ARTÍCULO ORIGINAL

Gobernanza dual de la inteligencia artificial. Retos tecnológicos y geopolíticos para la Unión Europea*

Dual governance of the artificial intelligence. Technological and geopolitical challenges for the European Union

Gonzalo León Serrano**
Académico Correspondiente de la Sección de Ingeniería de la Real Academia de Doctores de España
gonzalo.leon@upm.es

RESUMEN
El proceso de digitalización, apoyado en el valor dual (civil/militar) de los algoritmos de inteligencia artificial (IA), ha impulsado profundos cambios en la sociedad. Ello ha obligado a la Unión Europea (UE) a disponer de un marco geopolítico de actuación resiliente y realista basado en la mejora de su autonomía estratégica abierta y su soberanía tecnológica.
El artículo describe los problemas de la UE para mejorar su posicionamiento internacional en inteligencia artificial desde una visión multidimensional en el que los aspectos tecnológicos, los regulatorios, y su uso en el dominio de defensa y seguridad se imbrican en la geopolítica digital. El análisis comparado con los esfuerzos llevados a cabo por China y Estados Unidos en IA permite extraer las diferencias en planteamientos y actuaciones frente a los de la UE.
Finalmente, se aborda la fragmentación geopolítica de los mercados con trabas a importaciones y exportaciones de productos y servicios digitales ante los que la UE deberá complementar su enfoque regulatorio con interdependencias tecnológicas inteligentes con otros países

PALABRAS CLAVE: Unión Europea; Geopolítica; Gobernanza dual; Inteligencia artificial; Marco multidimensional.

ABSTRACT
The digitalization process, supported by the dual use (civil/defense) of artificial intelligence (AI) algorithms, has driven profound changes in society. This has forced the European Union (EU) to have a resilient and realistic geopolitical framework for action based on improving its open strategic autonomy and technological sovereignty.
The article describes the EU's problems to improve its international positioning in artificial intelligence from a multidimensional vision in which technological and regulatory aspects, and its use in defense and security domains are intertwined in digital geopolitics. The comparative analysis with the efforts carried out by China and the United States in AI allows us to extract the differences in approaches and actions compared to those of the EU.
Finally, it addresses the geopolitical fragmentation of markets with obstacles to imports and exports of digital products and services in which the EU will have to complement its regulatory approach with intelligent technological interdependencies with other countries.

KEYWORDS: European Union. Geopolitics. Dual governance. Artificial intelligence. Multidimensional framework.

* Sesión académica de la RADE celebrada el 29-11-2023 con el título *La tecnología y la innovación en el nuevo contexto geopolítico.* Situación actualizada a marzo 2023.

** Catedrático Emérito de la Universidad Politécnica de Madrid (UPM)

1.- CLAVES DEL PROCESO DE DIGITALIZACIÓN EN LA UE

1.1.- Relevancia estratégica

Desde el comienzo del siglo XXI la Unión Europea (UE) es consciente 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 y fortalecer o debilitar el papel de todos los países, incluida la UE, en su posicionamiento a nivel global.

Si la UE desea actuar en el contexto mundial como una gran potencia, debería afirmar ese carácter **dominando de forma efectiva un conjunto de tecnologías habilitadoras y emergentes frente a una competencia mundial creciente**, y haciendo que su marco de uso en la sociedad europea, 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, sea asumido por otras naciones.

El desarrollo tecnológico en las últimas décadas ha sido muy intenso en diversas disciplinas, pero es, sobre todo, en las últimas dos décadas cuando hemos asistido a un proceso acelerado de **"digitalización"** por el que la **penetración en la sociedad de productos y servicios digitales**, habilitado por el enorme desarrollo de la microelectrónica, aprovechando los avances en nanotecnología, ha **transformado nuestra sociedad**. En los años transcurridos del siglo XXI 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 la capacidad de los sistemas de defensa y seguridad, se han transformado profundamente.

En este proceso, el **valor de los datos** ha adquirido una creciente relevancia. Las capacidades disponibles para la captura o generación de datos, su protección, su intercambio masivo a alta velocidad a través de redes de comunicaciones terrestres, submarinas o satelitales, y las condiciones de acceso equitativo a los mismos, constituyen las **bases del funcionamiento de las cadenas de valor digitales globalizadas** cuyo control en una época convulsa como la actual es necesaria. Por este motivo, **asegurar la resiliencia en el intercambio de datos y su uso adaptado a unos principios y valores compartidos** se ha convertido en un factor geopolítico esencial dado que la sociedad actual depende, en gran medida, de asegurar ese flujo de información digital para asegurar su funcionamiento diario.

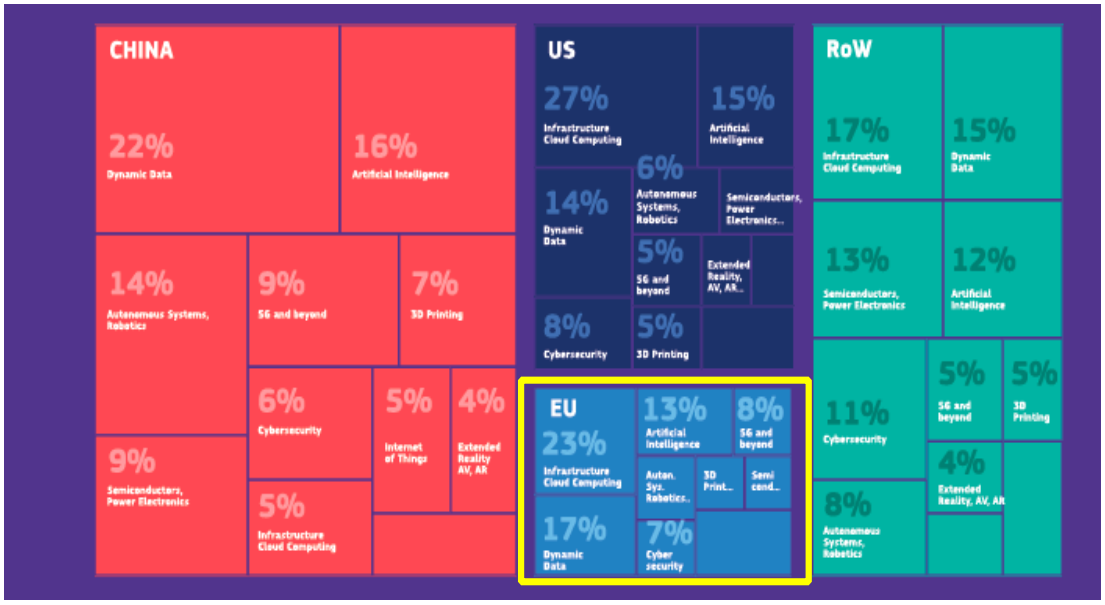

Figura 1. Posición comparada de la UE en el ámbito digital. Fuente: European Commission (2023b)

La **posición digital comparada de la UE en el contexto mundial del mercado TIC** que alcanzará los 6 trillones de euros en 2023, dista de ser la deseada, como se manifiesta gráficamente en la figura 1 extraída del informe sobre el estado de situación en 2023 del *Decenio Digital* europeo preparado por la Comisión Europea. Salvo en el ámbito de las infraestructuras y computación en la nube con un 23%, su peso relativo en otros ámbitos del mercado digital es bajo dificultando el que sus posiciones sean aceptadas o asumidas por el resto del mundo[1]. El esquema muestra también el gran peso que ha adquirido China en este sector.

Esta evolución y pérdida de relevancia ha provocado un profundo revulsivo en las políticas e instrumentos de actuación de la Unión Europea y sus estados miembros que han obligado a pensar en la **necesidad de disponer de un marco geopolítico de actuación más resiliente y realista basado en la mejora de la autonomía estratégica y la soberanía tecnológica de la Unión.**

1.2.- Autonomía estratégica abierta y soberanía tecnológica

La necesidad de **reafirmar la soberanía europea** se ha centrado en los últimos años en la búsqueda del óptimo posible de la denominada **autonomía estratégica abierta de la UE**,

[1] La participación de la UE en los ingresos mundiales en el mercado de las TIC ha disminuido drásticamente en la última década, pasando del 21,8 % en 2013 al 11,3 % en 2022, mientras que la cuota de los Estados Unidos aumentó del 26,8 % al 36 % (European Commission, 2023b)

entendida como (Damen, 2022) la *"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".*

Históricamente, **el concepto de autonomía estratégica apareció en el contexto de la defensa y la seguridad**, pero a partir de 2018 se empieza a extender a la intervención política para cubrir otras **muchas áreas que contribuyen a la seguridad** europea como son las políticas comerciales, de salud, de alimentación, de energía y de la propia estructura de las cadenas de provisión global.

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 factor de su carácter habilitador y por una tasa de evolución tecnológica muy rápida acompañada de un incremento de la penetración en la sociedad de productos y servicios digitales.

El objetivo de dominar (o conseguir el liderazgo) en un conjunto de tecnologías está estrechamente relacionado con el concepto de **"soberanía tecnológica"**. El Consejo Europeo de 2020 subrayaba 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*". No se trata de defender un enfoque autárquico, imposible y no deseable, sino de **reducir las interdependencias tecnológicas unilaterales.**

Una de las **definiciones de soberanía tecnológica** más empleadas es la formulada por el Instituto Fraunhofer (Alemania) en 2021 (Edler 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"*.

La autonomía estratégica y la soberanía tecnológica no son conceptos aislados. En la figura 2 se indica cómo la **autonomía estratégica** depende de alcanzar un nivel adecuado de **soberanía tecnológica** 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. La soberanía tecnológica (relativa) actúa como habilitadora de una mejora en la autonomía estratégica.

No debe olvidarse, sin embargo, que algunos países han pretendido en la historia reciente mejorar su autonomía estratégica en base a **adquisiciones desde el exterior de sistemas tecnológicos avanzados "llave en mano"** cuando disponían de recursos económicos no limitados y el coste de adquisición no era un problema. En mi opinión, ni siquiera en estos casos será posible garantizarlo porque las adquisiciones futuras estarán condicionadas a alianzas internacionales en un mundo más inestable. **Conseguir un mínimo de autonomía estratégica seguirá siendo esencial.**

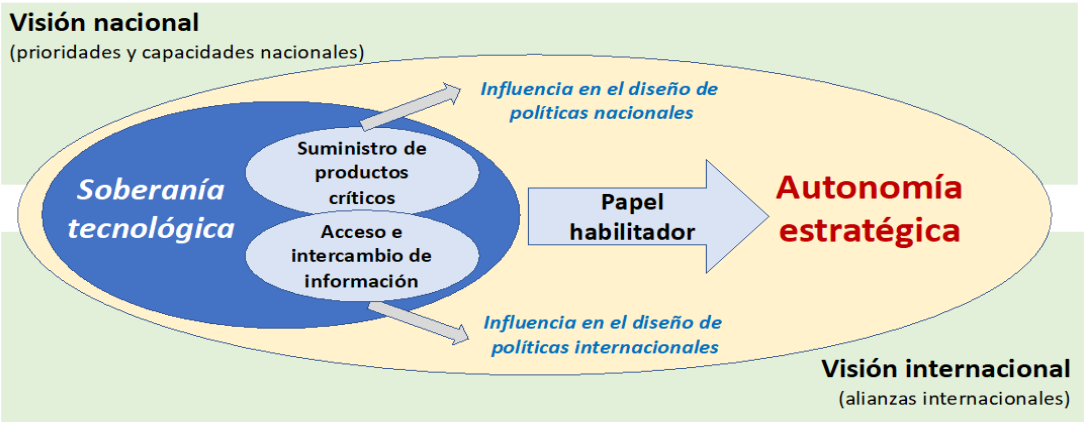

Figura 2. Relación entre autonomía estratégica y soberanía tecnológica en la UE.
Fuente: adaptada de León, G. 2023

En el **ámbito digital**, la UE se enfrenta a un **déficit de autonomía estratégica** en diversas áreas relacionadas no necesariamente disjuntas, pero que, al emerger de manera casi concurrente, se convierten en **puntos de fricción geopolítica** a los que debe hacerse frente:

- Dificultades de **acceso a materias primas** esenciales para múltiples dispositivos digitales como son las **tierras raras**, muy concentradas en China. Aunque la UE posee algunos yacimientos, el más importante en Suecia, la estricta regulación medioambiental europea y la presión ciudadana local puede hacer difícil su explotación.
- La dependencia de **cables submarinos de datos** para el funcionamiento de la sociedad europea (el 97% del tráfico de Internet internacional circula por ellos) que, en su mayoría, son propiedad de empresas privadas, y cuya seguridad está amenazada por roturas o atentados en aguas internacionales en los que la legislación es menos asertiva.
- La inexistencia de una **constelación europea de satélites de baja cota** que pueda ser empleada en aplicaciones de seguridad y defensa. El desarrollo de la constelación europea IRIS² no se completará antes de 2027-2028; mientras tanto, se depende de constelaciones operadas por otros países y empresas con sus propios intereses, no necesariamente alineados con los de la UE.

- Los condicionantes encontrados en el **despliegue de la tecnología móvil celular 5G** para no utilizar equipos de empresas muy ligadas a los gobiernos de países considerados competidores sistémicos como es el caso de Huawei y China, y reducir los potenciales riesgos de seguridad asociados. Esta situación puede ralentizar su uso y despliegue de 5G en la UE y hacerle perder la ventaja relativa que tenía frente a otras potencias.
- La escasa relevancia de la UE en la provisión de **servicios digitales proporcionados por plataformas digitales** (como las empleadas en redes sociales o comercio electrónico) en las que depende de grandes empresas ubicadas en Estados Unidos para el almacenamiento de datos personales e institucionales, y el acceso a servicios fundamentales para ciudadanos e instituciones europeas.

Aunque todos estos problemas en el dominio digital son muy relevantes y deben abordarse de manera sinérgica, el presente documento se centrará en un ámbito concreto del proceso de digitalización que ha adquirido una relevancia geopolítica notable en los últimos años: la **gobernanza de la inteligencia artificial.** Las siguientes secciones **enfatizan su carácter habilitador y dual y la forma en la que la UE debe responder** a ella para afirmar su papel en el mundo y, al mismo tiempo, **reforzar su autonomía estratégica.**

2.- RELEVANCIA DE LA INTELIGENCIA ARTIFICIAL EN LA AUTONOMÍA ESTRATÉGICA EUROPEA

2.1.- Carácter dual de las tecnologías digitales

Existen muchas áreas tecnológicas ligadas al proceso de digitalización en las que se está produciendo un fenómeno de **confrontación geopolítica** con impactos crecientes en el comportamiento de países, instituciones, y grandes empresas.

En algunos casos, se trata de asegurar el acceso a **tecnologías habilitadoras** que se incorporan a múltiples productos y servicios digitales; son las que, por este motivo, han suscitado una batalla competitiva global y provocado consecuencias geopolíticas notables. Actualmente, todas las áreas tecnológicas relacionadas con la digitalización emplean masivamente para el desarrollo de productos y servicios la **tecnología de semiconductores y la microelectrónica** (habilitada ésta, a su vez, por la nanotecnología) y, cada vez en mayor medida, el uso de **algoritmos de inteligencia artificial** para mejorar las prestaciones y funcionalidades de productos y sistemas digitales, ya sea empleando procesadores convencionales o especializados para gestionar eficientemente grandes conjuntos de datos en la ayuda a la toma de decisión.

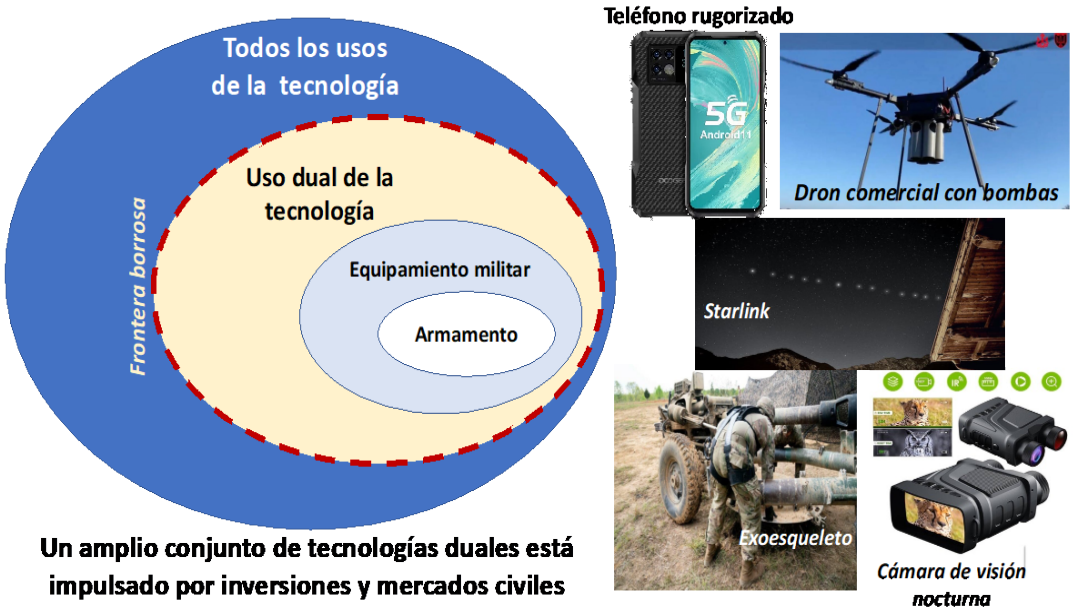

Figura 3. Tecnologías duales. Fuente: elaboración propia

Ambas tecnologías habilitadoras, **microelectrónica e inteligencia artificial,** muy relacionadas entre sí, **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, la propiedad intelectual, el uso de equipos de fabricación avanzados, algoritmos y dispositivos, así como el establecimiento de controles de importación y exportación. Esta dualidad de uso posee **fronteras borrosas que se expanden al ritmo en que lo hacen los conflictos híbridos** con zonas grises crecientes. En la figura 3 he querido señalar que, de todos los usos posible de una tecnología, un subconjunto cada vez mayor pertenece a su uso dual.

De estos usos duales, algunos se asocian a la aplicación de la tecnología para equipamiento militar, y un subconjunto aún más reducido al desarrollo de armamentos. A la derecha de la figura 3 se pueden ver algunos ejemplos de productos digitales surgidos del ámbito civil con aplicaciones duales en la actualidad: teléfonos móviles endurecidos, drones comerciales adaptados para el combate, uso de constelaciones satelitales para acceso a Internet como ocurre con Starlink en la guerra en Ucrania, uso de exoesqueletos inteligentes para mover grandes pesos, o empleo de cámaras de visión nocturna. No se pretende ser exhaustivo, existen muchos más casos.

El valor geopolítico que adquieren las **tecnologías duales** deriva de la necesidad del control de su uso con el fin de evitar su aplicación en sistemas militares por países potencialmente enemigos que les doten de superioridad en el campo de batalla. 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 (p.ej. armamento ligero) a los más complejos

(p.ej. 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 así actuar en función del objetivo y del contexto de forma dinámica (p.ej. variando la trayectoria de un dron o misil).

El reconocimiento de los peligros derivados de un acceso sin control por otros países ha conducido a la puesta en marcha de regulaciones aprobadas por países occidentales tecnológicamente avanzados como Estados Unidos, Australia, la UE, Japón, etc. que **limitan la exportación de dispositivos semiconductores o de los equipos que permitan fabricarlos** a países como Rusia, China, Corea del Norte, Irán, etc., para evitar que puedan usarse en el desarrollo de sistemas de armas. Todo ello, a pesar de que estas restricciones supongan también una **reducción del mercado potencial de las empresas de los países que las imponen**, y de las dificultades objetivas existentes para la efectiva **monitorización del cumplimiento** de las restricciones[2].

Focalizando la discusión en el caso de la **inteligencia artificial**, el crecimiento del **mercado de la IA es gigantesco** con un tamaño que en 2021 alcanzó los 87.000 millones de dólares, y que, previsiblemente, crecerá hasta los 1.597.000 millones de dólares en 2030 con un CAGR del 38,1 % de 2022 a 2030[3]. Esto hace que sea el **mercado civil** el impulsor fundamental del desarrollo actual de la inteligencia artificial, compatible con un **creciente interés en su adaptación a casos de uso militares**.

Al igual que su relevancia comercial, también ha crecido la **preocupación desde diversos ámbitos por el potencial mal uso de la IA** con un incremento de presiones a las autoridades, en algunos casos en tonos alarmistas, para que actúen de forma rápida. 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, es muy probable que, a medida que los modelos grandes de lenguaje (*Large Language Model, LLM*) mejoren sus prestaciones en la producción de texto que parezca auténticamente humano, y permitan la creación de contenido adaptado a las necesidades individuales de cada persona, serán capaces de **escribir correos electrónicos o videollamadas de "phishing" muy convincentes**. Será, sin duda, más difícil detectarlos y requieren no solo sofisticadas contramedidas, sino también una formación específica por parte de los usuarios.

[2] 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 de exportación efectivos.

[3] https://es.statista.com/estadisticas/1139768/inteligencia-artificial-vaolr-de-mercado/

Las mejoras en IA se suceden sin pausa: en 2022 el modelo de IA de Meta, denominado ***"Cicero"***, 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 en el que 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; **algunas de estas creaciones serían más tóxicas que cualquier arma química conocida**.

Un tercer ejemplo, ayuda a comprender el potencial impacto de la IA. Los avances obtenidos en los modelos de generación automática de código con IA podrían hacer posible producir *malware* con una experiencia mínima de programación. 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, recabar información, y seguir las instrucciones**.

Hacer frente a estos retos exigirá una gran **creatividad regulatoria** tanto de los responsables políticos como de los científicos, trabajando conjuntamente, que deberá equilibrarse con una estabilidad regulatoria en los mercados globales. Para algunos autores (Anderljung y Scharre, 2023) es solo cuestión de tiempo que sistemas de IA muy potentes y potencialmente peligrosos como los mencionados comiencen a extenderse, y **debemos asegurar que la sociedad esté preparada** para enfrentar los riesgos derivados, incrementando las habilidades formativas de la población y dotándose de herramientas tecnológicas y regulatorias.

En el fondo, **no es muy diferente de lo que ha habido que hacer en otros casos de tecnologías con alto grado de penetración social** como ha sido el caso del automóvil (regulación, formación, tecnología de control como cámaras y semáforos, etc.), pero ahora **deberá hacerse en plazos mucho más cortos.**

2.2.- Factores geopolíticos de la inteligencia artificial en la UE

Más allá de la capacidad de incremento de la funcionalidad de multitud de productos y servicios utilizando IA como corresponde a una tecnología habilitadora que ha penetrado en multitud de sistemas de usuarios, desde teléfonos móviles a sistemas de decisión empresarial o de gestión logística, el despliegue de sistemas de IA posee un valor creciente en la **discusión geopolítica global desde tres dimensiones complementarias: tecnológica, social, y de defensa y seguridad.**

La **dimensión tecnológica** en el desarrollo y penetración en la sociedad de la IA está ligada a otros dos ámbitos tecnológicos con interés geoestratégico que influyen y se ven influidos

por la IA: la tecnología de **microelectrónica y semiconductores**, y la captura y análisis de **grandes volúmenes de datos (*big data analytics*)**. Su convergencia permite la existencia de **sistemas autónomos interoperables potenciados por la IA.**

Las dos tecnologías citadas, aunque independientes en su concepción de la IA, tienen una clara sinergia con la IA en el desarrollo de productos y servicios avanzados. En el caso de la **tecnología de microelectrónica y semiconductores** esta relación se ve potenciada por la necesidad de ejecutar rápidamente algoritmos de IA para aplicaciones en tiempo real como puede ser las necesarias para el vehículo autónomo y también para (pre)entrenar eficientemente estos algoritmos. En estos casos, la opción más adecuada sería la del desarrollo de **circuitos integrados específicos para ejecutar algoritmos de IA de forma paralela** (p.ej. para análisis de patrones como sucede en el reconocimiento de imágenes) lo que hace que la evolución de la IA sea muy dependiente de los semiconductores y, por tanto, se encuentra ligada a los problemas geopolíticos en la fabricación y suministro de estos últimos.

El **manejo de los grandes volúmenes de datos necesarios para entrenar a los algoritmos de aprendizaje basados en redes neuronales** conlleva 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 para maximizar el paralelismo), y determinar cómo y en qué condiciones se pueden obtener estos datos de los usuarios. La rápida **emergencia de la inteligencia artificial generativa** ha incrementado las necesidades de entrenamiento[4].

Esta relevancia creciente 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*** cuyos chips de IA tipo tensorial como es el ***H100*** que integra *8 GPUs* y hasta *640 GB* de memoria están expresamente **diseñados para entrenamiento de algoritmos de IA y tareas de inferencia en centros de datos**. Las inversiones requeridas son enormes dado el coste de unos 40.000 dólares de Estados Unidos de cada uno de estos circuitos. La presión del mercado es tan elevada que, en noviembre de 2023, sólo un año después, ***Nvidia*** ha anunciado el chip ***H200*** duplicando la prestación del H100.

El valor en bolsa de ***Nvidia***, 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, Alphabet que superan los

[4] 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 a partir del acceso en grandes bases de datos o accediendo en línea a Internet.

1.000 billones de dólares. Su competidor en el mercado es la empresa ***AMD*** (Advanced Mico Devices) que lanzó al mercado en junio de 2023 el chip *MI300* para entrenamiento de algoritmos de IA, pero también grandes empresas como ***Intel***, ***Alphabet***, ***IBM***, ***Alibaba***, o ***Amazon Web Services*** han entrado en el mercado diseñando chips de IA específicos[5].

La segunda dimensión, **dimensión social** se apoya en 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), su grado de disrupción social fue muy elevado en base al desarrollo de aplicaciones que utilizan miles de millones de personas.

Ahora le toca el turno a la inteligencia artificial, apoyada en la microelectrónica y la gestión de grandes volúmenes de datos, la que va a adquirir una **dimensión social de carácter aún más disruptivo**. Los planteamientos estratégicos en IA por parte de las grandes potencias tecnológicas tendrán ganadores y vencedores durante el primer tercio de este siglo. Son, sobre todo, las condiciones de captura y uso de datos personales (como el análisis de datos faciales de millones de personas), su conversión en valor comercial, y su potencial uso como *"arma"* en conflictos híbridos, las que se asocian a condicionantes geopolíticos y en los que se centran las **incipientes regulaciones nacionales.**

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 la ***"inteligencia artificial generativa"*** en los últimos dos años es enorme. Esta tendencia se manifiesta en la forma en la que el fenómeno de ***ChatGPT*** de la empresa *Open AI* y otras similares han puesto de manifiesto en 2022 (alcanzando 100 millones de usuarios en sólo dos meses) y que las grandes empresas han empezado a incorporar a sus herramientas, como ha hecho Google en su buscador al incorporar la herramienta ***Google Bard*** (ahora sustituido por Gemini) que permite acceder a Internet para mejorar sus respuestas, y Microsoft al incorporar **ChatGPT** a su buscador ***Bing***.

[5] A ellas se han sumado en los últimos años nuevas empresas de hardware para IA con tecnologías avanzadas como SambaNova systems, Cerebras Systems, Groq o Graphcore. https://research.aimultiple.com/ai-chip-makers/

Finalmente, la relevancia de la **dimensión de defensa**, dado que la IA es inherentemente una tecnología de uso dual, procede de que su uso está **acelerando una carrera armamentística** para conseguir la superioridad potencial en el campo de batalla. De manera muy rápida se ha incorporado, junto a sistemas microelectrónicos, sensores y actuadores, en múltiples **sistemas de armas inteligentes** en una competición acelerada entre grandes potencias.

El desarrollo de los recientes y actuales conflictos armados ha permitido visibilizar el papel esencial de la IA en el desarrollo de múltiples **sistemas de armas de precisión inteligente** en las que se delega en algoritmos de IA decisiones operativas, y en su incorporación a sistemas de mando y control, o en sistemas de guerra electrónica. 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 existentes 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 o posición política ya sea a nivel individual como colectivo**. El posible uso de la **IA generativa** para la difusión de **noticias falsas o sesgadas** (generadas junto a texto, voz, imágenes, etc., creadas artificialmente y muy difíciles de detectar como sintéticas y no reales) genera un problema técnico de primer orden que está obligando a repensar el tipo de controles a realizar, y cómo trasladarlos a una regulación efectiva que no cercene el proceso innovador. Como ejemplo, la conocida distribución de un video falso del presidente de Ucrania Zelenski preparado por "hackers" rusos emitido en marzo de 2023 *"ordenando la rendición del ejército ucraniano".*

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. Para gestionar los peligros, algunos expertos han pedido una **pausa (moratoria) en el desarrollo de los sistemas de IA más avanzados**.

Dudo que se lleve a cabo puesto que estos modelos de IA son simplemente demasiado valiosos para que las entidades que invierten miles de millones de dólares en ellos congelen el progreso. Además, las moratorias propuestas para que dé 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 van a aplicarla, y supondría darles una ventaja decisiva.

Sin embargo, los **responsables de la formulación de políticas públicas pueden y deben ayudar a guiar el desarrollo del sector y preparar a los ciudadanos para mitigar sus**

efectos perniciosos. 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).

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 4 en la que las tres dimensiones mencionadas influyen y potencian la relevancia geopolítica de la IA.

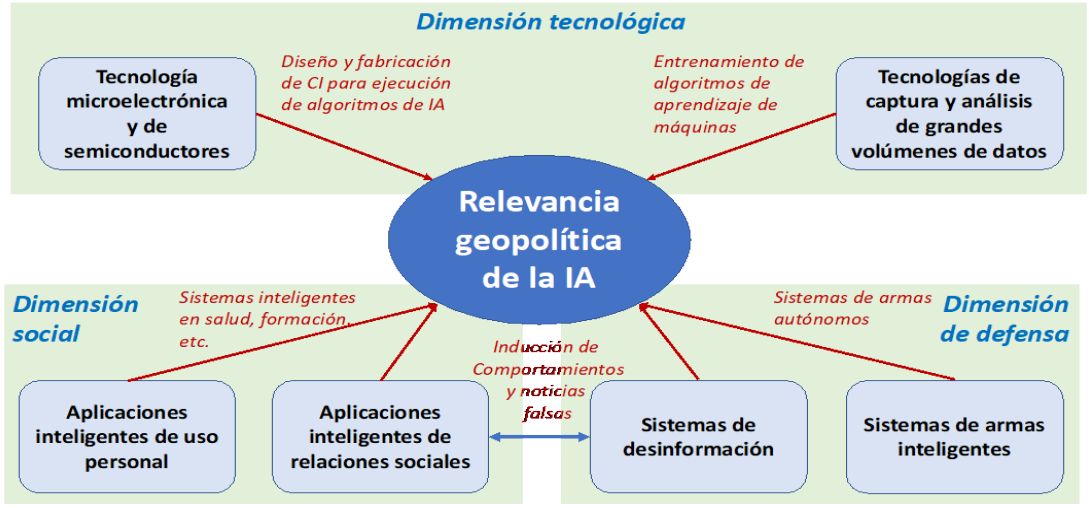

Figura 4. Relación entre las dimensiones coadyuvantes de la relevancia estratégica de la IA.
Fuente: elaboración propia

2.3.- Hacia un modelo de gobernanza de la IA

2.3.1.- Esfuerzos globales realizados

La evolución y penetración de la IA en múltiples dominios descrita en la sección anterior se ha producido en un plazo muy corto. No es extraño que, ante las consecuencias potenciales de la misma en la sociedad, se desee **buscar un consenso entre todas las partes interesadas para desarrollar un modelo de gobernanza de la IA que sea, a la vez, efectivo y eficiente**. Bremmer y Soleyman (2023) señalan que *"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"*. El "poder"

alcanzado por estas grandes empresas digitales con valoraciones bursátiles que superan el PIB anual de un país medio es enorme.

El **cambio de actitud a favor de una regulación de la IA** empieza a calar en gobiernos y organizaciones que han mantenido históricamente una actitud más orientada a la *"autorregulación"* por parte de los actores implicados. Sólo 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 independientemente, aunque debamos adoptar una actitud cautelosa sobre su posible éxito:

- 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 con un conjunto de directrices.
- 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** (ONU, 2023).
- En noviembre de 2023, organizada por el gobierno del Reino Unido, se celebra la **Cumbre de la Seguridad en IA** (AI Safety Summit 2023)[6] cuya *Declaración final*[7], aunque sea muy vaga, demuestra un interés creciente en abordar colectivamente (participaron 27 países y múltiples organizaciones y empresas) los riesgos derivados del uso de la IA.

A pesar de estos **esfuerzos de gobernanza multilateral de la IA** que tienen la virtud de reconocer el problema que plantea las aplicaciones de IA de alto riesgo, y elevar el debate por encima de los intereses particulares de países o empresas, **la responsabilidad actual sobre la gobernanza 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, de la ONU o de cumbres como la organizada recientemente por el gobierno del Reino Unido sean capaces de poner en marcha una gobernanza efectiva de la IA a tiempo en un momento en el que el desarrollo de modelos y aplicaciones se ha acelerado en todos los dominios. Aunque no deben despreciarse estos esfuerzos, **ninguna de estas iniciativas tiene capacidad operativa real** para obligar a los actores implicados, pero sí cumplen una función de **"foro de debate"** y, en el mejor de los casos, facilitarán llegar a conseguir acuerdos políticos muy generales.

[6] Los documentos de la Cumbre pueden encontrarse en: https://www.gov.uk/government/topical-events/ai-safety-summit-2023

[7] Bletchley Declaration: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-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 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 sólo un año y su distribución en productos por todo el mundo (sólo 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, como se verá en las siguientes secciones, han seguido rumbos diferentes.

2.3.2.- 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) 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:

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

La industria china de semiconductores, especialmente su industria de IA depende actualmente de estas dos empresas por lo que se verá indudablemente afectada[8]. También pueden ser afectadas en su negocio global las empresas de Estados Unidos como *Nvidia* ha avisado (Murgia et al., 2023). 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.

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.

En el caso de los Estados Unidos ya se levantan voces argumentando que un modelo de gobernanza de la IA basado en 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. 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").

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 se tomara la seguridad de la IA 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.

Un paso decisivo hacia la respuesta solicitada ha sido la aprobación el 30 de octubre de 2023 por la administración Biden de una ***Orden ejecutiva* sobre la inteligencia artificial**[9]

[8] 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/

[9] https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

enfatizando la necesidad de disponer de una **IA confiable y segura**. El objetivo, como se expresa en el mismo documento: *"establece nuevos estándares para la seguridad de la IA, protege la privacidad de los estadounidenses, promueve la equidad y los derechos civiles, defiende a los consumidores y trabajadores, promueve la innovación y la competencia, promueve el liderazgo estadounidense en todo el mundo y más."* Será necesario esperar a ver cómo se promueven todas las previsiones incluidas que siguen teniendo un enfoque de *"directrices voluntarias".* No creo que sea suficiente.

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 particular, 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 GDRP (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 sobre la IA, 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).

Las regulaciones siguen un doble y simultáneo proceso de desarrollo: un **marco político** que conduce a la aprobación por el Partido Comunista de China, y un **marco de impacto tecno-económico** no limitado exclusivamente a China, sino también a su impacto en otros países en desarrollo influidos por China (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**[10]. 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. Adaptación similar a lo que les sucede para comercializar sus servicios en la UE.

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[11].

Parte de esta postura procede no solo de la importancia en los mercados globales, sino 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 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**. 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

[10] 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).

[11] El anuncio por Huawei en septiembre de 2023 del lanzamiento de su nuevo teléfono inteligente *Mate 60* con soporte a redes 5G fabricado en China por la empresa *SMIC* en tecnología de 7 nanómetros, implica que ha logrado un nivel de miniaturización para el que es necesario un equipo especial de litografía al que China, en un principio, no tiene acceso. ¿Son efectivas las restricciones de exportación de tecnología?

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 alcanzar 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.

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. 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).

En definitiva, **no será sencillo establecer una gobernanza global de la IA duradera** si persiste un clima de confrontación tecnológica geopolítica como el actual.

2.3.3.- 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**.

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 comunitarios (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**"* 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 Europeo 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".*

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"[12] (European Commission, 2021b). 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**[13]**.** Este enfoque no será sencillo de aplicar en la práctica porque **supone un análisis individualizado de las aplicaciones de IA** y las fronteras entre niveles de riesgos no son nítidas (Marcus, 2023).

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".*

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".* Contrasta en este sentido con lo que sí se permite en China.

La clasificación como **alto riesgo** conlleva el análisis del potencial lesivo en la salud y la seguridad o los derechos fundamentales de las personas, y las finalidades para las que se contempla su uso. Estos sistemas estarán sujetos a obligaciones estrictas antes de que puedan comercializarse. Los **sistemas de IA considerados de alto riesgo en el Reglamento europeo** en discusión abarcan las tecnologías de IA empleadas en:

[12] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0206

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

- *Infraestructuras críticas (por ejemplo, transportes), que pueden poner en peligro la vida y la salud de los ciudadanos;*
- *Formación educativa o profesional, que pueden determinar el acceso a la educación y la carrera profesional de una persona;*
- *Componentes de seguridad de los productos (ej. aplicación de IA en cirugía asistida por robots);*
- *Empleo, gestión de trabajadores y acceso al trabajo por cuenta propia (ej. programas informáticos de clasificación de CV);*
- *Servicios públicos y privados esenciales (ej. sistemas de calificación crediticia que priven a los ciudadanos de la oportunidad de obtener un préstamo);*
- *Aplicación de las leyes, que pueden interferir con los derechos fundamentales de las personas (ej. evaluación de la fiabilidad de las pruebas);*
- *Gestión de la migración, el asilo y el control de las fronteras (ej. comprobación de documentos);*
- *Administración de justicia y procesos democráticos*

La valoración del esfuerzo regulatorio europeo en IA debe contemplarse en el contexto de un **esfuerzo más amplio en el ámbito digital** como se indica en la figura 5, aún no concluido. Algunas de estas regulaciones también alcanzan a la IA desde diversas perspectivas.

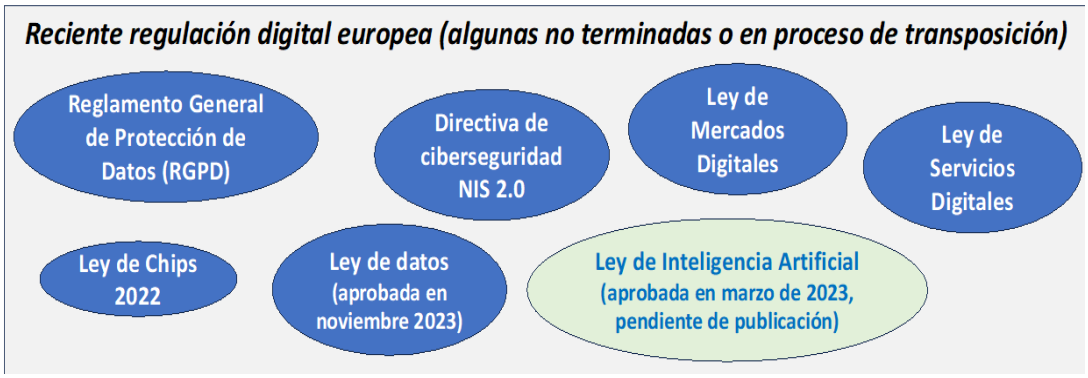

Figura 5. Esfuerzo regulatorio de la UE en el ámbito digital. Fuente: elaboración propia

El proceso de negociación de la Regulación de la IA 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. 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.

Finalmente, se ha alcanzado un acuerdo en marzo de 2024, pendiente de su revisión lingüística y publicación, 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.

Teniendo en cuenta que la Ley de IA que 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 aprobada 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 (LLM) 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 LLM es de alto riesgo, independientemente de lo que se haga con ella, y otra sería ir caso a caso (inviable).

El riesgo anunciado es que, 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 técnicos y legales para hacerlo, **en contra de las PYMES que tendrán más dificultades para obtenerlas y poder entrar en el mercado a tiempo**.

En resumen, será necesario, en mi opinión, que la UE basado en el **equilibrio alcanzado** en la redacción final 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[14].

[14] *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

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* (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****…. Tenemos la intención de ampliar 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.".*

2.3.4.- Control del desarrollo y acceso a chips de IA y sistemas de supercomputación

Ya se ha indicado anteriormente que existe una relación estrecha entre la microelectrónica y el desarrollo de la IA. Por este motivo, los esfuerzos de mejora de la autonomía estratégica de la UE en semiconductores son muy relevantes. Desgraciadamente, con solo un **9% del mercado mundial de semiconductores en 2022** como se indica en la figura 6, la UE tiene una capacidad de influencia global limitada.

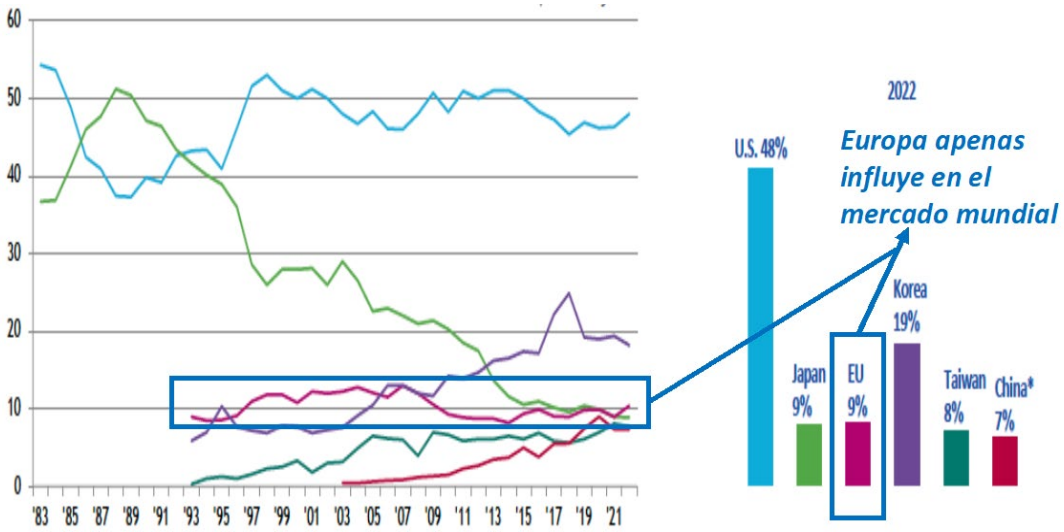

Figura 6. Mercado mundial de semiconductores. Fuente: SWD (2022)

A esta situación se suma el que no se dispone en la UE de capacidades de fabricar dispositivos y circuitos integrados comerciales con resoluciones inferiores a 10 nm

redactarse "*en cuestión de semanas*". https://www.reuters.com/technology/eu-tech-chief-calls-voluntary-ai-code-conduct-within-months-2023-05-31/

cuando las más avanzadas se acercan a los 2 nm[15]. Las fábricas ("*foundries*") de semiconductores más avanzadas, su peso relativo, y su concentración geográfica indican una relevancia de China, Taiwán y Corea del Sur.

La UE sí ocupa una **posición privilegiada en el desarrollo de equipos para la fabricación de dispositivos semiconductores** de menos de 5 nm a través de la empresa ***ASML*** propietaria de una tecnología de fotolitografía extrema, aunque ASML no pueda vender sus equipos más avanzados a China debido a las restricciones impuestas por Estados Unidos dado su carácter dual.

De la figura 6 puede extraerse la conclusión de que **la UE necesita importar todo tipo de circuitos integrados avanzados, entre ellos los de IA o los empleados en supercomputadores,** para poder emplearlos en el desarrollo de los sectores tecnológicos más competitivos.

Tampoco es mejor la situación europea en relación con los ***supercomputadores[16]***. Desde hace años se desarrolla una ***"competición 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. Estados Unidos, la UE, Japón y China, cuatro grandes potencias tecnológicas, compiten en disponer de los **supercomputadores más potentes** que ya superan 1 Exa-FLOP (10^{18} o un trillón de operaciones de punto flotante por segundo)[17].

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**. Concretamente, la necesidad de **entrenar a algoritmos de inteligencia artificial** basados en **modelos grandes de lenguaje** empleando un volumen muy elevado de datos ha dado a los supercomputadores una relevancia aún mayor de la que ya tenían en otros múltiples dominios de aplicación (p.ej. predicción meteorológica, modelos climáticos, análisis molecular).

[15] Para hacerse una idea, el chip de IA de *Nvidia* anunciado en noviembre de 2023, H200, ha sido realizado en tecnología de 4 nm y fabricado en Taiwán por TSMC.

[16] A los ordenadores más potentes en cada momento se les ha denominado históricamente "supercomputadores" y a las tecnologías informáticas que permitían desarrollar estos equipos "computación de altas prestaciones" ("*high performance computing", HPC*). Obviamente, lo que hace veinte años era denominado "supercomputador" tiene poco que ver con lo que es ahora.

[17] Aunque China decidió en 2018 no presentar los datos de sus supercomputadores para evitar sanciones de Estados Unidos, diversos informes indican que el nuevo supercomputador chino **New Generation Sunway** parece haber superado al *Frontier* americano que es el supercomputador más rápido del planeta según el ranking Top500.

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). Para **entrenar modelos de IA generativa**, las organizaciones suelen confiar en centros de datos a gran escala equipados con una potente infraestructura de hardware y redes. Estos centros de datos albergan numerosos servidores y aceleradores de hardware especializados, como unidades de procesamiento gráfico (GPU) o unidades de procesamiento tensorial (TPU), que están optimizadas para cargas de trabajo de IA.

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 Exa-FLOPS. CG-1[18], está en funcionamiento desde julio de 2023 y se encuentra ubicado en Santa Clara, California.

El supercomputador ***Condor Galaxy 1*** se ha diseñado específicamente para grandes modelos lingüísticos e IA generativa y, previsiblemente, aparecerá a final del año 2023 en el primer lugar del TOP500 (ranking de supercomputadores). 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.

Los datos que se han publicado respecto a las necesidades de computación para el entrenamiento de diversos algoritmos de IA muestran la enorme dependencia de capacidades exponenciales de cálculo medida en FLOPS. Como ejemplo, la capacidad de cálculo utilizada para entrenar a Minerva, una IA que puede resolver problemas matemáticos complejos, es casi **6 millones de veces mayor** que la que se usó para entrenar AlexNet hace 10 años.

La evolución en el tiempo de los recursos de computación empleados para el entrenamiento de algoritmos de IA queda de manifiesto. Los últimos, ligados a la IA generativa, ya superan los 10^{24} operaciones en punto flotante.

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[19] en septiembre de 2023 es la de permitir a las start-ups europeas

[18] https://www.cerebras.net/blog/introducing-condor-galaxy-1-a-4-exaflop-supercomputer-for-generative-ai/
[19] https://techcrunch.com/2023/09/13/eu-supercomputers-for-ai/

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).

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 también 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 del software de gestión del mismo.

El 13 de octubre de 2022 el gobierno de Estados Unidos impuso nuevos controles a la exportación de circuitos integrados de computación avanzada a China, productos informáticos que contengan dichos circuitos y ciertos artículos de fabricación de semiconductores. Específicamente, se aborda el control de exportaciones a China para el caso de los **supercomputadores que superen los 100 Peta-FLOPS** (1 PetaFLOP significa 10^{15} operaciones de punto flotante por segundo) **a 64 bits en un determinado espacio físico** (generalmente, máquinas situadas en un 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 al *"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* l*a 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 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 regulación de exportación.

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

3.- LA INTELIGENCIA ARTIFICIAL EN EL SECTOR DE LA DEFENSA

3.1.- De la Evolución de la política digital de defensa en la UE

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 la **Política Común de Seguridad y Defensa (PCSD)** de la UE, especificando los objetivos principales[20].

Nada de eso se hizo realidad. La ambición política 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 Europa o próximos geográficamente 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.

El objetivo de autonomía estratégica en defensa ha vuelto a relanzarse recientemente con la creación de ***PeSCO*** (*Permanent Structured Cooperation*) complementado por la creación del **Fondo Europeo de Defensa** (**FED)** o el **Fondo Europeo de Apoyo a la Paz (FEAP)** aprobado en 2021, empleado en el apoyo a Ucrania, incrementan la visibilidad hacia el ciudadano 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"***[21] (Unión Europea, 2022) (EEAS, 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

[20] Entre ellos el 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.

[21] 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.

Estados miembros en reforzar su compromiso militar para construir una Europa de la defensa, especialmente tras la invasión rusa de Ucrania.

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 la estrategia contenida en la "***Brújula Estratégica***" (*Strategic Compass*) (Soares, 2023). 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 (IISS, 2022).

Al proceso de digitalización de la UE 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 despliegue de tecnologías y aplicaciones en 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 presente contribución. 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 puede 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[22]. La Comisión Europea (CE), el EUMC y la **Agencia Europea de Defensa** (AED) están trabajando activamente en diferentes aspectos

[22] 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.

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.

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.

Este proceso de reforzamiento de la política de defensa europea hacia una mayor autonomía estratégica no será efectiva si no se produce una **aceleración en la adopción de tecnologías emergentes y disruptivas en las fuerzas armadas de los países europeos** y, sobre todo, aquéllas ligadas con el proceso de digitalización. Ello no solo debe implicar el incremento de recursos presupuestarios para la adquisición de sistemas militares, sino incrementar las capacidades de la industria de defensa europea. La **adquisición de sistemas avanzados de armas procedente de países no europeos** mejorará, sin duda, las capacidades operativas en defensa de la UE, pero **no ayuda a mejorar la soberanía tecnológica europea**[23]. ¿Cómo actuar a largo plazo?

Desde un punto de vista tecnológico, existe un amplio acuerdo de que la **digitalización 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. A ello contribuye la **confluencia de múltiples tecnologías en el campo de batalla**, de diferentes generaciones tecnológicas, que está haciendo que la obtención de datos en tiempo real de múltiples sensores y su integración en sistemas de armas haya adquirido una relevancia fundamental.

También es un fenómeno imparable la **incorporación de la inteligencia artificial** en la toma de decisiones. De esta manera, se está produciendo una **transición tecnológica** en la 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

[23] Suele ser habitual que las condiciones establecidas para las adquisiciones de equipamiento militar de otros países, además de exigir autorización gubernamental, restrinjan fuertemente el acceso a la tecnología adquirida cuya evolución durante el ciclo de vida del sistema depende del país productor.

individual al del planeamiento de operaciones del estado mayor empleando algoritmos de IA capaces de coordinar e integrar la información relevante a cada nivel.

Otro factor relevante es que, hoy en día, **el desarrollo de un gran conjunto de tecnologías de doble uso está impulsado por inversiones civiles y por la evolución de los mercados internacionales**, salvo en unos pocos casos. Este hecho implica que la adaptación a usos militares de tecnologías digitales aparece en una segunda fase cuando las tecnologías ya han demostrado su viabilidad y posibles usos en sistemas civiles disruptivos.

La consecuencia es que **el proceso de transformación digital en los ámbitos militares es más lento y arriesgado que en los ámbitos civiles**. Los sistemas militares deben trabajar en condiciones muy duras, su tolerancia al fallo es muy pequeña, deben coexistir con sistemas heredados de tecnologías menos avanzadas, y tienen ciclos de vida mucho más largos que los empleados en el mundo civil; en consecuencia, la adopción de una tecnología digital en el ámbito militar sucede con posterioridad en comparación con la adopción de una tecnología digital similar en el contexto civil.

Los **casos de uso** en el ámbito de la defensa están madurando rápidamente, lo que conduce a pensar en la mejor forma en que podrían integrarse de forma efectiva en las operaciones militares. La figura 7 muestra varios tipos de aplicaciones duales en las que la tecnología de IA está transformando el uso de la defensa, incluso cuando los ejemplos mostrados en la figura estén lejos de estar completamente maduros y se trate de experiencias en evaluación. En todos esos casos de uso, se están probando diversos prototipos con usuarios finales. Si madurasen, podrían emerger en el campo de batalla en los próximos años.

Como ha ocurrido repetidamente en la historia de la humanidad, **los conflictos armados prolongados aceleran este proceso de cambio** puesto que los bandos combatientes se ven "obligados" a reducir los criterios de precaución y acelerar los procedimientos administrativos de adquisición y despliegue en comparación con lo que ocurre en tiempos de paz.

- El enorme y rápido impacto de la **IA generativa** podría utilizarse no solo para la generación de contenidos (texto, imágenes, vídeo) de forma similar a como se hace en los mercados civiles, sino también para la generación automática de escenarios o datos sintéticos para la guerra electrónica. También será útil para ejecutar *"gemelos digitales"* más realistas de escenarios de combate.
- **Los enjambres colaborativos de drones** para detectar y rastrear objetivos militares en un entorno representativo en tiempo real son posibles con la IA. Acelerar el desarrollo de estas tecnologías tendrá un impacto masivo en la capacidad militar de la coalición**.**

- **El análisis de imágenes en tiempo real** es hoy en día una de las aplicaciones típicas de la IA para el reconocimiento de rostros u objetos en combinación con la captura de fotos o vídeos desde una cámara terrestre o en satélites.
- **La robótica inteligente** avanza hacia una nueva generación de robots empáticos con comportamientos impulsados por IA. La comunicación en equipos híbridos (humano/robot) sería una tendencia fascinante si se resolvieran los problemas técnicos y se lograse una interacción más realista y sofisticada con los humanos.
- **El control cerebral de dispositivos** como los drones es posible con el uso de técnicas de neuroestimulación no invasivas. Su uso está pasando de pacientes en hospitales a personas sanas en uso específico en operaciones militares.
- **La evaluación inteligente de las condiciones físicas/psicológicas** del personal militar en misiones es una de las aplicaciones de la IA en medicina que se está trasladando al análisis en tiempo real de pilotos u otro personal militar en operaciones críticas.

La figura 7 representa esquemáticamente alguno de estos usos.

Figura 7. Usos innovadores de la IA en el ámbito de la defensa. Fuente: elaboración propia

Muchos de estos casos de uso se ven facilitados por el rápido desarrollo de sistemas de IA impulsados por el uso de circuitos integrados de IA específicos, que son necesarios para entrenar y ejecutar complejos algoritmos de redes neuronales de manera eficiente. El

acceso a chips avanzados de IA se ha convertido en una cuestión geopolítica en la que las grandes potencias están imponiendo restricciones a la exportación.

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 para IA 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 en tiempo real y a incrementar la capacidad de análisis de estos datos** se ha convertido en un componente crítico de la capacidad de combate.

El compromiso de llevar a cabo esta transformación digital se ha reforzado en la **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.

En mi opinión, **la UE se juega en esta década reafirmar su soberanía tecnológica en defensa** como base de su deseada autonomía estratégica o depender, en el supuesto de que existan recursos económicos, de adquisiciones de sistemas de otros países**. ¿Estamos dispuestos a realizar el esfuerzo necesario para ello?**

4. CONCLUSIONES

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 posicionamiento de todos los países en su continua búsqueda de la autonomía estratégica, digital en este caso.

De hecho, 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 desde el siglo XX, 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.

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** con trabas crecientes a las importaciones y exportaciones de productos y servicios tecnológicos no beneficia a la UE que depende para su crecimiento de la existencia de **mercados abiertos**. Deberá saber conciliar este planteamiento con una política sostenida de **interdependencias tecnológicas inteligentes** en un marco de **maximización realista de su autonomía estratégica**.

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**

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.**

5.- 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. 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
3. 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).

4. 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).

5. 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%20the%20Balance%20of%20Power,%20PRIO%20Paper%202022.pdf

6. CBInsights (2023). Generative AI Bible. The ultimate guide to genAI disruption. CBInsights. November 2023.

7. 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

8. 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.

9. EEAS (2022). A Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

10. 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

11. 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

12. 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

13. EUROPEAN COMMISSION (2023b). Report on the State of the Digital Decade. 29 September 2023. https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade

14. G7 (2023). G7 Hiroshima Leaders' Communiqué May 20, 2023. https://www.g7hiroshima.go.jp/documents/pdf/Leaders_Communique_01_en.pdf

15. IISS (2022). 'Defence Innovation and the European Union's Strategic Compass', IISS Strategic Comments, vol. 28, no. 10, 30 May 2022.

16. 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/

17. 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

18. 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

19. 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

20. 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

21. 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

22. 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

23. 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

24. 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/

25. 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

26. 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/

27. PÉREZ-MARTÍNEZ, F. (2023). Las Tecnologías Digitales y el Futuro Combate Inteligente. Foro 2E+I Ejército 35. Combate inteligente. Toledo. 4 de octubre de 2023.

28. 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.

29. 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

30. SWD (2002). COMMISSION STAFF WORKING DOCUMENT A Chips Act for Europe. SWD (2022) 147 final - PART ¼. Brussels, 12 May 2022.

31. 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