nuevas empresas de base tecnológica creadas en Europa** capaces de ofrecer productos y servicios digitales disruptivos. Sin embargo, aún tienen dificultades para escalar en la UE y tienen más fácil su crecimiento en Estados Unidos. Todo ello ocurre a pesar del esfuerzo de la UE en retenerlas con la puesta en marcha del **Consejo Europeo de Innovación** ("*European Innovation Council, EIC*)[206]" con una especial dedicación a empresas digitales, la creación ya hace años de **EIT Digital**[207], la comunidad de innovación y conocimiento (KIC) digital del *Instituto Europeo de Innovación y Tecnología (EIT)* focalizada en emprendimiento digital, y de la puesta en marcha de multitud de programas e incubadoras de empresas a nivel nacional o regional focalizadas en empresas disruptivas digitales.

A ello se une como **debilidades estructurales** una dependencia en materiales especiales (p.ej. materias primas como litio y tierras raras), componentes y productos digitales, en gran parte procedentes de Asia (China, Taiwán, Corea, Japón), capacidades muy limitadas de fabricación de circuitos integrados avanzados[208], así como la dependencia de grandes plataformas digitales no europeas en el acceso a servicios digitales avanzados. Esta situación se complica aún más por la existencia de un **déficit persistente de especialistas** en tecnologías digitales que obligará a reaccionar para atraer y retener el talento digital en Europa en un contexto de necesidades compartidas por otros países[209].

Un último problema es el relativo a **la dificultad en establecer una**

205 Sí es verdad que, a cambio, la UE posee empresas fuertemente digitalizadas en sectores industriales de alta tecnología como el aeroespacial, el químico, el de defensa o el de servicios financieros que juegan un papel relevante en el posicionamiento global de Europa. Sobre ellas será más sencillo articular una autonomía estratégica digital.

206 https://eic.ec.europa.eu

207 https://www.eitdigital.eu

208 Las fábricas de semiconductores (foundries) anunciadas por Intel y TSMC que se construirán en Alemania no estarán operativas hasta 2025-2026, si encuentran el personal que necesitan.

209 Sobre todo, por Estados Unidos que prevé que en 2030 el sector de la microelectrónica de Estados Unidos tenga un déficit de 67.000 técnicos, informáticos e ingenieros, y alrededor de 1,4 millones de esos trabajadores en toda la economía en general (Lafayette, 2023). Estas necesidades pueden hacer más difícil para la UE retener el personal especializado necesario en los estados miembros.

visión única en la Unión ante un marco competencial fragmentado y los diferentes intereses de los 27 estados miembros. Esta situación es especialmente delicada en los casos en los que se requiere llevar a cabo complejas negociaciones a nivel internacional con intereses contrapuestos entre los países mediatizados por la situación en sus políticas nacionales. Una opinión del *Atlantic Council* en 2022, desde la perspectiva de Estados Unidos, lo indica claramente:

"*La UE ciertamente tiene derecho a regular su economía nacional, incluida su economía digital. Pero en un momento en que las democracias occidentales y sus economías de mercado están cada vez más amenazadas, aquellos que buscan abordar los excesos de la economía digital desde una perspectiva democrática y basada en reglas deberían actuar juntos, no establecer reglas que dificulten la cooperación".*

Desde la visión de la UE, Estados Unidos actúa también unilateralmente como ha demostrado a Europa la aprobación en agosto de 2022 de la *Ley de Reducción de la Inflación (IRA)*[210] por Estados Unidos con el objetivo declarado de que Estados Unidos siga siendo el líder mundial en tecnología, fabricación e innovación de energía limpia. La **asignación de 370.000 millones de dólares de inversiones en la IRA** pretende: reducir los costos de energía para las familias y las pequeñas empresas, acelerar la inversión privada en soluciones de energía limpia en todos los sectores de la economía y en todos los rincones del país, fortalecer las cadenas de suministro, desde minerales críticos hasta electrodomésticos eficientes, y crear empleos bien remunerados y nuevas oportunidades económicas para los trabajadores.

Debe recordarse que la Ley CHIPS y Ciencia de agosto de 2022 tiene como objetivo fortalecer la fabricación estadounidense, las cadenas de suministro y la seguridad nacional, e invertir en investigación y desarrollo, ciencia y tecnología, y la fuerza laboral del futuro para mantener a los Estados Unidos como líder en las industrias del mañana, incluida la nanotecnología, la energía limpia, la computación cuántica y la inteligencia artificial.

El problema para la UE es que **acceder a un nivel de subvenciones como el indicado obliga a empresas europeas a trasladar su fabricación a Estados Unidos** lo que dificultará el objetivo de reindustrialización europea.

210 https://www.whitehouse.gov/wp-content/uploads/2022/12/Inflation-Reduction-Act-Guidebook.pdf

La crítica europea[211] procede de que se ha desarrollado sin una verdadera negociación con la UE a lo que Estados Unidos dice que tampoco la UE había acordado con Estados Unidos los fondos de recuperación de COVID. Es un ejemplo de la dificultad de alinear actuaciones entre supuestos socios cuando los intereses nacionales están en juego.

La reunión del **TTC** (*US-EU Trade and Technology Council*)[212] entre la UE y Estados Unidos celebrada el 5 de diciembre de 2022, más allá de la corrección del texto de la Declaración[213] indica preocupaciones conjuntas. Los temas identificados son: la seguridad de las comunicaciones de datos, la diversificación de proveedores y rutas en las cadenas de provisión, y la discusión sobre las *"tendencias del mercado hacia enfoques abiertos e interoperables, junto con arquitecturas confiables y establecidas, de una manera tecnológicamente neutra.*

Uno de los resultados positivos del TTC ha sido el de liderar conjuntamente la **formulación de los nuevos estándares técnicos en IA y tecnologías emergentes** para promover *"seguridad, equidad, no discriminación, interoperabilidad, innovación, transparencia, mercados diversos, compatibilidad e inclusión"*. Veremos cómo todo eso se concreta en regulaciones apropiadas y compatibles a ambos lados del Atlántico, pero, al menos, el marco de discusión está bien establecido. En mi opinión, anuncia un periodo en el que las **divergencias en la regulación digital entre Estados Unidos y la UE** y las consecuencias en el flujo de inversiones tecnológicas derivadas de ellas seguirán siendo notables.

No le basta a la UE con mirar exclusivamente a Estados Unidos; **India es también un actor muy relevante para la UE** como demuestran los siguientes datos. La UE es el segundo mayor socio comercial de la India, con un valor de 120.000 millones de euros en el comercio de mercancías en 2022, o el 10,8 % del comercio total de la India. La India es el 10º mayor socio comercial de la UE, representando el 2 % del comercio total de mercancías de la UE. El comercio de servicios entre la UE y la India alcanzó los 40.000 millones EUR en 2021. **Desde un punto de vista geopolítico, India se ha convertido en un actor muy relevante en el denominado**

211 Tras la aprobación del IRA, la UE, para contrarrestar sus efectos negativos sobre la industria europea decidió conceder un apoyo adicional basado en la relajación de las ayudas de Estado, aprovechando el Marco de Crisis Temporal creado en marzo de 2022 como respuesta de la invasión rusa de Ucrania; en marzo de 2023, se ha transformado en el "Temporary Crisis and Transition Framework (TCTF)", que, de facto, es la respuesta europea al IRA.
https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/740087/IPOL_IDA(2023)740087_EN.pdf

212 El propósito del TTC es mejorar el comercio y la inversión, fortalecer el liderazgo tecnológico e industrial, impulsar la innovación, promover tecnologías e infraestructura emergentes y alentar estándares y regulaciones compatibles basados en valores democráticos compartidos. https://digital-strategy.ec.europa.eu/en/policies/trade-and-technology-council

213 https://ec.europa.eu/commission/presscorner/detail/en/statement_22_7516

"Sur Global" y en el movimiento de los países denominados BRICS[214] y su prevista expansión a once miembros[215] como contrapunto al G7[216].

La puesta en marcha de un enfoque de coordinación similar a Estados Unidos se ha puesto en marcha recientemente con la **India** mediante la creación del ***EU-India Trade and Technology Council***. La primera reunión mantenida el 16 de mayo de 2023[217] reafirmó la visión compartida de que *"Los retos geoestratégicos han reforzado el interés común de la UE y la India por garantizar la seguridad, la prosperidad y el desarrollo sostenible basado en valores compartidos"*[218].

Ambos países también se comprometieron a buscar la cooperación en **inteligencia artificial confiable** (con una coordinación bilateral en el marco de la *Asociación Mundial sobre Inteligencia Artificial (GPAI)* y explorar la cooperación bilateral en inteligencia artificial fiable y responsable), y en el sector estratégico de **semiconductores** a través de un *Acuerdo de Entendimiento* específico previsto para septiembre de 2023 (EU-India, 2023).

Esta **cooperación estratégica de la UE en el ámbito digital con países con visiones similares** se ha reforzado con la puesta en marcha de **partenariados con tres países asiáticos** relevantes en tecnologías digitales como son *Japón* y *Corea del Sur* en 2022, y *Singapur* en 2023. Las áreas prioritarias acordadas difieren en cada uno, aunque hay muchas coincidencias[219].

¿Sería posible para la UE actuar de forma similar en otras regiones del mundo consideradas clave para ella? Uno de estos casos posibles y rele-

214 El término BRIC deriva del movimiento de países no alineados nacido en Bandung (Indonesia) en 1955 para permanecer al margen de los dos grandes bloques rivales de entonces: el estadounidense y el soviético. El acrónimo BRIC surge en 2001 acuñado por Jim O'Neil, director de Economía Global de Goldman Sachs, para estructurar el enorme potencial de crecimiento de Brasil, Rusia, India y China como mercados emergentes. La adhesión de Sudáfrica data de 2011. https://www.almendron.com/tribuna/apilando-paises-brics/

215 Se pretende ampliar tras la cumbre mantenida en Sudáfrica en agosto de 2023 con la incorporación de Arabia Saudí, Emiratos Árabes Unidos, Irán, Egipto, Etiopía y Argentina; finalmente, Indonesia no ha sido invitada. Con ellos, el grupo representaría el 46 % de la población del planeta y más de un tercio del PIB mundial. La implementación efectiva de este proceso tardará por la necesidad de crear un modus operandi consensuado y vencer resistencias internas que pueden difuminar el peso geopolítico de algunos de los actuales miembros de BRICS.

216 El G7 incluye al Reino Unido, Canadá, Francia, Alemania, Italia, Japón, y Estados Unido, junto a la participación en las reuniones de los presidentes de la Comisión Europea y del Consejo Europeo.

217 https://digital-strategy.ec.europa.eu/en/library/eu-india-ttc-joint-statement

218 El primer grupo de trabajo creado se centrará en Tecnologías Estratégicas, Gobernanza Digital y Conectividad Digital. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2728

219 Como ejemplo, en el caso de Japón las prioridades se refieren a: seguridad en 5G, tecnologías más allá de 5G/6G, aplicaciones éticas y seguras de la IA, y la resiliencia de las cadenas globales de suministros de la industria de semiconductores; en el de Corea del Sur estas prioridades incluye semiconductores, la siguiente generación de redes móviles, tecnologías cuánticas y de computación de altas prestaciones, ciberseguridad, inteligencia artificial, y plataformas, datos y habilidades digitales. Finalmente, las prioridades con Singapur fueron: semiconductores, flujo de datos confiables, confianza digital, estándares, facilitar el comercio digital, habilidades digitales para trabajadores, y la transformación digital de empresas y servicios públicos. https://digital-strategy.ec.europa.eu/en/policies/partnerships

vantes sería la creación de un **TTC específico para Latinoamérica** como foro estratégico bilateral de alto nivel que ha sido propuesto informalmente (Arteaga et al., 2023) aprovechando el semestre de presidencia española del Consejo de la Unión en vez de la celebración de cumbres periódicas. No será fácil tras los, en mi opinión, escasos compromisos concretos alcanzados en la *Cumbre UE-CELAC* celebrada en Bruselas en julio de 2023 (Consejo Europeo, 2023)[220].

5.2. RECOMENDACIONES PARA LA AUTONOMÍA DIGITAL DE LA UE

En vista de la situación descrita, y asumiendo que no hay una "solución mágica" a corto plazo a ninguno de los problemas abordados en el presente informe, presento seguidamente un **conjunto de recomendaciones para que la UE pueda mejorar su autonomía estratégica digital abierta** durante la presente década fomentando una **interdependencia inteligente** con países aliados.

R1. Acelerar el despliegue en todo el territorio europeo de tecnologías digitales innovadoras modificando, en su caso, las prioridades de la política de cohesión europea y los recursos de Next Generation.

Se trata de una recomendación genérica que debe estar acompañada de compromisos concretos de cada estado miembro ligados a la **asignación de recursos nacionales y comunitarios** (p.ej. en los fondos de la política de cohesión comunitaria o en los de *Next Generation*) **para el despliegue de comunicaciones avanzadas** móviles, fijas y satelitales, y de nuevos servicios ligados a la digitalización de los sectores públicos y privados en línea con los objetivos del Decenio Digital Europeo. Adicionalmente, la UE debe acelerar el desarrollo de infraestructuras paneuropeas basados en una constelación propia de nanosatélites y el despliegue de redes cuánticas seguras.

Asegurar el acceso en banda ancha a internet tanto en comunicaciones fijas como móviles y satelitales no es una opción, es una necesidad que debe completarse en el menor tiempo posible para todos los ciudadanos europeos siendo conscientes de que la propia evolución tecnológica hará necesario **continuar y repetir este proceso de despliegue de comunicaciones avanzadas en el futuro** con objeto de mantener la competitividad frente a otras regiones.

220 En la Declaración Final de la Cumbre (apartado 29) se lee en referencia al ámbito digital: "Destacamos la importancia de cooperar para promover un modelo responsable de transformación digital centrado en el ser humano, basado en valores e inclusivo, que proteja la privacidad como derecho fundamental, aumente la conectividad digital y la ciberseguridad, tenga por objeto colmar las brechas digitales, fomente un desarrollo y un uso fiables de la inteligencia artificial y contribuya a generar confianza en la economía digital. Acogemos con satisfacción la labor de la Iniciativa Conjunta UE-CELAC sobre Investigación e Innovación y deseamos que prosiga". https://data.consilium.europa.eu/doc/document/ST-12000-2023-REV-1/es/pdf

Disponer de comunicaciones avanzadas será un **estímulo para el desarrollo de la industria digital europea**. Este proceso asegurará, además, el mantenimiento del interés de todas las empresas multinacionales en el mercado europeo como base de clientes para sus productos y servicios más avanzados lo que, indirectamente, les obligará a adaptarse a cumplir la regulación digital europea.

R2. Apoyar la creación de programas formativos intensivos en todos los niveles educativos para que la población europea posea calificaciones digitales mínimas, y, además, se disponga del número de especialistas digitales que la UE requiere.

Al igual que con el despliegue de infraestructura de comunicaciones de banda ancha, también existe una necesidad perentoria de **asegurar que todos los ciudadanos europeos posean los niveles de cualificación digital** necesario para convertirlos en usuarios avanzados de servicios digitales.

Por otro lado, es perentorio acelerar la formación de especialistas en las tecnologías digitales ante la necesidad de cubrir el reto de la **reducción paulatina de las vocaciones en titulaciones STEM y el déficit de especialistas en la UE en áreas clave** como IA, semiconductores, comunicaciones móviles, análisis de datos, o aplicaciones en la nube. Ello requiere acometer un esfuerzo continuado y apoyado por la UE a pesar de que las competencias educativas recaen en los estados miembros primando desde la formación continua a la universitaria, y el reciclado de conocimientos como elemento clave.

En este sentido, ante la creciente competencia internacional por especialistas, la UE deberá en marcha una p**olítica migratoria de atracción de talento especializado** desde otros países, y crear un contexto favorable para su retención en la UE.

R3. Preparar el nuevo programa marco de investigación e innovación de la UE que comenzará en enero de 2028 desde la perspectiva de servir como instrumento político básico para reforzar la autonomía estratégica digital abierta de la Unión centrando el esfuerzo en un conjunto limitado de tecnologías digitales emergentes.

El actual programa marco denominado *Horizonte Europa* se desarrolla desde enero de 2021 hasta diciembre de 2027; nos encontramos, por tanto, en el comienzo de su **evaluación intermedia** que suele significar también en base a las conclusiones que se obtengan, el comienzo de las discusiones informales sobre lo que se requiere para el futuro programa marco, así como la estrecha interacción con los programas de los estados miembros.

La propuesta formal de la Comisión Europea sobre el siguiente programa marco no se producirá hasta la segunda mitad de 2025, pero es ahora el momento de repensar sus logros y los cuellos de botella existentes. De hecho, la experiencia indica que los últimos años de un programa marco suelen también emplearse para **"ensayar" determinadas actuaciones piloto** que se incorporarán en el siguiente. Desde mi punto de vista, el papel del programa marco de investigación e innovación, extendiéndose previsiblemente desde 2028 a 2034 debe actuar como un elemento clave para mejorar la soberanía tecnológica de la UE desde la perspectiva de **incrementar la autonomía estratégica europea en un contexto de interdependencia inteligente** fomentando la cooperación tecnológica a largo plazo con países aliados

Aunque estos acuerdos, deben tener un ámbito de actuación global, **el dominio digital deberá ser prioritario por su carácter habilitador y dual**. Ello obligará a repensar la colaboración con otros países reinterpretando el término de "abierto" en el sentido de aceptar una interdependencia tecnológica digital como mejor forma de preservar los beneficios de la globalización, lo que implicará **robustecer los instrumentos y condiciones necesarias para incrementar la cooperación internacional digital** en el futuro programa marco.

R4. Completar lo antes posible el desarrollo normativo básico digital, creando un marco regulatorio estable e impulsando acuerdos para acelerar la transposición de directivas comunitarias en los estados miembros buscando un equilibrio entre el principio de precaución y el fomento de la innovación.

La evolución de las tecnologías digitales seguirá acelerándose, alimentada a su vez por una convergencia temporal en la maduración de tecnologías emergentes. Como resultado de ello, **el marco regulatorio creado por la UE requerirá actualizaciones continuadas** buscando un equilibrio entre la opción de esperar a que las tecnologías maduren, y la opción de adelantarse para evitar la consolidación de situaciones de difícil retorno. En mi opinión, la complejidad de las relaciones internacionales en el ámbito digital y las interdependencias existentes va a obligar a la UE a discutir y negociar sus propias regulaciones con otros países aliados con los que pueda llegarse a acuerdos que mejoren su eficiencia.

En este contexto, la UE debe **evitar la existencia de un marco digital fragmentado en la propia UE** debido a procesos de transposición de directivas muy dilatados en el tiempo en función de los intereses nacionales. Difícilmente, se puede lograr un alineamiento con otros países fuera de la UE si persiste una diferencia significativa dentro de las fronteras de la UE.

R5.Promover la creación de "sandbox" regulatorios en áreas en las que disponer de experiencia es básico para estimular la creación de productos y servicios digitales que puedan expandirse a nivel global con una regulación inteligente.

Resolver el "*dilema de Collingridge*", entre esperar a la consolidación de la tecnología de una manera práctica y promover la innovación tecnológica no esperando a que madure, requiere establecer **mecanismos de experimentación** con nuevas tecnologías sin necesidad de disponer de una legislación consolidada, alentando su uso en un contexto de seguridad jurídica por empresas digitales para que puedan conocer de primera mano el efecto que tendrían las regulaciones sobre sus propios productos y servicios; al mismo tiempo, conocer esta experiencia es también necesaria para los legisladores.

Para ello, la creación de **zonas geográficas delimitadas** a modo de espacios de prueba controlados en las que se pueda explorar el efecto de determinadas regulaciones innovadoras, lo que se denomina **"sandbox" regulatorios**, es especialmente atractivo. La experiencia obtenida en estos espacios de prueba regulatoria puede servir de base para la generación y actualización de una regulación adecuada que permita la implementación de las leyes digitales aprobadas y pueda ser expandida para cubrir todo el territorio europeo.

R6.Asegurar la existencia de acuerdos en el ámbito digital con otros países, fundamentalmente con Estados Unidos, Japón, Corea del Sur, Singapur, India, Canadá, Australia, los países asociados a la UE, y en lo posible con China, para acordar regulaciones digitales alineadas en defensa de los principios y valores éticos europeos.

La *cooperación internacional* es un elemento clave en un posicionamiento internacional estable y prolongado en el tiempo. Europa es consciente de que su influencia es limitada y acuerdos concretos en tecnologías o sistemas tecnológicos concretos, apoyados por desarrollos conjuntos de tecnologías avanzadas cuando sea posible, supone un reto y una gran oportunidad.

Por este motivo, la puesta en marcha de **partenariados digitales internacionales de geometría variable** en las que gobiernos de los estados miembros, junto a la Comisión Europea y otros países aliados, en cooperación con el sector industrial promuevan el desarrollo y despliegue de tecnologías avanzadas, incluyendo su normalización, encaja con la visión de "abierta" con la que se adjetiva la autonomía estratégica digital europea.

Su discusión y acuerdo en el seno de **"*Comités de Comercio y Tecnología*" conjuntos** como los existentes con Estados Unidos e India deben

extenderse y adoptar configuraciones multilaterales cuando los temas lo aconsejen para reforzar las posiciones europeas.

R7. Proponer grandes **proyectos movilizadores digitales** en la Unión, tomando como base los IPCEI y modificando, si fuera necesario, la regulación de ayudas de estado, con la implicación del sector público y privado, y abiertos a la cooperación con otros países.

Los **proyectos importantes de interés común europeo (IPCEI)** se han propuesto para combinar recursos de los estados miembros y de la Comisión Europea en ámbitos en los que una actuación decidida y conjunta es necesaria para conseguir un impacto real en la autonomía estratégica europea con estrecha implicación de la industria europea. En estos proyectos la aplicación de las ayudas de estado se aplica de forma menos estricta para favorecer su puesta en marcha.

Lo relevante en estos casos es favorecer el desarrollo de productos y servicios avanzados y ambiciosos cubriendo el gap desde prototipos avanzados a productos comerciales (de TRL 6 a TRL 8) con implicación de empresas y gobiernos europeos. El uso de instrumentos financieros innovadores como la **compra pública innovadora** puede ser fundamental como, de hecho, ha sucedido en el ámbito del espacio o el de la defensa en los que se pueda explotar el carácter dual de las tecnologías digitales.

La experiencia obtenida hasta el momento puede extenderse en los próximos años a todas aquellas áreas en las que la UE considere necesario una mejora de su autonomía digital. Debemos, por tanto, **repensar el marco de ayudas de Estado** con objeto de incrementar la flexibilidad y poder competir mejor a nivel internacional.

R8. Potenciar la creación de amplias alianzas tecnológicas de raíz europea capaces de liderar el desarrollo de la nueva generación de sistemas digitales en tecnologías emergentes mediante la creación de ecosistemas digitales innovadores.Se requiere promover la creación de **alianzas tecnológicas** estables focalizadas en el desarrollo de sistemas de base digital apoyadas por la colaboración política entre gobiernos a largo plazo que proporcione el marco de apoyo político a las colaboraciones de la industria.

La **exitosa experiencia europea de alianzas tecnológicas entre grandes empresas** movilizando a otras muchas PYME y centros de investigación públicos en los ámbitos espaciales o aeronáuticos en el pasado debe extenderse a otros en el sector digital en relación con productos y servicios de datos en la nube, procesadores europeos, etc. superando las limitaciones de los IPCEI, con ambición de liderar el mercado mundial apoyados en la creación de ecosistemas innovadores focalizados.

R9. Restructurar las **cadenas globales de provisión** de materiales y productos digitales que requiere la industria europea, buscando reducir la dependencia de los materiales y componentes críticos identificados por la UE.

La UE depende fuertemente de productos y materiales generados en otros países y que se importan a través de cadenas de valor frágiles y sometidas a inestabilidades. Los análisis cualitativos y cuantitativos de dependencia realizados por la Comisión Europea (Arjona et al., 2023) y su reevaluación periódica suponen un punto de partida para la adopción de medidas urgentes que permitan reducir progresivamente esta dependencia en línea con la **Ley de materias primas críticas** en discusión.

El énfasis no solo debe ser puesto en la mejora de la resiliencia en la provisión de bienes físicos, sino también en el intercambio de datos en el que **asegurar la operatividad de cables submarinos y comunicaciones satelitales** debe cobrar una mayor prioridad mediante cooperaciones público-privadas. La puesta en marcha de estas medidas es urgente y debe contar con el consenso político y los recursos económicos suficientes para facilitar un equilibrio de su urgencia con la necesidad de cumplir los requisitos medioambientales.

R10. Prestar una atención preferente al **desarrollo de sistemas tecnológicos duales paneuropeos** que conjuguen el interés de actores púbicos y privados en dominios civiles y de defensa que sirvan para estimular el desarrollo e integración de tecnologías disruptivas.

El desarrollo de tecnologías duales debe aprovecharse como un incentivo clave para mejorar la soberanía tecnológica europea. Para ello, la UE deberá primar el desarrollo de tecnologías duales en los programas marco de investigación e innovación, deberá incrementar sustancialmente los recursos destinados al FED para incorporar tecnologías avanzadas desarrolladas en la UE, y aprovechar los recursos de la Ley del Chip y de la IA para disponer de capacidades propias.

Todo ello, puede también aprovecharse de **sistemas paneuropeos en defensa y seguridad** ya aprobados como el desarrollo de *IRIS*^{2}, la evolución de *Galileo*, o el sistema de combate aéreo *ECFAS* que ofrecen un marco plurianual de conjunción de recursos nacionales y comunitarios, y en los que el peso de los componentes digitales en su coste es muy elevado.

La ventaja de centrarse en el desarrollo de grandes sistemas duales en los que las ayudas de Estado se interpretan de manera más laxa por razones de seguridad nacional, suponen una oportunidad que la UE debe aprovechar. La necesidad de disponer de **sistemas militares digitales**

avanzados europeos interoperables en el contexto de la OTAN debe verse como una oportunidad en un momento de presupuestos de defensa expansivos.

R11. Potenciar y acelerar la **digitalización de la industria de defensa** con el fin de reforzar la seguridad de la UE en un contexto de cooperación y complementariedad con la OTAN, la Agencia Europea de Defensa, y la Agencia Europea del Espacio.

La potenciación de la posición estratégica de la UE en el ámbito de defensa y seguridad alrededor de la puesta en marcha de las actuaciones de la ***"Brújula Estratégica"*** pasa fundamentalmente por reforzar la industria de defensa europea. Este reforzamiento implica no solo que adquiera un tamaño y capacidad de coordinación suficiente para disponer de los sistemas de armas avanzados que se requiera, sino también para reducir la dependencia, fundamentalmente de Estados Unidos que no disminuye.

En este contexto la **digitalización de las operaciones de defensa** es una tendencia persistente que obliga a desarrollar e integrar tecnologías avanzadas de forma conjunta para asegurar la superioridad en caso de conflictos. Los compromisos adquiridos por los miembros de la UE que son, a su vez, miembros de la OTAN en incrementar sus recursos en defensa para alcanzar el 2% del PIB puede suponer una oportunidad para este proceso si se dedicasen gran parte de ellos a acelerar el proceso de digitalización.

R12. Reforzar la **presencia de la UE,** a través del Vicepresidente de la Comisión Europea y Alto Representante de la Unión, con un peso decisivo **en organizaciones internacionales favoreciendo su contribución al desarrollo de una gobernanza digital global.**

La importancia de **consolidar la presencia europea en la gobernanza digital global** reside en que la mayor parte de los conflictos tecnológicos internacionales tienen como origen el desarrollo y uso de las tecnologías digitales por parte de la población; su penetración social es enorme y la UE debe contribuir a determinar la gobernanza global futura de las mismas.

Una medida no estrictamente ligada a la autonomía estratégica digital, pero que ayudaría a ese proceso implica conceder al Vicepresidente de la Comisión Europea y Alto Representante de la Unión un peso decisivo en las relaciones internacionales de la UE en la esfera digital. Para ello, será necesario **reevaluar la distribución de competencias actuales** entre los estados miembros de la UE y las instituciones comunitarias que, en mi opinión, constituye un marco de discusión necesario y prerrequisito para asegurar el papel internacional de la Unión.

5.3. CONTRIBUCIÓN DE ESPAÑA A LA AUTONOMÍA ESTRATÉGICA DIGITAL DE LA UE

Focalizándose en la dimensión **digital**, esta sección presenta de una forma realista la manera en la que España puede **contribuir a la mejora de la autonomía estratégica y la soberanía digital de la UE** en su conjunto. No se trata, por tanto, de defender un planteamiento autárquico, no es posible, sino de **asumir un protagonismo en la UE** en las áreas en las que, a mi modo de ver, España sí puede hacerlo.

Los últimos datos de DESI (2022) presentados en el presente informe muestran una **buena posición de España en relación con la conectividad digital**; de hecho, desde un punto de vista comparado, es muy superior a la posición que ocupa España en los indicadores de innovación que publica anualmente la Comisión Europea en el que pertenece al grupo de países denominados "*innovadores moderados*" (EIS, 2023). Detrás de este eufemismo se esconde una **posición innovadora inferior a la media de la UE**.

España, como es obvio, se encuentra en el ámbito digital sometida a la legislación desarrollada por la UE en la que, en algunas de ellas, ha tenido un **papel activo en el proceso de aprobación**, y en la legislación nacional compatible o complementaria con la comunitaria en el ámbito digital. Ello no quiere decir que no deba impulsar, adelantándose a la UE, algunas **regulaciones en ámbitos emergentes** en los que puede actuar con una posición de liderazgo en el conjunto de la Unión aprovechando los denominados *"sandbox"* (entornos de prueba) regulatorios digitales para facilitar y encaminar la implementación de las regulaciones europeas.

En este sentido, el gobierno español ha anunciado en junio de 2023 que, tras un periodo de consulta pública, España contará con un ***"sandbox regulatorio en IA"*** para probar medidas del proyecto de reglamento de la UE sobre inteligencia artificial centrándose en aplicaciones de "*alto riesgo*" de acuerdo con el Reglamento[221]. Asimismo, también se ha anunciado en julio de 2023 la puesta en marcha del "***sandbox financiero"***[222] cuyo objetivo es probar innovaciones tecnológicas aplicables al sistema financiero en un entorno de pruebas controlado por las autoridades supervisoras.

El **buen posicionamiento español en algunas tecnologías y sistemas digitales** como son las del despliegue de comunicaciones móviles 5G o los satélites de comunicaciones, el uso de servicios digitales por las administraciones públicas o el ritmo de digitalización de la industria suponen un buen punto de partida. Un repaso de los indicadores de DESI permiten

221 https://finreg360.com/alerta/espana-contara-con-un-sandbox-regulatorio-para-probar-medidas-del-proyecto-de-reglamento-de-la-ue-sobre-inteligencia-artificial/

222 https://www.tesoro.es/sandbox/solicitudes-para-el-espacio-controlado-de-pruebas

identificar fortalezas que deben ser empleadas como base para la mejora de la posición española y su contribución a la autonomía estratégica digital de la UE.

Desde el punto de vista económico, los recursos que puede obtener de su participación (activa) en programas y proyectos europeos competitivos en los que se ha demostrado competitiva a nivel internacional[223] le permite liderar algunas actuaciones a su alcance. Ello se complementa con las asignaciones que voluntariamente (alineados con las directrices políticas adoptadas por el Consejo Europeo) realiza el gobierno español en tecnologías y aplicaciones digitales en otros programas asignados a España con recursos procedentes de la Unión; fundamentalmente, en los fondos estructurales, fundamentalmente **FEDER**, cofinanciado con recursos nacionales, y en el ***Plan de Recuperación, Transformación y Resiliencia***[224] financiado por los recursos de "*Next Generation EU*". En conjunto, proporcionan la base de inversión pública para acelerar la digitalización española.

Ante la tesitura de determinar las actuaciones que España debe hacer para que, en base a su potencial actual, pueda contribuir a la mejora del posicionamiento digital de la UE, considero que **las recomendaciones descritas para la UE en la sección anterior son aplicables de forma general al caso español**. Obviamente, deben estar condicionadas por su situación de partida y sus capacidades científicas, tecnológicas y económicas.

No obstante, y para el caso de España, planteo las siguientes **recomendaciones específicas**:

R1. Crear un órgano de carácter interministerial para **monitorizar la situación de la autonomía estratégica y la soberanía tecnológica digital española** que pueda analizar la evolución de los sectores y tecnologías críticos y proponer la adopción de medidas concretas para reforzarla.

Se trata con esta medida de **conocer de forma periódica y actualizada las dependencias digitales españolas y los riesgos asociados a ella**, en el desarrollo y la provisión de productos y servicios digitales con el nivel de detalle necesario para adoptar medidas concretas que incrementen su autonomía estratégica y la contribución a la europea.

Este órgano deberá coordinar y colaborar con otros observatorios temáticos existentes en España y con los de la UE para obtener una visión

223 En el pasado programa marco H2020, tomando como base datos del CDTI, la participación española en el área TIC alcanzó un retorno de 580,6 millones de euros que suponía el 10,1% del total de UE-28 (participaba el RU) ocupando el 3º puesto entre todos los países. https://www.horizonteeuropa.es/sites/default/files/noticias/Nota%20-%20Resultados%20participaci%C3%B3n%20espa%C3%B1ola%20en%20H2020%20vpub_1.pdf

224 https://planderecuperacion.gob.es/

global. Concretamente, puede ser una función que el *Observatorio Nacional de 5G* (https://on5g.es/) puede asumir en ese ámbito concreto más allá del cumplimiento de determinados indicadores. También deben participar en esta monitorización las **estructuras creadas para la ejecución de los PERTE** directamente relacionados con el ámbito digital como es el caso del PERTE de microelectrónica y semiconductores, pero también en los de la lengua, el aeroespacial, o el del automóvil en los que las tecnologías digitales tienen una relevancia crítica.

R2. Identificar **sectores industriales o de servicios con alta dependencia en IA y semiconductores** en los que deberá centrarse el esfuerzo presupuestario, regulatorio y formativo para reducir la dependencia exterior de conocimiento o componentes tecnológicos prestando especial atención a las tecnologías duales.

Aun aceptando el carácter habilitador y transversal en todos los sectores económicos de las tecnologías de semiconductores e inteligencia artificial, el impacto de la provisión de circuitos integrados o de acceso a algoritmos en algunos sectores es más destacado que en otros y, por tanto, también lo son las dependencias asociadas.

Los ejemplos de **dependencias del sector del automóvil** y su evolución hacia el vehículo autónomo y conectado, o la **transición energética basada en energías renovables**, requieren la adopción de medidas concretas de política industrial y energética para asegurar que España siga siendo un punto clave de referencia en la fabricación y digitalización de los sectores indicados.

Conseguir este objetivo requiere **actuar de forma coordinada entre el gobierno y las organizaciones empresariales** para incrementar la resiliencia de las cadenas de provisión que nutren los sectores identificados como prioritarios. Ello puede requerir alinear las necesidades industriales con los esfuerzos de diplomacia tecnológica con el fin de llegar a acuerdos de cooperación con países clave.

R3. Aprovechar el **desarrollo de los 12 PERTE aprobados** para considerar la autonomía estratégica digital como un objetivo transversal a todos ellos que deberá sustanciarse en las actuaciones que emanen de cada uno de ellos.

Prácticamente todos los PERTE aprobados van a tener una relación con las tecnologías digitales, ya sea porque es objeto directo de ella (como el caso del PERTE Chip) o porque constituye una tecnología habilitadora básica (como en los PERTE del automóvil conectado, el aeroespacial, el de la lengua y muchos otros).

Por este motivo una consideración de su contribución a la autonomía estratégica digital me parece especialmente apropiado en una **ventana de tiempo de ejecución de los recursos comunitarios de *Next Generation EU* relativamente corta** en la que los recursos empleados se conviertan en el incentivo para una transformación digital acelerada.

R4. Consolidar la digitalización del **sector español de la defensa** acelerando los programas que permitan una disponibilidad de sistemas digitales integrados con la OTAN.

El proceso de digitalización del sector de la defensa es imparable y se está acelerando hacia un **campo de batalla inteligente** que llegará a ser una realidad en los próximos años. Este reconocimiento, y los compromisos gubernamentales de incremento de los recursos disponibles en Defensa proporciona una oportunidad para que España pueda especializarse en algunos ámbitos industriales concretos buscando en ellos el reconocimiento de los mercados internacionales, y facilitar la interoperabilidad con la OTAN. La base industrial de partida merece la pena, aunque la falte dimensión.

Para ello, España deberá conjuntar sus capacidades alrededor de la **creación de un ecosistema innovador en el ámbito digital de la defensa** con la participación del sector público, de la industria de defensa, de start-ups innovadoras, y de los ministerios directamente implicados, y establecer objetivos a medio y largo plazo. Este ecosistema deberá estar estrechamente alineado con los que se establezcan a nivel europeo por parte de la EDA y de las prioridades del FED. El ejemplo de la participación española en el sistema de combate europeo ECFAS deberá ir acompañado de otros en los que la industria española tenga un papel relevante.

R5. Participar con decisión en las propuestas de iniciativas ambiciosas para el desarrollo de **sistemas y programas digitales paneuropeos** adoptando, en lo posible, una posición de liderazgo y arrastrando la participación de otros países.

España deberá realizar un esfuerzo mayor que en el pasado en la **participación significativa en programas innovadores de sistemas duales o de armamento**, priorizando el desarrollo de sistemas autónomos, en los que la integración de tecnologías digitales constituirá un elemento clave para alcanzar sus objetivos de prestaciones.

En mi opinión, el **sector espacial**, en el que España está bien situada, permitiría incrementar el liderazgo de nuevos sistemas satelitales, **tomando como base su participación en la ESA**. El modelo de "*justo retorno*" con el que ha operado históricamente la ESA y que se encuentra

en revisión para conseguir mayor eficiencia tras el Consejo de Ministros de 2023 en Sevilla, que las aportaciones españolas en programas voluntarios repercutan directamente en contratos industriales y en un sector como el espacial, facilitan una consolidación a largo plazo del sector industrial. En el futuro, España pueda que deba competir sin retorno garantizado, pero tiene las bases para poder hacerlo.

R6. Movilizar la formación, atracción y recuperación de **recursos humanos digitales** en cantidad suficiente para no estrangular el desarrollo económico digital español.

La **disponibilidad de talento digital** es una precondición para el desarrollo empresarial y de las administraciones públicas. Desde esta perspectiva, el **déficit de personal especializado formado en el ámbito digital** (realmente, en el ámbito STEM) se ha convertido en un problema general en la UE (y en otros países avanzados) ante el que España debe actuar desde una doble vía: asegurar la existencia de personal especializado altamente formado en los volúmenes y calidad requeridos para servir de atractivo a la ubicación de empresas europeas o multinacionales, y crear las condiciones para retener este personal en España; problema similar al que tiene la UE en su conjunto. Para ello, es necesario establecer unas condiciones de contexto salariales, y de calidad de vida que lo haga atractivo concentrando los recursos en zonas geográficas que, objetivamente, posean las condiciones para ello.

Esta actuación hacia el personal especializado es compatible con la de acelerar la formación básica de la población en competencias digitales de acuerdo con los **niveles de cualificación digital desarrollados en la UE** que permita apoyar la digitalización de España e, indirectamente, contribuir a mejorar el nivel de empleo, sobre todo, pensando en los jóvenes.

R7. Interactuar con la **Oficina de Ciencia y tecnología del Congreso de los Diputados**[225] con el fin de implicar en este problema a los diputados españoles que faciliten el desarrollo legislativo de las normas necesarias, así como la transposición de las directivas europeas.

La recientemente creada *"Oficina C"* es un instrumento que permitiría implicar a los diputados (y senadores) españoles disponer de información científica y tecnológica relevante y veraz que permitiera desarrollar regulaciones inteligentes en el marco digital en tecnologías digitales emergentes. De los informes realizados hasta el momento, dos están relacionados con el ámbito digital: "*Inteligencia artificial y salud*" (Oficina C, 2022a), y "*Ciberseguridad*" (Oficina C, 21022b).

225 https://www.oficinac.es/

Esta función puede también ayudar a transponer las directivas digitales europeas a las necesidades españolas con prontitud y eficacia, así como contribuir mejor a las negociaciones de los reglamentos del ámbito digital en los órganos comunitarios interaccionando con los europarlamentarios.

6

CONCLUSIONES

6.1. LA UE EN UN CONTEXTO GLOBAL CON NUEVOS ACTORES

En la presente monografía he pretendido **analizar el concepto de autonomía estratégica digital abierta de la UE y su relación con la soberanía tecnológica digital** en un contexto internacional convulso e inestable que puede describirse como ***VUCA*** (*Volátil, Incierto, Complejo y Ambiguo*) en el que los **factores geopolíticos** han adquirido mayor relevancia arrastrando con su impacto al posicionamiento de otros países, y a la creación y evolución de las alianzas entre ellos.

Esta situación de volatilidad e incertidumbre ha provocado **cambios estratégicos profundos de las grandes potencias tecnológicas** con impactos y consecuencias todavía inciertas. Ciurak (2023) decía que "*Hoy en día, el mundo está en guerra –guerra caliente, guerra fría, guerra tecnológica, guerra comercial, guerra social y guerra política intestina– y Estados Unidos, que fue pionero en las tecnologías que han desempeñado un papel decisivo en la generación de estas guerras, está (sorprendentemente) jugando a la defensiva en una geopolítica profundamente alterada".*

En este nuevo (des)orden mundial redefinido a trompicones desde la última década, soy consciente de que la UE no va a poder imponer unilateralmente sus puntos de vista al resto del mundo, pero sí **debe y puede contribuir con decisión a configurar los elementos que definan un nuevo orden mundial digital durante la presente década.** Podría hacerlo, aprovechando todos los instrumentos de "*poder inteligente"* a su alcance para alcanzar un grado suficiente de **autonomía estratégica digital realista**, en el supuesto de que logre actuar de forma conjunta y alineada entre los estados miembros y las instituciones comunitarias, y sepa forjar alianzas globales a largo plazo.

Más difícil aún es determinar el grado en el que esta autonomía digital puede ser realmente ***"abierta".*** La **"apertura"**, concebida como un

objetivo deseable que permita **conciliar** la satisfacción de los **legítimos intereses nacionales** que eviten una dependencia excesiva y unilateral por parte de otros países, implica la necesidad de **mantener al máximo nivel posible las relaciones e intercambios internacionales** en los planos científico-técnicos, comerciales, de cooperación industrial, o de seguridad y defensa; todas ellas son condiciones esenciales para proseguir el desarrollo socioeconómico de la UE en un marco de relaciones estables.

En la práctica, supone alcanzar un **equilibrio** entre naciones en un contexto global caracterizado como VUCA sometido a una **rápida evolución tecnológica en el dominio digital** en el que mantener de forma estable y a largo plazo las alianzas tecnológicas entre países que cooperan y compiten entre sí, con el peso económico e influencia que han adquirido algunas grandes multinacionales digitales, no es sencillo de conseguir.

Basta ver cómo la UE ha tratado de racionalizar la complejidad de las relaciones internacionales actuales estableciendo una **posición estructurada en diferentes niveles con respecto a su relación con China** para otear las dificultades que se encontrará en el futuro. El esquema elegido por la UE de considerar a China simultáneamente con cuatro roles diferentes manifiesta esa dificultad: 1) como *socio cooperador* en áreas en las que tienen objetivos estrechamente alineados, 2) como *socio negociador* donde era necesario alcanzar un equilibrio de intereses, 3) como *competidor económico* en la búsqueda del liderazgo tecnológico y 4) como rival sistémico al promover modelos alternativos de gobernanza (Ciuriak, 2023).

Hacer todo eso al mismo tiempo no es sencillo cuando la UE tiene, además de defender sus propias posiciones, la necesidad de mantener una relación privilegiada con Estados Unidos[224], reforzada por la pertenencia a la OTAN de la mayor parte de los estados miembros, y asegurar la mejor relación posible con otras potencias tecnológicas como India, Japón, Corea del Sur o el mismo Reino Unido, ahora fuera de la UE[225].

Los **condicionantes geopolíticos del desarrollo tecnológico** afectan a todo el abanico de tecnologías, pero es en las denominadas **tecnologías digitales** en las que se manifiesta con mayor crudeza dado su **simultáneo carácter habilitador y dual** junto a su enorme penetración en la sociedad y la dificultad de establecer fronteras. De su dominio depende el posicio-

224 Lo que no significa simple "seguidismo" como indica Tierney (2023) argumentando que una discrepancia controlada de la UE con respecto a Estados Unidos cumple un papel estabilizador esencial a nivel mundial contribuyendo a centrar las políticas de la administración americana.

225 La interacción simultánea entre la UE, China y Estados Unidos en el concierto mundial se ha asemejado a la complejidad física del "problema de los tres cuerpos". De igual manera que las fuerzas gravitacionales entre los cuerpos celestes pueden conducir a un movimiento impredecible y caótico, la interacción de factores económicos, políticos y estratégicos entre estas tres potencias (la UE, Estados Unidos y China) ha llevado a resultados aparentemente contradictorios e inestabilidad con impacto en otros muchos países "obligados" a alinearse con algunas de las potencias... aunque se resistan a ello.

namiento de todos los países en su continua búsqueda de la autonomía estratégica, digital en este caso.

La situación de partida de la Unión Europea en el ámbito digital, analizada en este informe desde diversas perspectivas empleando un **modelo conceptual multidimensional en niveles**, ha permitido extraer algunas claves de las **posibilidades reales que tiene de conseguirlo y la dimensión del reto al que se enfrenta**. Aunque de acuerdo con los indicadores de DESI es innegable que la UE ha avanzado en los últimos años en relación consigo misma, en unos estados miembros más rápido que en otros, también otros países fuera de la UE, referentes en el ámbito digital, lo han hecho más deprisa que la propia UE.

Parto del convencimiento de que, en mi opinión, **la UE no tiene sencillo conseguir la autonomía estratégica digital pretendida** porque sus debilidades objetivas actuales en el ámbito digital en varios de los niveles indicados en la presente monografía señalan una situación inestable que puede deteriorase en el futuro, a pesar de haberse dotado de un marco regulatorio protector, ambicioso e innovador por la falta de un tejido empresarial digital que compita con éxito frente a las multinacionales sistémicas digitales de Asia o de Estados Unidos.

Durante los próximos años, **nuevas potencias tecnológicas irrumpirán con fuerza en el ámbito digital,** no solo para ubicar instalaciones de fabricación a bajo coste de productos digitales de gran consumo o para albergar grandes centros de datos aprovechando costes energéticos reducidos, sino participando o liderando el desarrollo de nuevas tecnologías emergentes digitales. Téngase en cuenta que **las barreras de entrada en el sector digital son menores de las que pueden encontrarse en otros sectores** económicos si se dispone de suficiente capacidad de inversión y abundantes personas formadas. Y en este contexto, la búsqueda de oportunidades de inversión en la UE de grandes fondos de inversión soberanos de otros países y las tendencias demográficas cuentan.

La emergencia como actores digitales relevantes de nuevas potencias tecnológicas ancladas en lo que se ha denominado el *Sur Global* que decidan acelerar su capacidad tecnológica digital, establezcan condiciones más duras de entrada a sus mercados en la medida en la que se sienten más fuertes para hacerlo, o primen su desarrollo más allá del marco de valores y principios que la UE desea establecer en sus regulaciones digitales (centrada en la protección de sus ciudadanos) puede conducir a un **aislamiento de la UE en el acceso a los mercados globales de productos y servicios digitales emergentes**. En mi opinión, **un incremento de la fragmentación de los mercados digitales no beneficia a la UE.**

En este contexto, ya **no basta con analizar la posición de la UE frente a Estados Unidos y China** en el ámbito digital como base para la toma de decisiones estratégicas**.** Otros actores, buscando un posicionamiento digital propio, pueden jugar un papel clave en el futuro ante los que la UE deberá interaccionar manteniendo una posición estratégica que le permita disponer de un marco de colaboración tanto bilateral como multilateral suficiente para poder influir en un contexto de **alianzas tecnológicas de geometría variable muy dinámicas.**

De los muchos actores posibles que alcanzarán un papel clave al final de la presente década, es relevante, en mi opinión, la reafirmación del **papel geopolítico que puede alcanzar *India*** durante la presente década y el incremento de complejidad geopolítica alcanzado[226]. Por ello, es necesario que la **estrategia de la UE en el Océano Índico** alcance una relevancia mucho mayor que la actual definida por la estrategia europea aprobada en 2021[227] y que Francia ya ha pretendido revitalizar en 2023[228].

India ya es el país más poblado del mundo con una población estimada en agosto de 2023 de 1.431 millones de personas, y con una **tecnología avanzada** en algunos ámbitos como demuestran sus éxitos espaciales con el alunizaje de una sonda en el polo sur de la Luna en agosto de 2023[229], su capacidad nuclear obtenida desde hace muchos años, y una dinámica industria de servicios software que supone el 7,5% del PIB de India y alcanzó en 2022 un volumen de exportación de 178.000 millones de dólares USA[230]. Además, en una situación como la actual puede beneficiarse de la estrategia de algunos países occidentales y asiáticos de reducir su exposición a China apostando por India[231].

La puesta en marcha de la iniciativa ***"India Semiconductors Mission"*** mencionada anteriormente en esta monografía indica su interés político en mejorar su posicionamiento en la cadena de valor de los semiconductores, al menos, de los no muy avanzados con resoluciones superiores a 22 nm, y las dificultades que encuentra para atraer inversiones.

226 En la referencia anterior al denominado "problema de los tres cuerpos", con la inclusión de India nos encontraríamos ante un problema de una dimensión de complejidad superior en el que la gobernanza global será mucho más compleja.

227 En el ámbito digital se creó en 2022 un partenariado EU-India en conectividad digital ligado a la Global Gateway Strategy de la UE con los objetivos de reforzar las conexiones seguras, cables submarinos, redes satelitales, 5G, pagos transfronterizos y servicios de alerta. https://www.eeas.europa.eu/eeas/factsheet-eu-india-connectivity-partnership_en

228 Más focalizada que la estrategia europea en la región Indo-Pacífica propugnada por Francia (France Diplomacy, 2023).

229 https://www.space.com/chandrayaan-3-moon-south-pole-why-nasa-wants-to-go-too

230 https://www.statista.com/topics/9497/software-industry-in-india/#topicOverview y https://www.statista.com/topics/2256/it-industry-in-india/#topicOverview

231 Sin entrar en muchos detalles, la posibilidad de que India consiga convertirse en un actor global digital relevante dependerá de que sea capaz de lograr una estabilidad socioeconómica a largo plazo sin caer en una deriva hacia nacionalismos excesivos que rompan una delicada cohesión interna en un país multicultural como India con estados del Norte más empobrecidos que los del Sur.

También India está transformando el marco de la regulación digital. En agosto de 2023 se ha aprobado la "***Ley de Protección de Datos Personales Digitales***"[232] que establece el procesamiento de datos personales digitales siguiendo la estela del RGPD de la UE. En el ámbito de la regulación de servicios y mercados digitales ha empezado en 2023 la discusión sobre la "***Digital India Act***"[233] como elemento clave de la estrategia de ***India Digital*** para 2026 cuyos principios básicos, sin aventurar el contenido de los textos definitivos, ni su futura implementación, no son muy diferentes de los planteados en la UE con la DSA y la MDA.

La **cumbre del G20** celebrada en India el 9-10 de septiembre de 2023 reafirma el papel de liderazgo de India entre los grandes países[234]. Estoy seguro de que lo va a ejercer entre los países del *Sur Global*, en su impulso a la expansión de los BRICS y, por supuesto, en su soterrado enfrentamiento geopolítico con China. En relación con la UE, la reciente creación del *Consejo de Comercio y Tecnología* entre la India y la UE (*"EU-India Technology & Trade Council")* será un elemento clave para determinar hasta qué punto puede crearse un partenariado en el ámbito digital entre ambos.

En el **ámbito digital**, y anclado en la necesidad de mejorar la competitividad europea, la UE está tratando de lograr **acuerdos sobre normas comerciales digitales** (Comisión Europea, 2023), centrándose en los socios de Asia, basándose, en su caso, en partenariados digitales como los que ha realizado con Corea del Sur y Singapur, además de buscar la extensión de los acuerdos comerciales digitales con los miembros de ASEAN, promoviendo así los derechos de la UE y sus valores. El *Consejo de Comercio y Tecnología UE-India* mencionado anteriormente es otro ejemplo de cómo reforzar la cooperación internacional con socios estratégicos. Aún es pronto para ver los resultados de este esfuerzo.

6.2. NO TODO ES QUERER Y SABER REGULAR

El presente informe ha mostrado un mundo sometido a cambios globales muy profundos en el que **las instituciones multilaterales están en entredicho y las nuevas no han acabado de emerger**. La UE quiere y debe jugar en este nuevo terreno de juego. Parkes (2023) lo expone diciendo:

232 Reconoce tanto el derecho de las personas a proteger sus datos personales como la necesidad de procesar dichos datos personales para fines legales y para asuntos relacionados o incidentales con ellos. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

233 "La nueva ley digital debe ser evolutiva y coherente con las tendencias cambiantes del mercado, la disrupción de las tecnologías, el desarrollo de la jurisprudencia internacional y los estándares globales para el marco cualitativo de prestación de servicios / productos. Con el fin de crear, modificar y hacer cumplir rápidamente las regulaciones, adoptará un "enfoque basado en principios y reglas" para la regulación que proporciona un marco legislativo bajo principios rectores y medidas efectivas para garantizar el cumplimiento del estado de derecho en constante evolución."
https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf

234 https://g20.mygov.in/

"La Unión Europea es consciente de estos cambios globales y su respuesta ha sido lanzarse sin contemplaciones a una competición geoeconómica. Ha desechado su fe incuestionable en las instituciones económicas mundiales y ahora se centra en la protección comercial unilateral, la política industrial y en asegurarse el acceso a recursos y tecnologías críticas. Los líderes de la UE explican que esto equivale a un despertar geoeconómico, y que están elaborando el equilibrio adecuado de cooperación, competencia y contención frente a su viejo aliado Estados Unidos y el mercado emergente de China".

Dado que los valores y principios que preconiza la Unión en el acceso y uso de productos y servicios digitales no coinciden, necesariamente, con los de otros países, **no bastará con un enfoque regulatorio** de amplio impacto sobre terceros (el conocido como *"efecto Bruselas"*) para forzar su cumplimiento y expansión sin incrementar el riesgo de perder la batalla en el desarrollo tecnológico y ralentizar la comercialización en la UE de servicios digitales avanzados. Desgraciadamente, pocas empresas multinacionales digitales no europeas ven a la UE como un mercado atractivo en el que desarrollar y perfeccionar nuevos productos para su entrada en los mercados mundiales. **No basta con querer y saber regular, hay que poder.**

La iniciativa que ha tomado la UE en la regulación digital de algunas tecnologías emergentes como es el caso de la protección de datos o la IA, anticipándose a otros países es un elemento muy relevante para convertirse en un referente global. Pero ello **no asegura el dominio de los mercados con productos y servicios digitales europeos.** Ortega (2023) lo expresa diciendo que *"Europa regula, pero esta no es una fuerza de poder real, sino de valores, importantes, sin duda"*; importantes, sí, pero no suficientes.

Incluso en el supuesto de un **éxito regulatorio** de la UE y que, por ejemplo, las nuevas leyes de mercados y servicios digitales obliguen a todas las plataformas digitales (en estos momentos dominadas por empresas de Estados Unidos y China) a adaptarse a ellas, el que otros países como India también adopten regulaciones similares, y que exista una **conciencia global centrada en los derechos digitales del ciudadano**, no exime de que los europeos sigamos utilizando fundamentalmente productos y servicios digitales no europeos. ¿Es eso lo que queremos?

Enfrentarse a estas limitaciones va a requerir una **concienciación colectiva prolongada en el tiempo sobre el valor transformador de las tecnologías emergentes** a la que, personalmente, veo aún poca decisión real en la Unión y sus estados miembros de llevar a sus últimas consecuencias, más allá de las declaraciones políticas y el lanzamiento de programas concretos de I+D o infraestructuras con recursos económicos limitados y, muchas veces, fragmentados entre los estados miembros.

Desde mi punto de vista, la UE necesita **reforzar fuertemente su industria de alta tecnología** actuando sobre sectores no necesariamente

digitales, pero sí muy digitalizados por su estrecha dependencia de la integración de productos y servicios digitales como son los de la aeronáutica, el espacio, la automoción, la robótica industrial, las comunicaciones móviles, o la gestión inteligente de las energías renovables para asegurar su competitividad en los mercados globales. **Es en estos sectores tecnológicos altamente competitivos en los que la UE puede defender mejor sus planteamientos a nivel global de manera integrada.**

Será difícil conseguirlo si la UE no avanza en una **integración política mayor** que permita negociar con una "voz única" en el ámbito internacional, si no dispone de personas suficientes formadas en ámbitos digitales especializados que vean su futuro profesional en la UE, y si no es capaz de atraer inversiones tecnológicas a largo plazo no especulativas; alejado de lo que hoy sucede. **Todo ello es posible, pero tiene que actuar con decisión.**

Expresamente, la necesidad de **conciliar un mayor nivel de cohesión digital interior** (monitorizado anualmente en los indicadores DESI) con la necesidad de encontrar una **agenda exterior acordada unánimemente y defendida con una voz única europea** va a requerir, para que sea efectiva, un **replanteamiento del marco competencial** entre los órganos comunitarios y los estados miembros definido en el Tratado de la UE.

No será sencillo conseguirlo cuando el **modelo futuro de la gobernanza real de la UE sigue sin ser totalmente compartido** por los 27 estados miembros y cuando la nueva fase de expansión con Ucrania, Moldavia y algunos países de los Balcanes se aproxima en el horizonte exigiendo un esfuerzo de cohesión interior mayor y unos mecanismos de toma de decisiones más eficientes.

El análisis sobre la situación digital de la UE se ha focalizado en el presente informe en los ámbitos concretos de los **semiconductores** y la **inteligencia artificial**, considerados parte esencial de las tecnologías digitales y con una función habilitadora para todos los sectores, reforzada también por su carácter de uso dual. Ello ha permitido acercarse un poco más a analizar la situación europea en ámbitos de enorme importancia actual, que seguirán, sin duda, creciendo y evolucionando rápidamente durante la presente década, y **en el que todas las grandes potencias están redoblando su esfuerzo con implicaciones civiles y militares**. Se trata de una situación con luces y sombras y muy cambiante.

Finalmente, el **conjunto de recomendaciones** para el conjunto de la UE, y algunas específicas para España, presentadas en el informe pretenden guiar el debate en el conjunto de la sociedad alrededor de las **posibilidades realistas de configurar una autonomía estratégica digital abierta de la UE**; debate que, en mi opinión, es necesario y urgente.

7

REFERENCIAS

1. Anderljung, M. y Scharre, P. (2023). How to Prevent an AI Catastrophe: Society Must Get Ready for Very Powerful Artificial Intelligence. Foreign Affairs. August 14, 2023. https://reader.foreignaffairs.com/2023/08/14/how-to-prevent-an-ai-catastrophe-2/content.html

2. Arjona, R., Connell, W. y Herghelegiu, C. (2023). An enhanced methodology to monitor the EUs' strategic dependencies and vulnerabilities. Working Paper 14. Single market and Economics papers. ISBN: 978-92-68-02647-2. Doi: 10.2873/768035.

3. Arnal, J, y Ricart, R.J. (2023). A Connectivity Package for the EU: considerations on digital strategic autonomy. Policy Paper. Real Instituto Elcano. 17 May 2023. https://www.realinstitutoelcano.org/en/policy-paper/a-connectivity-package-for-the-eu-considerations-on-digital-strategic-autonomy/

4. Arteaga, F., Escribano, G., Feás, E., García-Calvo, C., González-Enríquez, C., Jorge, R. Lázaro, L., Malamud, C., Núñez, R., Talvi, E., Urbasos, I., Vicente, A. (2023). Un Consejo de Comercio y Tecnología Unión Europea-América Latina. ARI 79/2023 21 de agosto de 2023. Real Instituto Elcano, https://www.realinstitutoelcano.org/analisis/un-consejo-de-comercio-y-tecnologia-union-europea-america-latina/

5. Baur, A. (2023). European Dreams of the Cloud: Imagining Innovation and Political Control. Geopolitics, Routledge. January 2023. https://doi.org/10.1080/14650045.2022.2151902

6. Beidou (2022). China's BeiDou Navigation Satellite System in the New Era. The State Council Information Office of the People's Republic of China. November 2022. ISBN 978-7-119-13150-4 © Foreign Languages Press Co. Ltd, Beijing, China, 2022. https://english.www.gov.cn/archive/whitepaper/202211/04/content_WS63647de9c6d0a757729e249d.html

7. Biscop, S. (2022). 'Strategic autonomy: not without integration'. Policy Brief. Brussels: Foundation for European Progressive Studies (FEPS), Fondation Jean-Jaurès, Friedrich-Ebert-Stiftung EU-Office Brussels. January 2022. https://feps-europe.eu/wp-content/uploads/2022/01/Strategic-Autonomy-Not-without-integration.pdf

8. Borrell, J. (2023). The year that war returned to Europe. EU foreign policy in 2022. European Union External Action. ISBN 978-92-9463-233-4. DOI: 10.2871/90017

9. Bradford, A. (2020). The Brussels effect. How the European Union Rules the World. Oxford Scholarship. Print ISBN-13: 9780190088583.

10. Bremmer, I. Suleyman, M. (2023). The AI Power Paradox: Can States Learn to Govern Artificial Intelligence—Before It's Too Late? Foreign Affairs, August 16, 2023. (issue September/October 2023).

11. Broeders, D. (2022). DIGITAL SOVEREIGNTY: FROM NARRATIVE TO POLICY? EU Cyber Direct and The Hague Program on International Cyber Security. December 2022.

12. 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. March 2023. DOI: 10.1111/jcms.13462

13. Bueger, C., Liebetrau, T., Franken, J. (2022). Security threats to undersea communications cables and infrastructure – consequences for the EU. PE 702.557 EP/EXPO/SEDE/FWC/2019-01/LOT4/1/C/12. June 2022.

14. Burni (2023). Progressive Pathways to European Strategic Autonomy. How can the EU become more independent in an increasingly challenging world? Policy Brief. The Foundation For European Progressive Studies (FEPS).

15. Burwell, F.G. and Propp, K. (2022). Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy. Atlantic Council. Europe Center. October 2022. ISBN-13: 978-1-61977-254-0.

16. Cagnin, C. Muench, S., Scapolo, F., Störmer, E., Vesnic-Alujevic. L. (2021). Shaping & securing the EU's Open Strategic Autonomy by 2040 and beyond. Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-41020-1, doi:10.2760/414963, EUR 30802 EN, JRC125994.

17. Carnap, von K. (2023). Fragmentando Internet: más allá (y más acá) de la Gran Muralla digital china. Política Exterior. 14 de marzo de 2023. https://www.politicaexterior.com/fragmentando-internet-mas-alla-y-mas-aca-de-la-gran-muralla-digital-china/

18. Carrozza, I., Marsh, N. Reichberg, G.M. (2022). Dual-Use AI Technology in China, the US and the EU. Strategic Implications for the Balance of Power. PRIO Paper 2022. Peace Research Institute Oslo (PRIO). ISBN: 978-82-343-0368-5 (online) https://www.prio.org/download/publicationfile/3567/Carrozza,%20Marsh,%20Reichberg%20-%20Dual-Use%20AI%20Technology%20in%20China,%20the%20US%20and%20the%20EU%20-%20Strategic%20Implications%20for%20-the%20Balance%20of%20Power,%20PRIO%20Paper%202022.pdf

19. CEPAL (2023). Extracción e industrialización del litio. Oportunidades y desafíos para América Latina y el Caribe. Comisión Económica para América Latina y el Caribe. Junio de 2023.

20. Cheng, J. & Zeng, J. (2023a) Shaping AI's Future? China in Global AI Governance, Journal of Contemporary China, 32:143, 794-810. https://doi.org/10.1080/10670564.2022.2107391

21. Cheng, J. & Zebg, J. (2023b). "Digital Silk Road" as a Slogan Instead of a Grand Strategy. Journal of Contemporary China. 15 June 2023. https://doi.org/10.1080/10670564.2023.2222269

22. Ciuriak, D. (2023). The Digital Revolution Has Transformed Geopolitics. Center for International Governance Innovation (CIGI). July 19, 2023. https://www.cigionline.org/articles/the-digital-revolution-has-transformed-geopolitics/

23. Colback, L. (2023). The rise of the platform economy. FT Tech for Growth Forum, March, 13, 2023. https://www.ft.com/content/e5f5e5b9-3aec-439a-b917-7267a08d320f

24. Collingridge, D. (1980). The Social Control of Technology. Publisher. Palgrave Macmillan; ISBN-10. 031273168X 1980.

25. Condorelli, D., Padilla, J., Tuffin, A., Vasas, Z. (2023). Why TELCOs' Fair Share Proposal Makes Economic Sense And it is not rent seeking! Compacc Lexecon. 17 May 2023. https://www.telefonica.com/en/wp-content/uploads/sites/5/2023/05/The-Fair-Share-Proposal-in-Telco.pdf

26. Consejo Europeo (2023). 12000/1/23 REV 1 (es). Declaración de la Cumbre UE-CELAC de 2023. COLAC 98. Bruselas, 1 de agosto de 2023. https://data.consilium.europa.eu/doc/document/ST-12000-2023-REV-1/es/pdf

27. Cordesman, A.H. (2014). The Real Revolution in Military Affairs. Center for Strategic and International Studies (CISS). August 5, 2014. https://www.csis.org/analysis/real-revolution-military-affairs

28. Da Ponte, A., León, G., Álvarez, I. (2022). Technological sovereignty of the EU in advanced 5G mobile communications: An empirical approach. Telecommunications Policy. 19 de octubre de 2022. https://doi.org/10.1016/j.telpol.2022.102459

29. Damen, M. (2022). EU strategic autonomy 2013-2023: From concept to capacity. Briefing, Strategic Foresight and Capabilities Unit PE 733.589 – EPRS | European Parliamentary Research Service. July 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf

30. Drewel M., Özcan, L., Koldewey, C., Gausemeier, J. (2020). Pattern-based development of digital platforms. Creativity and Innovation Managem0ent. 3 December 2020 https://doi.org/10.1111/caim.12415

31. Edler J, Blind K, Kroll H, Schubert T (2021). "Technology Sovereignty as an Emerging Frame for Innovation Policy- Defining Rationales, Ends and Means". Fraunhofer ISI Discussion Papers Innovation Systems and Policy Analysis n. 70. Karlsruhe July 2021.

32. DESI (2022). Digital Economy and Society Index (DESI) 2022. Thematic chapters

33. EEAS (2022). A Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

34. EIS (2023). European Innovation Scoreboard. 6 July 2023. https://research-and-innovation.ec.europa.eu/statistics/performance-indicators/european-innovation-scoreboard_en#european-innovation-scoreboard-2023

35. European Commission (2021a). 2030 Digital Compass: the European way for the Digital Decade. Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of the Regions. COM/2021/118 final. 9-3-2021. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

36. European Commission (2021b). Proposal for a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts. COM/2021/206 final https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

37. European Commission (2022). Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se establece un marco de medidas para reforzar el ecosistema europeo de semiconductores (Ley de Chips). COM(2022) 46 final 2022/0032 Bruselas, 8.2.2022. https://eur-lex.europa.eu/resource.html?uri=cellar:ca05000a-89d4-11ec-8c40-01aa75ed71a1.0010.02/DOC_1&format=PDF

38. European Commission (2023a). Joint Statement EU-US Trade and Technology Council of 31 May 2023 in Lulea, Sweden. Brussels, 31 May 2023. https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2992

39. European Commission (2023b). REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se establece un marco para garantizar el suministro seguro y sostenible de materias primas fundamentales y se modifican los Reglamentos (UE) 168/2013, (UE) 2018/858, (UE) 2018/1724 y (UE) 2019/1020. Comunicación de la Comisión COM(2023) 160 final Brussels, 16.3.2023 2023/0079(COD) https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52023PC0160

40. European Commission (2023c). Aplicación del conjunto de instrumentos de la UE para la seguridad de las redes 5G. COMUNICACIÓN DE LA COMISIÓN C(2023) 4049 final. Bruselas, 15.6.2023. https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox

41. European Commission (2023d). Report on the State of the Digital Decade. 29 September 2023. https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

42. European Union (2023). Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027. Document 32023R0588. PE/65/2022/REV/1. http://data.europa.eu/eli/reg/2023/588/oj

43. EU-India (2023). EU – India Joint Statement 1st Meeting of the Trade and Technology Council. 16 May 2023. Brussels, Belgium https://digital-strategy.ec.europa.eu/en/library/eu-india-ttc-joint-statement

44. EU-US (2022). EU-US Joint Statement of the Trade and Technology Council. European Commission 5 December 2022. https://ec.europa.eu/commission/presscorner/detail/en/statement_22_7516

45. Fan, J.H., Omura, A., Roca, E. (2023). Geopolitics of rare earths. European Journal of Political Economy. Vol 78. June 2023, 102356. https://doi.org/10.1016/j.ejpoleco.2022.102356

46. Fiott, D. (2023). ¿Invertir e innovar? España y el Fondo Europeo de Defensa. Real Instituto Elcano. 25 de septiembre de 2023. https://www.realinstitutoelcano.org/analisis/invertir-e-innovar-espana-y-el-fondo-europeo-de-defensa/

47. France Diplomacy (2023). The European Union in the Indo-Pacific. https://www.diplomatie.gouv.fr/en/country-files/regional-strategies/indo-pacific/the-european-union-in-the-indo-pacific/#:~:text=EU%20Strategy%20for%20Cooperation%20in%20the%20Indo%2DPacific&text=With%20this%20new%20strategy%20and,human%20rights%20and%20international%20law.

48. Glenny, M. (2022). The scramble for rare earths carries big geopolitical risks. Financial Times, September 27, 2022. https://www.ft.com/content/a7bf7029-9374-4a77-88b2-b4c21c865cbd

49. Gómez, A. (2023). Inteligencia artificial y lengua española. Discurso leído. Real Academia Española. 21 de mayo 2023.

50. Gavin, V. (2005). La Comunidad Europea de Defensa (1950-1954) ¿Idealismo europeo o interés de Estado? Tesis doctoral Universidad de la Rioja. Fundación Dialnet. https://dialnet.unirioja.es/servlet/tesis?codigo=3571

51. Grevi, G. (2019). Strategic autonomy for European choices: The key to Europe's shaping power. Discussion Paper. Europe In the World Programme. European Policy Center. 19 July 2019. https://www.epc.eu/content/PDF/2019/190719_Strategicautonomy_GG.pdf

52. G7 (2023). G7 Hiroshima Leaders' Communiqué May 20, 2023. https://www.g7hiroshima.go.jp/documents/pdf/Leaders_Communique_01_en.pdf

53. Hartmann, J. (2023). Protecting the EU's Submarine Cable Infrastructure. Germany's Opportunity to Transform Vulnerability into Mutual Resilience. DGAP Policy Brief. German Council on Foreign Relations. No. 23, July 2023. https://dgap.org/system/files/article_pdfs/DGAP-PolicyBrief-2023-23-EN.pdf

54. Hartmann, J., Kremer, K., Ross, J., Stockle, J., Tallis, B. y TolskdorfF, D. (2023). 'Zeitenwende' más allá de Alemania. Política Exterior. 16 de marzo de 2023.

55. IISS (2022). 'Defence Innovation and the European Union's Strategic Compass', IISS Strategic Comments, vol. 28, no. 10, 30 May 2022.

56. Intellinews (2023). Russia is successfully evading Western technology sanctions. Bne Intellinews. March 2023. https://intellinews.com/russia-is-successfully-evading-western-technology-sanctions-271899/

57. Karistad, W. (2023). Digital Sovereignty. Adapting to a challenging digital landscape. Tietovery. https://www.tietoevry.com/en/blog/2023/05/all-you-need-to-know-about-digital-sovereignty/

58. Lafayette, W. (2023). America is building chip factories. Now to find the workers. The country's chipmaking goals will test its manufacturing potential. The Economist. August 5, 2023. https://www.economist.com/united-states/2023/08/05/america-is-building-chip-factories-now-to-find-the-workers?frsc=dg%7Ce

59. Larsen, B.C. (2022). The geopolitics of AI and the rise of digital sovereignty. Economic Studies. Brooking. https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/

60. Lee, Kai-Fu (2021). The Third Revolution in Warfare. The Atlantic, 11 September, 2021. https://www.theatlantic.com/technology/archive/2021/09/i-weapons-are-third-revolution-warfare/620013/

61. León, G. (2023a). Relevancia geopolítica de las tecnologías duales. consecuencias y oportunidades para reforzar la soberanía tecnológica de la Unión Europea. UPM Press. Julio 2023. ISBN: 978-84-18661-45-7

62. León, G. (2023b). Reforzar la soberanía tecnológica en el seno de la autonomía estratégica: Hacia una menor dependencia internacional. Informe anual de ciencia y tecnología. Fundación Alternativas. Mayo de 2023.

63. León, G. (2023c). Autonomía estratégica abierta digital de la UE. Fundación Alternativas, Documento de trabajo. No. 228/ 2023. Septiembre 2023.

64. León, G. y da Ponte, A. (2023). Soberanía Tecnológica de la UE, ¿Un Objetivo Alcanzable? Aproximación Conceptual y Derivaciones Prácticas. Monográfico. Revista de Economía Industrial. 2023.

65. Marcus, S. (2023). Adapting the European Union AI Act to deal with generative artificial intelligence. Bruegel. 19 July 2023. https://www.bruegel.org/analysis/adapting-european-union-ai-act-deal-generative-artificial-intelligence

66. MFA (2023a). The Global Security Initiative Concept Paper. MFA News. Ministry of Foreign Affairs of the People's Republic of China. February 21, 2023. https://www.fmprc.gov.cn/mfa_eng/wjbxw/202302/t20230221_11028348.html

67. MFA (2023b). Remarks by Ambassador Zhang Jun at the UN Security Council Briefing on Artificial Intelligence: Opportunities and Risks for International Peace and Security. Permanent Mission of People's Republic of China to the UN. July 18, 2023. http://un.china-mission.gov.cn/eng/hyyfy/202307/t20230719_11114947.htm

68. Morillas, P. (2021). An architecture fit for strategic autonomy: institutional and operational steps towards a more autonomous EU external action'. Policy Brief. Brussels: Foundation for European Progressive Studies (FEPS), Fondation Jean-Jaurès, Friedrich-Ebert-Stiftung EU-Office Brussels. November 2021. https://feps-europe.eu/wp-content/uploads/2021/11/211125-policy-brief_strategic-autonomy2.pdf

69. Müller, M. (2023). The 'New Geopolitics' of Mineral Supply Chains: A Window of Opportunity for African Countries. SAIIA program. 29 July 2023. South African Journal of International Affairs, 30:2, 177-203, DOI: https://doi.org/10.1080/10220461.2023.2226108

70. Murgia, M., Bradshaw, T. y Waters, R. (2023). Nvidia avisa del gran impacto de la guerra de los chips con China. Financial Times 24 May 2023

71. NATO (2023). Vilnius Summit Communiqué. Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023. Press Note. https://www.nato.int/cps/en/natohq/official_texts_217320.htm

72. Negreiro (2022). The NIS2 Directive. A high-common level of cybersecurity in the Union. European Parliamentary Research Service PE 689333. June 2022. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

73. Nocetti, J. (2022). "Europe and the Geopolitics of 5G: Walking a Technological Tightrope", Geopolitics of Technology Program. Études de l'Ifri. Institut Francais des relations Intenationales. January 2022. ISBN: 979-10-373-0518-3 https://www.ifri.org/sites/default/files/atoms/files/nocetti_5g_europe_2022_us.pdf

74. Nye, J. (2005). Soft Power, The Means to Success in World Politics, Public Affairs, 2005.

75. Nye, J. (2009). "Get Smart: Combining Hard and Soft Power", Foreign Affairs. Vol. 88, No. 4, July/August 2009.

76. OECD (2023a). Artificial Intelligence in Science. Challenges, Opportunities and the Future of Research. OECD Publishing, Paris, ISBN 978-92-64-44621-2 (pdf) https://doi.org/10.1787/a8d820bd-en

77. OECD (2023b). Artificial intelligence and jobs. An urgent need to act. OECD Employment Outlook 2023. 12 July 2023. https://www.oecd.org/employment-outlook/2023/

78. OCDE (2023c). Regulatory Sandboxes in Artificial Intelligence. OECD DIGITAL ECONOMY PAPERS July 2023. No. 356 R. https://www.oecd-ilibrary.org/deliver/8f80a0e6-en.pdf?itemId=/content/paper/8f80a0e6-en&mimeType=pdf

79. Oficina C (2022a). Informe C: Inteligencia artificial y salud. Oficina de Ciencia y Tecnología del Congreso de los Diputados 2022; doi: https://doi.org/10.57952/tcsx-b678

80. Oficina C (2022b). Informe C: Ciberseguridad. Oficina de Ciencia y Tecnología del Congreso de los Diputados (Oficina C). 2022. doi: https://doi.org/10.57952/C8HY-6C31

81. ONU (2023). Secretary-General Urges Security Council to Ensure Transparency, Accountability, Oversight, in First Debate on Artificial Intelligence. SG/SM/21880 18 July 2023. https://press.un.org/en/2023/sgsm21880.doc.htm

82. Ortega, A. (2023). Europa corre, corre y se queda rezagada. Política Exterior. 19 de septiembre de 2023. https://www.politicaexterior.com/europa-corre-corre-y-se-queda-rezagada/

83. Patel, D., Ahmad, A., Xie, M. (2023). China AI & Semiconductors Rise: US Sanctions Have Failed. September 2023. https://www.semianalysis.com/p/china-ai-and-semiconductors-rise

84. Parkes, R. (2023). Europa necesita redescubrir el arte de la innovación política. Política Exterior. 27 de septiembre de 2023. https://www.politicaexterior.com/por-que-europa-necesita-redescubrir-el-arte-de-la-innovacion-politica/

85. Pérez-Martínez, F. (2023a). La Transformación Digital en los Nuevos Escenarios de Conflicto: del Campo de Batalla Digital al Campo de Batalla Inteligente. Discurso de toma de posesión como Académico de Número en la ACADEMIA DE LAS CIENCIAS Y LAS ARTES MILITARES. 8 de febrero de 2023. https://www.acami.es/wp-content/uploads/2023/02/Discurso-toma-posesion-Felix-Perez-Martinez.pdf

86. Pérez-Martínez, F. (2023b). Las Tecnologías Digitales y el Futuro Combate Inteligente. Foro 2E+I Ejército 35. Combate inteligente. Toledo. 4 de octubre de 2023.

87. Piqué, J. (2018). El mundo que nos viene. Ediciones Deusto (Centro libros PAPF). ISBN 978-84-234-2930-1. (5ª edición, septiembre 2022).

88. Reports, S. (2022). The supply chain that keeps tech flowing to Russia. Reuters. December 13, 2022. Retrieved February 6, 2023, from https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-tech-middlemen/

89. Sheehan, M. (2023). China's AI Regulations and How They Get Made. Working paper. REVERSE ENGINEERING CHINESE AI GOVERNANCE. © 2023 Carnegie Endowment for International Peace. July 2023.

90. Shidore, S. (2023). The Return of the Global South: Realism, Not Moralism, Drives a New Critique of Western Power. Foreign Affairs, August 31, 2023. https://reader.foreignaffairs.com/2023/08/31/the-return-of-the-global-south/content.html

91. SIA (2023). The 2023 SIA Factbook: Your Source for Semiconductor Industry Data Semiconductor Industry Association. May 05, 2023. https://www.semiconductors.org/the-2023-sia-factbook-your-source-for-semiconductor-industry-data/

92. Smit, S., Tyreman, M., Mischke, J., Ernst, P., Evers, M., Hazan, E., Novak, J., y Hieronimus, S. (2022). Securing Europe's future beyond energy: Addressing its corporate and technology gap. McKinsey Global Institute. May 2022.

93. Soares, S.R. (2023). Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age. The International Institute for Strategic Studies (IISS). August 2023. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/08/digitalisation-of-defence-in-nato-and-the-eu-making-european-defence-fit-for-the-digital-age.pdf

94. S&D (2023). S&D Group Strategy Paper on European Union Open Strategic Autonomy. Group of the Progressive Alliance of Socialists and Democrat in the European Parliament. Brussels, 6 February 2023. https://www.socialistsanddemocrats.eu/sites/default/files/2023-02/S%26D_Group_Strategy_Paper_on_European_Union_Open_Strategic_Autonomy_230206_0.pdf

95. SWD (2022). A Chips Act for Europe. Commission Staff Working Document. SWD (2022) 147 final. Brussels, 11.5.2022. https://data.consilium.europa.eu/doc/document/ST-8799-2022-INIT/en/pdf

96. Tierney, D. (2023). Why It's Good for Europe to Argue with America. Transatlantic Disagreements Make the World Safer. Foreign Affairs. September 11, 2023. https://www.foreignaffairs.com/united-states/why-its-good-europe-argue-america

97. Timmers, P. (2022). Strategic Autonomy Tech Alliances. Political-Industrial Collaboration in Strategic Technologies. EFPS policy brief. April 2022. https://feps-europe.eu/wp-content/uploads/2022/06/Strategic-Autonomy-Tech-Alliances.pdf

98. Torreblanca, J.I. (2023). Onwards and outwards: Why the EU needs to move from strategic autonomy to strategic interdependence. ECFR. 24 August 2023. https://ecfr.eu/article/onwards-and-outwards-why-the-eu-needs-to-move-from-strategic-autonomy-to-strategic-interdependence/

99. Tripathi, N. (2023). Can India truly become a global semiconductor hub? India Forbes. August 16, 2023. https://www.forbesindia.com/article/take-one-big-story-of-the-day/can-india-truly-become-a-global-semiconductor-hub/87349/1#:~:text=The%20current%20demand%20for%20semiconductors,global%20real%20estate%20services%20firm.

100. Tufail, A., Namoun, A., Alrehaili, A., Ali, A. (2021). A Survey on 5G Enabled Multi-Access Edge Computing for Smart Cities: Issues and Future Prospects. IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.6, June 2021. DOI:10.22937/IJCSNS.2021.21.6.1

101. Unión Europea (2022). Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales. Consejo de la Unión Europea. Bruselas, 21 de marzo de 2022 (OR. en) 7371/22. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf

102. UK (2023). Defence's response to a more contested and volatile world. Command Paper UK Ministry of Defence. Presented to Parliament by the Secretary of State for Defence by Command of His Majesty 18th July 2023. ISBN 978-1-5286-4291-0. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1171269/Defence_Command_Paper_2023_Defence_s_response_to_a_more_contested_and_volatile_world.pdf

103. UN (2020). Report of the Secretary-General Roadmap for Digital Cooperation. June 2020. https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

104. Van den Abeele, E. (2021). Towards a new paradigm in open strategic autonomy? Working Paper 2021.03. European Trade Union Institute. https://ssrn.com/abstract=3873798

105. Wieringen, K. (2022). Global Semiconductor Trends and the Future of EU Chip Capabilities. ESPAS Ideas Paper Series. European Strategy and Policy Analysis System. https://espas.eu/files/Global-Semiconductor-Trends-and-the-Future-of-EU-Chip-Capabilities-2022.pdf

106. Xiao, A. y Ding, Y. (2023). Evolution of China's Belt and Road Initiative: Digital Silk Road. INVESCO. March 1, 2023. https://www.invesco.com/apac/en/institutional/insights/fixed-income/evolution-of-chinas-belt-and-road-initiative-digital-silk-road.html

107. Yurchenko, O., Khmeleva, I., Mykytiuk, A. (2023). EU Sanctions against Russia: Coherence and Efficiency during the Large- Scale Invasion of Ukraine. A Ukrainian Assessment. With commentary by Maria Perrotta Berlin, Toms Rostoks, Vytautas Kuokštis & Rebecca Harding. SCEEUS GUEST REPORT. No. 11, 202310 May 2023. ©2023 Stockholm Centre for Eastern European Studies.

108. Zhang, Y., Han G., and Jürisoo, M. (2014). The geopolitics of China's rare earths: a glimpse of things to come in a resource-scarce world? Stockholm Environment Institute (2014) Stable URL: http://www.jstor.com/stable/resrep00363

ANEXO

SITUACIÓN DEL MARCO LEGISLATIVO DIGITAL DE LA UE

Iniciativas legislativas ya aprobadas y otras que se encuentran en el proceso de aprobación (en azul). Actualizado en agosto de 2023.

Instrumento legislativo	Año de aprobación/ presentación	Objetivo principal	Referencia
Reglamento General de Protección de Datos	2016	Soberanía digital	REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://data.europa.eu/eli/reg/2016/679/oj
Directiva NIS	2016	Soberanía digital	DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148
Directiva de protección de los consumidores	2019	Construcción del mercado interior	Directiva (UE) 2019/2161 del Parlamento Europeo y del Consejo de 27 de noviembre de 2019 por la que se modifica la Directiva 93/13/CEE del Consejo y las Directivas 98/6/CE, 2005/29/CE y 2011/83/UE del Parlamento Europeo y del Consejo, en lo que atañe a la mejora de la aplicación y la modernización de las normas de protección de los consumidores de la Unión. https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-81968
Ley de ciberseguridad	2019	Soberanía digital	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15

Directiva de Comercio electrónico	2020	Construcción del mercado interior	Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295
Ley de servicios digitales	2022 (plenamente aplicable a partir del 17 de febrero de 2024)	Construcción del mercado interior	Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81573
Ley de mercados digitales	2022	Construcción del mercado interior	Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81470
Reglamento General de Seguridad de productos	2021	Construcción del mercado interior	Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la seguridad general de los productos, por el que se modifica el Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo y se deroga la Directiva 87/357/CEE del Consejo y la Directiva 2001/95/CE del Parlamento Europeo y del Consejo COM/2021/346 final https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:346:FIN
Directiva de cargadores comunes	2022 (obligatorio en 2024)	Construcción del mercado interior	Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva 2014/53/UE, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos https://data.consilium.europa.eu/doc/document/ST-10713-2022-INIT/x/pdf
Directiva NIS 2.0	2020 (aprobada por el Parlamento Europeo el 11-11-2022)	Soberanía digital	Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM(2020) 823 final https://www.consilium.europa.eu/media/60338/st-10193-2022-init_x.pdf
Ley de gobernanza de datos	2022 (aprobada el 30 de mayo de 2022)	Soberanía tecnológica	REGLAMENTO (UE) 2022/868 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) http://data.europa.eu/eli/reg/2022/868/oj

Ley de chips	2023 (aprobada el 25 de julio de 2023)	Soberanía tecnológica	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act) COM/2022/46 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022AE1354&-qid=1663948354673
Ley de Datos	2022 (aprobada el 27 de noviembre de 2023)	Soberanía tecnológica	Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos) COM(2022) 68 final. https://data.consilium.europa.eu/doc/document/PE-49-2023-INIT/en/pdf
Ley de Inteligencia artificial (EN TRAMITACIÓN)	2021 (adopción de la posición común del Consejo el 22 de diciembre de 2022) (acuerdo de la Comisión del PE en mayo de 2023) Acuerdo político alcanzado en diciembre de 2023	Soberanía tecnológica	Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen Normas Armonizadas en Materia de Inteligencia Artificial (Ley De Inteligencia Artificial) y se Modifican Determinados Actos Legislativos de la Unión COM/2021/206 final https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206
Ley de Materias Primas Críticas (EN TRAMITACIÓN)	2023 (Comunicación de la Comisión Europea el 16 de marzo de 2023)	Soberanía tecnológica	REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO por el que se establece un marco para garantizar el suministro seguro y sostenible de materias primas fundamentales y se modifican los Reglamentos (UE) 168/2013, (UE) 2018/858, (UE) 2018/1724 y (UE) 2019/1020 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52023PC0160

ACERCA DEL AUTOR

GONZALO LEÓN SERRANO

Académico Correspondiente de la Sección de Ingeniería de la Real Academia de Doctores de España

Profesor emérito contratado. Catedrático de Ingeniería Telemática en la Universidad Politécnica de Madrid. Delegado del Rector para relaciones institucionales en Defensa.

Es miembro del Comité Ejecutivo del Foro de Empresas Innovadoras (FEI) y vicepresidente de la Fundación Círculo de Tecnologías para la Defensa y la Seguridad.

Es Académico correspondiente de la Academia de Artes y Ciencias Militares. Posee la Medalla al Mérito Militar.

En la UPM ha sido director de departamento, vicerrector de Investigación, adjunto al Rector para Alianzas para la Innovación y director del Centro de Innovación Tecnológica. Ha creado tres empresas tecnológicas con participación de la UPM y ha dirigido cuatro cátedras universidad empresa.

Ha sido secretario general de Política Científica, Subdirector General de Relaciones Internacionales en I+D, Subdirector de la Oficina de Ciencia y Tecnología en la Presidencia del Gobierno y Presidente del Comité Asesor de Grandes Instalaciones Científicas.

En los últimos cinco años ha sido Asesor en la Secretaría General de Investigación, representante español del Foro Estratégico de Cooperación Internacional del Consejo de la UE, presidente del Grupo de Trabajo UE-África en investigación e innovación de Foro Estratégico de Cooperación Internacional del Consejo de la UE y representante español en el Diálogo 5+5 con los países del Magreb y Sur de Europa.

Ha trabajado con la Comisión Europea como presidente del Grupo Asesor de Investigación Espacial, presidente del Grupo de Expertos sobre la Estrategia de Lisboa para la I+D, presidente del Grupo de Expertos en Infraestructuras de Investigación y presidente del Ejercicio de Aprendizaje Mutuo de Sinergias entre los Programas Marco y los Fondos Estructurales. Asimismo. Ha sido relator del G7 para infraestructuras de investigación en nombre de la UE. Consultor en nombre de la Comisión Europea en políticas de investigación e innovación de la UE para los gobiernos de Sudáfrica, México, Rumania, Eslovenia, Túnez y Marruecos.

Ha dirigido por parte de la UPM 14 proyectos de investigación de los programas marco de investigación e innovación de la UE y de la ESA, y participado en otros, ha dirigido 15 proyectos de investigación nacionales y regionales y más de 25 proyectos con el sector empresarial y las administraciones públicas. Ha sido responsable de innovación en el Proyecto "Human Brain" de la UE y coordinador del nodo español de la infraestructura de investigación sobre el cerebro humano (EBRAINS). Ha sido presidente de la Comisión de nuevas tecnologías del Instituto Español de Estudios Estratégicos (IEEE) del CESEDEN (Ministerio de Defensa).

MONOGRAFÍAS
DE LA
REAL ACADEMIA DE DOCTORES DE ESPAÑA

Real Academia de Doctores de España
San Bernardo, 49. 28015 Madrid publicaciones@rade.es 915319522
Contacto: Angela García Cascales


DOCTORES DEL
CLAUSTRO
EXTRAORDINARIO