Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Laurent Chrzanovski
Profesor Universidad de Sibiu (Rumania),
Profesor Visitante Universidades de Ginebra (Suiza),
Lyon (Francia) y Varsovia (Polonia)

Stephane Mortier
Profesor asociado Université Gustave Eiffel (Laboratorio DICEN - Dispositivos de información y comunicación en la era digital), y
Centro de Investigación Gendarmería Nacional Francesa (CREOGN)

LA DICOTOMÍA DE LOS USOS DE LA INTELIGENCIA ARTIFICIAL EN SEGURIDAD NACIONAL

LA DICOTOMÍA DE LOS USOS DE LA INTELIGENCIA ARTIFICIAL EN SEGURIDAD NACIONAL

Resumen (Es): La inteligencia artificial es probablemente el vector más importante de la transformación de la seguridad y la aplicación de la ley. La necesidad de seguridad responde a la defensa de los intereses fundamentales de los Estados. ¿Cómo proteger estos intereses con herramientas y tecnologías de inteligencia artificial frente a los Estados extranjeros? Más allá de las grandes potencias estatales, es necesario abordar el entorno económico de la inteligencia artificial. Los principales actores en el desarrollo de la inteligencia artificial en el mundo son las mayores empresas tecnológicas: GAFAM (Google, Apple, Facebook-Meta, Amazon, Microsoft) y BATHX (Baidu, Alibaba, Tencent, Huawei, Xiaomi). La realidad es que su capacidad de influencia va más allá de las fronteras de Estados Unidos o China y su poder no se limita a las empresas, sino que se extiende a los Estados, las ONG y las organizaciones internacionales y regionales. Esta hegemonía es una realidad también en Europa. La mayoría de los países de la UE tienen el *modus vivendi* grecorromano que exige nuevas leyes antes de la aplicación de cualquier novedad en un tribunal. En un mundo en el que cada día aparecen nuevas tecnologías, aplicaciones y programas informáticos, ya no tenemos tiempo para eso.

Abstract (En): Artificial intelligence is probably the most important vector of security and law enforcement transformation. The need of security is a response to the defense of fundamental interests of states. How to protect these interest with artificial intelligence tools and technologies from foreign states? Más allá de las principales potencias estatales, es necesario abordar el entorno económico de la inteligencia artificial. The main players in the development of artificial intelligence in the world are the largest technology companies: GAFAM (Google, Apple, Facebook-Meta, Amazon, Microsoft) and BATHX (Baidu, Alibaba, Tencent, Huawei, Xiaomi). The reality is that their capacity to influence extends beyond the borders of the United States or China and their power is not limited to companies, but extends to States, NGOs, international and regional organizations. This hegemony is a reality also in Europe.

Most of the EU countries have the graeco-roman "modus vivendi" that requires new laws before the implementation of any single novelty in a court. In a world where new technologies, apps, softwares, appear on a daily base, we have no more time for that.

Palabras clave: inteligencia artificial, seguridad, intereses fundamentales, dependencia.

Keywords: Artificial intelligence, security, fundamental interests, dependency.

1.- INTRODUCCIÓN

En 1996, Francis Heylighen y Johan Bollen, de la Vrij Universiteit Brussel (VUB), presentaron en un artículo titulado «The World Wide Web as Super-Brain: from Metaphor to Model» («La "world wide web" como supercerebro: de la metáfora al modelo») algunas propuestas interesantes sobre el desarrollo del «supercerebro» y lo que le permite aprender, sin dejar de señalar que no es el cerebro en sí el que piensa, sino los usuarios de la red. Es más, el poder de este «supercerebro» reside en el tenue vínculo con sus usuarios, un vínculo autorreferencial. Asimismo, se han desarrollado algoritmos que (por analogía con el cerebro humano) fortalecen los vínculos y debilitan los que se utilizan con menos frecuencia. Mediante el principio de transitividad, se puede automatizar la construcción de nuevos enlaces. Pero nada de esto significa que este «supercerebro» pueda pensar en realidad de forma independiente de los usuarios que lo componen (Mortier, 2019). Hoy en día, se dan las condiciones para una evolución generalizada de las técnicas de inteligencia artificial: disponibilidad y diversidad de datos, desarrollo de ofertas y rendimiento de los dispositivos y equipos de TI (Marellin, 2021).

En este documento, emplearemos el concepto de inteligencia artificial y sistema de inteligencia artificial tal como los define el Parlamento Europeo[1]: «La inteligencia artificial (IA) es la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear. La IA permite que los sistemas tecnológicos perciban su entorno, gestionen estas percepciones, resuelvan problemas y actúen con un fin específico. La máquina recibe datos (ya preparados o recopilados a través de sus propios sensores, por ejemplo, una cámara), los procesa y responde a ellos. Los sistemas de IA pueden adaptar su comportamiento en cierta medida, analizar los efectos de acciones previas y trabajar de forma autónoma».

La inteligencia artificial (IA) presenta enormes posibilidades para optimizar la lucha contra la delincuencia y fortalecer la seguridad nacional. En condiciones de acumulación inconcebible de información y de necesidad de tomar decisiones rápidas, solo el uso de la IA puede llevar al éxito. La inteligencia, la contrainteligencia, la ciencia forense, la lucha contra la delincuencia organizada, el rápido tratamiento de la información disponible, el esbozo de distintas decisiones, la elaboración de planes y escenarios multivariantes y la ejecución de diversos análisis es un proceso que lleva mucho tiempo. Únicamente su uso puede reducir significativamente este tiempo y, por tanto, aumentar drásticamente las posibilidades de detección, prevención y limitación de

[1] https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa

los delitos (Radulov, 2019). En resumen, la inteligencia artificial (IA) y el aprendizaje automático (AA) pueden ser una gran estrategia de ciberdefensa y también un arma de doble filo (Meghani, Essomba, Chrzanovski, 2023).

La inteligencia artificial es y será cada vez más indispensable para la seguridad nacional. Es impensable excluir esta tecnología de las estrategias de seguridad. Cada vez más, los servicios del Estado utilizan herramientas de inteligencia artificial, tanto para las investigaciones judiciales como en la policía administrativa o la inteligencia policial. Por ejemplo, la Gendarmería Nacional francesa ha desarrollado una «plataforma de inteligencia artificial» que recibió el Premio Europol a la Excelencia en Innovación en 2022. Esta plataforma de IA proporciona a sus usuarios un conjunto de herramientas avanzadas de análisis de delitos, desarrolladas específicamente para satisfacer las necesidades de los investigadores a la hora de procesar información sobre delitos. Incluye una herramienta de comparación de textos, detección de objetos a partir de imágenes (armas y drogas), transcripción de voz a texto, extracción de entidades y herramientas de traducción automática en más de 100 idiomas[2]. En Europa, el proyecto AIDA (2020-2023), financiado con fondos europeos, se centra en la ciberdelincuencia y el terrorismo, para lo cual aborda problemas específicos aplicables a la aplicación de la ley mediante el uso de métodos pioneros de aprendizaje automático e inteligencia artificial. El proyecto proporcionará una plataforma de análisis de datos descriptivo y predictivo y las herramientas correspondientes para prevenir, identificar, analizar y combatir la ciberdelincuencia y las actividades terroristas. La plataforma se basa en una tecnología básica aplicada al análisis de macrodatos, con amplias técnicas de IA y aprendizaje profundo personalizadas con capacidades y herramientas adicionales específicas para delitos[3]. Este proyecto, dirigido por «Engineering Ingegneria Informatica S.p.A.», la empresa de transformación digital líder en Italia, está compuesto por un consorcio de 21 socios, entre los que se encuentran Europol y siete fuerzas del orden de siete estados miembros de la UE: Guardia Civil (España), Policía de Grecia (Grecia), Servicio de Policía de Irlanda del Norte (Reino Unido), Inspectoratul General al Politiei Romane (Rumanía), Policia Judiciaria (Portugal), Nationale Politie — Landelijke Eenheid (Países Bajos) y Cuerpo de Policía y Guardia Fronteriza de Estonia (Estonia). Los resultados se publicarán en los próximos meses en el sitio web del proyecto[4].

Si bien la IA es una tecnología importante destinada a extenderse a todos los sectores de actividad, la velocidad con que se despliega también aumenta el riesgo de fallos y representa un problema de seguridad y resiliencia a escala nacional e internacional (Institut Montaigne, 2023). Con el aumento de los recursos, incluidos los privados, EE. UU. y China disponen de una importante ventaja en el desarrollo económico y tecnológico de la IA. Así, pues, Europa ha acumulado un retraso difícil de compensar. Según un informe del grupo de reflexión Skema Publika de 2022, en los últimos 30 años se han presentado más de 860 000 patentes relacionadas con la inteligencia artificial. Así se distribuye la procedencia de estas patentes[5]: Estados Unidos (30 %), China (26 %), Japón (12 %), Corea del Sur (6 %), Alemania (5 %), Reino Unido (2,5 %), Francia (2,4 %) y Canadá (1,9 %). Esto quiere decir que las potencias estadounidenses y asiáticas

[2] https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2022/europol-la-gendarmerie-recompensee-pour-sa-plateforme-d-outils-d-intelligence-artificielle-i.a.
[3] https://cordis.europa.eu/project/id/883596/es
[4] https://www.project-aida.eu/index.php
[5] https://www.cio-online.com/actualites/lire-l-europe-a-la-traine-pour-les-brevets-autour-de-l-ia-14132.html

representan casi las tres cuartas partes del mercado de la innovación en IA. Sin embargo, la Unión Europea se está preparando para imponer requisitos de seguridad y confianza a los sistemas de IA mediante reglamentos específicos (Ley de IA) y cuenta con muchos investigadores de gran calidad en matemáticas e inteligencia artificial.

El riesgo no se encuentra en el uso de la inteligencia artificial, sino en los algoritmos o herramientas que se basan en ella y que permiten utilizarla. La mayoría de los algoritmos y herramientas se desarrollan fuera de la Unión Europea y colocan a los Estados miembros en una cierta situación de dependencia de las potencias extranjeras. Por supuesto, ello genera riesgos para la seguridad nacional y la protección de los intereses fundamentales de los estados europeos.

Tras revisar el contexto en el que la inteligencia artificial evoluciona y se hace ineludible, abordaremos los riesgos a los que están expuestos actualmente los países europeos a través de casos concretos.

2.- ENTORNO DE SEGURIDAD NACIONAL

2.1.- Un ciberespacio no territorializado: ¿Distopía o Utopía?

Generalmente, se acepta que la noción de territorio procede del latín *territorium* en cuanto a área de tierra ocupada por un grupo humano. En efecto, se trata de una dimensión física (un área de tierra) con presencia humana, una ocupación humana. Sin embargo, hay otro significado menos conocido, derivado de *terrere*, que significa «asustar», «aterrorizar». Hugo Grotius hizo un análisis más que pertinente en *De jure belli ac pacis* a principios del siglo XVII:

«*Por eso Siculus Flaccus deriva la palabra territorio [...] del verbo latino "terrendis hostibus", que significa asustar, porque, según él, quien lo domina asusta a los enemigos: una etimología que parece tan fundada como las que dan otros. Varron deriva la palabra territorio del verbo «terrere», pisotear; Frontinus la deriva de la palabra «tierra»; el jurisconsulto Pomponio, de la misma palabra que Siculus Flaccus, pero por otra razón: dice que los magistrados tienen derecho a asustar dentro del territorio».*

La dimensión física es menos acusada en este sentido. Efectivamente, «asustar» son comportamientos, significa controlar otros comportamientos y, en consecuencia, los comportamientos de los humanos en un contexto determinado, en un espacio determinado controlado por una autoridad. Aunque este espacio es un territorio físico en palabras de Grotius, «aterrar» o «aterrador» podría referirse a un espacio virtual, abstracto y no territorializado, en el sentido primario de la palabra.

Aquí es donde entra en juego el término ciberespacio; su origen está particularmente arraigado en este lado aterrador. De hecho, en 1984 apareció en una novela de ciencia ficción (*Neuromante*, de William Gibson), donde se define como «*Una alucinación consensuada que experimentan a diario con toda legalidad decenas de millones de operadores, en todos los países, niños a los que se les enseñan los conceptos de las matemáticas... Una representación gráfica de los datos extraídos de las memorias de todos los ordenadores del sistema humano. Una complejidad impensable. Líneas de luz dispuestas en el no espacio de la mente, cúmulos y constelaciones de datos. Como las*

luces de la ciudad, en la distancia...». Este es un mundo totalmente nuevo, totalmente extraterritorializado, «aterrador». Esta obra de ciencia ficción pertenece al género literario denominado «ciberpunk», que describe un mundo violento, oscuro y casi apocalíptico en el que la tecnología informática y la inteligencia artificial están en el centro del funcionamiento de la sociedad. En este sentido, este género literario se acerca a la distopía, que no es más que un impedimento para alcanzar la felicidad, un mundo caótico.

Por otro lado, otros círculos defienden una visión distinta del ciberespacio, bastante utópica. El proyecto de Infraestructura global de información (GII) promovido por Al Gore en Estados Unidos entre 1993 y 1994 confirmó esta tendencia utópica. En 1994, Gore declaró ante la Unión Internacional de Telecomunicaciones:

«La Infraestructura global de información (GII) no solo será una metáfora de una democracia en funcionamiento, sino que, de hecho, fomentará el funcionamiento de la democracia al mejorar la participación de los ciudadanos en la toma de decisiones. Promoverá la capacidad de las naciones para cooperar entre sí. La veo como una nueva era ateniense de la democracia forjada en los foros que creará el GII».

Pero el punto culminante llegó dos años después, en 1996, con la «*Declaración de independencia del ciberespacio6*» de John Barlow. Se trata sin duda del elemento más fuerte de esta representación. Es, en más de un sentido, evocador. En efecto, se parece claramente a una nueva ideología basada en un espacio virtual, infinito e impalpable y, sobre todo, en contra de un mundo físico compartido entre los estados-nación y en el que dichos estados no son bienvenidos ni pueden controlar el ciberespacio:

«En China, Alemania, Francia, Singapur, Italia y los Estados Unidos se intenta contener el virus de la libertad levantando puestos de guardia en las fronteras del ciberespacio. Es posible que contengan el contagio durante un tiempo, pero no funcionarán en un mundo que pronto aparecerá en los medios digitales».

Aquí tenemos algo para «asustar» a los estados-nación. Ni utopía ni distopía, sino un cuarto espacio liberado de su dimensión física. De hecho, los territorios y las fronteras constituyen los cimientos de su existencia y supervivencia... Sin embargo, en el mundo físico, estas dos nociones suelen diluirse un poco. A modo de ilustración, citemos dos ejemplos: el «espacio Schengen» y la optimización fiscal. El espacio Schengen, además del pintoresco encanto de dicho pueblo luxemburgués, es un área de libre circulación de bienes, capitales, servicios y personas que incluye a los 27 estados[7] que han firmado este acuerdo. El principio de la libre circulación de personas[8] significa que cualquier persona (ciudadana de la UE o de terceros países[9]) puede cruzar las fronteras de los demás países sin estar sujeta a controles sistemáticos una vez que haya entrado en el territorio de uno de los estados miembros. Los vuelos entre ciudades del espacio Schengen se consideran

[6] Poeta y activista libertario estadounidense fallecido en 2018, cofundador de Electronic Frontier Foundation (una ONG dedicada a defender la libertad de expresión en Internet).

[7] Excepto Bulgaria, Chipre, Irlanda y Rumanía, todos los estados de la UE forman parte del espacio Schengen. También son miembros Suiza, Liechtenstein, Islandia y Noruega. El estatuto de Gibraltar aún se está negociando como parte del acuerdo del Brexit.

[8] Artículo 3 del Tratado de la UE

[9] La Unión Europea ya ha implantado el Sistema de Entradas y Salidas (SES), que entrará en vigor en mayo de 2023. El sistema tiene como objetivo registrar la entrada y salida de ciudadanos no pertenecientes a la UE que crucen una frontera exterior del espacio Schengen. Almacena datos de documentos de identidad y de viaje, así como datos biométricos.

vuelos nacionales sin el control de pasaportes biométricos (datos personales que pueden usarse en un sistema de IA). Por último, ¿acaso no son las técnicas de optimización fiscal un medio para eludir ciertas fronteras y, por tanto, la autoridad que se ejerce dentro de ellas, es decir, en un territorio determinado? Consiste en técnicas y métodos propios o externos que pueden utilizarse para reducir la carga tributaria tanto para las personas como para las empresas. Esto se hace de manera completamente legal (a diferencia de la evasión, que es ilegal), y el contribuyente tiene derecho a buscar y utilizar la ruta menos gravada. En resumen, a través de estos dos ejemplos, queda claro que las nociones de frontera y territorio se están diluyendo poco a poco, en un caso, mediante la entrega de la soberanía y, en el otro, mediante la elusión legal. A esto podríamos añadir movimientos de la sociedad civil como «No Border[10]», una red internacional que lucha por un mundo... sin fronteras.

3.- INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD: ¿QUÉ SEGURIDAD HAY EN EL CIBERESPACIO?

Ya sea distópica o utópica, la visión del ciberespacio plantea la cuestión de la alteración o incluso la desaparición de las fronteras. Sin embargo, esto no prescinde de la existencia física que caracteriza al ciberespacio. La definición oficial de los servicios estatales franceses, como la Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) o el Ministerio para Europa y de Asuntos Exteriores (MEAE) así lo atestigua: «Un espacio de comunicación constituido por la interconexión mundial de equipos automatizados de tratamiento digital de datos, los objetos a ellos conectados y los datos que en ellos se tratan». El espacio de comunicación es virtual, el equipo y la infraestructura son básicamente materiales (el almacenamiento puede ser inmaterial, la nube) y los datos que se tratan son... inmateriales. Si el ciberespacio es un cuarto espacio sin dimensión física, ¿cómo expresar la soberanía sobre los datos, excepto en los dispositivos de almacenamiento físico? Especialmente, en el caso de la IA ¿quién es el propietario de los algoritmos y los datos de entrenamiento?

El concepto de soberanía digital puede entenderse en un sentido distinto, y se refiere a la capacidad de una entidad determinada (una nación, una empresa o una persona) para dominar los atributos digitales (datos, información, conocimiento, algoritmos) en objetos que afirma observar o incluso controlar. El término «control» no significa necesariamente que la entidad posea (en el sentido de plena propiedad) los objetos en cuestión y, con mayor razón, los atributos digitales, en este caso los datos, de estos objetos (Ganascie, Germain, Kirchner, 2018)[11]. Así es como se concibe la soberanía digital en Francia y, por extensión, en Europa. De hecho, son los datos (inmateriales) los que representan el desafío de esta soberanía. En este sentido, y teniendo esto en cuenta, la Unión Europea cuenta con un arsenal legislativo en este ámbito.

El 23 de junio de 2022 entró oficialmente en vigor la nueva Ley Europea de Gobernanza de Datos (DGA), aplicable a partir de septiembre de 2023.

[10] Consulte el sitio web de la red http://noborder.org/

[11] Disponible en: http://cerna-ethics-allistene.org/digitalAssets/55/55160_AvisSouverainete-CERNA-2018-05-27.pdf

Este texto forma parte de la «Estrategia europea de datos*12»*, que a su vez es una subdivisión de la estrategia «Configurar el futuro digital de Europa*13»*, presentada en febrero de 2020 por la Comisión Europea, una de cuyas seis prioridades para el período 2019-2024 es «adaptar Europa a la era digital*14»*. Para ello, la Unión Europea se ha comprometido, en particular, a dotarse de nuevos instrumentos legales en los ámbitos de la economía de plataformas (Ley de Mercados Digitales**15** y Ley de Servicios Digitales**16**) y la inteligencia artificial (Ley de Inteligencia Artificial**17**) y, por supuesto, en lo que respecta a la materia prima de la economía digital: los datos.

La iniciativa legislativa más importante y relevante es el proyecto de Ley de Inteligencia Artificial, el primer marco legal europeo dedicado a los sistemas de IA. La Comisión ha decidido no regular la IA en sí misma como tecnología, sino centrarse en los sistemas de IA, entendidos como software capaz de generar resultados como contenido, predicciones, recomendaciones o decisiones (artículo 3 del proyecto de reglamento sobre la IA), y utilizar un enfoque multidimensional basado en el riesgo. Algunos usos de la IA conllevan un riesgo inaceptable y están prohibidos; otros representan un riesgo elevado y están permitidos si sus proveedores cumplen ciertos requisitos y llevan a cabo una evaluación de cumplimiento. Se permiten los usos que se consideran de bajo o mínimo riesgo. Los usos de la IA que socavan los valores fundamentales se consideran riesgos inaceptables. Sin embargo, el texto solo ofrece algunas excepciones, como la búsqueda de posibles víctimas de un delito, incluidos menores desaparecidos; determinadas amenazas para la vida o la seguridad física de las personas, incluidos los atentados terroristas; y la detección, localización, identificación o enjuiciamiento de los autores o sospechosos de delitos penales de al menos tres años (art. 5 y considerando 19[18]). Estos incluyen sistemas que utilizan técnicas subliminales, explotan las vulnerabilidades para alterar el comportamiento humano o se utilizan para la clasificación social algorítmica. Por último, el uso de la identificación biométrica a distancia «en tiempo real» de personas en espacios públicos se considera especialmente intrusivo y, en principio, está prohibido (Ponce del Castillo, 2021)[19].

Por tanto, el mundo real trata de «dominar» el ciberespacio a través de la seguridad (ciberseguridad) de los datos inmateriales, concretamente. Se trata de un intento de territorializar lo desmaterializado sin poseer el elemento material: una decorrelación entre el territorio y el espacio de soberanía (no territorializado) (Mortier, 2020).

[12] Comisión Europea, «Una estrategia europea de datos», Comunicación de la Comisión al Parlamento Europeo, el Consejo, el Comité Económico y Social Europeo y el Comité de las Regiones, Bruselas, 19 de febrero de 2020.
[13] Comisión Europea, «Shaping Europe's Digital Future», Comunicación de la Comisión al Parlamento Europeo, el Consejo, el Comité Económico y Social Europeo y el Comité de las Regiones, Bruselas, 19 de febrero de 2020.
[14] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_es.
[15] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020PC0842
[16] https://eur-lex.europa.eu/eli/reg/2022/2065/oj?locale=es
[17] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52021PC0206 y https://artificialintelligenceact.eu/the-act/
[18] https://artificialintelligenceact.eu/the-act/
[19] Disponible en https://www.etui.org/sites/default/files/2022-03/04_La%20strat%C3%A9gie%20num%C3%A9rique%20de%20l%E2%80%99Europe_2022.pdf

Por tanto, la ciberseguridad permite expresar la soberanía «digital». La ANSSI*20* lo define como el estado que busca un sistema de información que le permita resistirse a los acontecimientos que se originan en el ciberespacio y que puedan comprometer la disponibilidad, la integridad o la confidencialidad de los datos almacenados, tratados o transmitidos y los servicios correspondientes que estos sistemas ofrecen o ponen al alcance. La ciberseguridad implica el uso de técnicas de seguridad de los sistemas de información y se basa en la lucha contra la ciberdelincuencia y el establecimiento de una ciberdefensa. Esta definición incluye elementos puramente soberanos, como la lucha contra la delincuencia y la defensa, pero se refiere a los datos deseados en el ciberespacio.

En cuanto a la inteligencia artificial, ¿qué lugar ocupa en el ámbito del ciberespacio y, más concretamente, en la expresión de la soberanía en su seno? La IA es una tecnología disruptiva que se está implantando de manera gradual, mientras que la ciberseguridad tiene que ver con la seguridad de las infraestructuras digitales y la seguridad digital de los usuarios. Sin embargo, algunos procesos de IA pueden ayudar a crear ciberespacios más seguros. Un sistema de inteligencia artificial es un sistema automatizado que puede hacer predicciones, recomendaciones o tomar decisiones que afecten a entornos reales o virtuales en relación con un conjunto determinado de objetivos definidos por el ser humano. Un sistema de este tipo funciona mediante algoritmos que intentan reproducir la inteligencia humana de forma probabilística y determinista mediante el tratamiento de grandes volúmenes de datos. Estos algoritmos, estos programas informáticos, constituyen la base de la inteligencia artificial y son el resultado de un proceso de creación por parte del ser humano, de ahí el término artificial. No se trata de un proceso natural, sino de una construcción artificial. El aprendizaje automático, uno de los campos de la inteligencia artificial, tiene como objetivo permitir que, mediante el uso de algoritmos de aprendizaje, una máquina determine el mejor resultado posible o, si es necesario, detecte comportamientos maliciosos, por ejemplo, en materia de ciberseguridad. Para que este «método» funcione, es necesario que tenga acceso a los datos. Esto nos devuelve a las características inmateriales y virtuales que permiten la expresión de la soberanía digital sobre un espacio no territorializado (ciberespacio en el que se encuentran los datos) (Mortier, 2020).

Hoy en día, nuestra comprensión de lo que es la IA varía a medida que se superan hitos en este campo. La adaptabilidad, flexibilidad, predictibilidad y proactividad en cuanto a recursos temporales mínimos, la rapidez de la toma de decisiones y las circunstancias para hacerlo deberían ser las prioridades de la IA utilizada en el ámbito de la seguridad (Radulov, 2019).

En este sentido, la inteligencia artificial, compuesta por algoritmos y programas informáticos, sería solo uno de los aspectos físicos de las redes mencionados anteriormente en la definición de ciberespacio propuesta por las autoridades francesas: «... interconexión mundial de equipos automatizados de tratamiento digital de datos...». La inteligencia artificial podría entonces volver a una comprensión más convencional de la soberanía, ya que los algoritmos que le dan vida tendrían una nacionalidad en virtud de su creación por un ser humano que, de momento, posee una nacionalidad conforme a una expresión clásica de soberanía.

[20] Agence Nationale de la Sécurité des Systèmes d'Information /Agencia Nacional de Seguridad de los Sistemas de Información https://www.ssi.gouv.fr/

Estas pocas reflexiones sobre el territorio, las fronteras y la soberanía no pretenden en modo alguno ser exhaustivas o perentorias, sino más bien crear conciencia sobre el hecho de que la naturaleza humana siempre intenta unir lo que se conoce con lo que a veces puede trascenderla. Una reinterpretación natural de lo inmaterial para conservar los puntos de referencia propios. El impacto de la tecnología digital, el impacto del ciberespacio, que ha llegado como una ola en tan solo unas décadas (próximo a cero en la escala de la humanidad), exige que el hombre se replantee su condición en un mundo que es nuevo y a la vez sigue marcado por una existencia ineludible. Desde una «trascendencia negra» (Hottois, 1984) hasta un «reencantamiento del mundo», todo es posible y el ritmo parece estar marcado por... los datos, la inteligencia artificial, el vínculo entre el mundo real y el ciberespacio, entre la utopía y la distopía (ambas igualmente «aterradoras») pero también por el objeto de la ley, la seguridad y el fundamento de una inteligencia creada por el hombre, artificial.

4.- INTELIGENCIA ARTIFICIAL Y SEGURIDAD NACIONAL: ¿UN CALLEJÓN SIN SALIDA?

Para una empresa, un ciudadano o un Estado estratégico y soberano, la seguridad nacional se define como el hecho de poder tener un control total sobre sus datos. Y ello también implica saber cómo defenderse desde el punto de vista legal, económico y tecnológico de otros estados –o empresas extranjeras– proveedores del almacenamiento, la captura y la explotación de datos (Decloquement, Luttrin, 2023).

El Código Penal francés define los intereses fundamentales de la nación, los objetos de la seguridad nacional, de la siguiente manera (art. 410-1):

«su independencia, (...) la integridad de su territorio, (...) su seguridad, (...) la forma republicana de sus instituciones, [los] medios para su defensa y (...) su diplomacia, (...) la protección de su población en Francia y en el extranjero, (...) el equilibrio de su entorno natural y su entorno y [los] elementos esenciales de su potencial científico y económico y de su patrimonio cultural».

Por tanto, un estado tiene la obligación de salvaguardar su soberanía de este modo. Para ello, y para hacer frente a las amenazas, debe disponer de los recursos necesarios, incluida la tecnología. La inteligencia artificial es ahora uno de sus componentes, debido al progreso que sugiere. La defensa de los intereses fundamentales ya no se limita al plano físico, sino que también abarca el dominio virtual.

El principal riesgo del uso de la inteligencia artificial para la seguridad nacional es la dependencia de tecnologías extranjeras. De hecho, existe una auténtica competencia tecnológica entre Estados Unidos y China. Las inversiones de estas dos potencias en empresas europeas concuerdan totalmente con esta competencia. Es especialmente difícil para los estados europeos coordinarse para combatir este tipo de depredación económica, a pesar del mecanismo europeo de control de la inversión extranjera. Por tanto, los estados europeos se están convirtiendo cada vez más en países importadores de tecnología. Esto puede traducirse en el acceso a información sesgada u operaciones estratégicas por parte de potencias extranjeras: el uso de algoritmos desarrollados y controlados por ellas no solo genera dependencia, sino también un riesgo. Además, la inteligencia artificial controlada por terceros abre la puerta al riesgo de ciberataques, la manipulación del contenido e incluso la apropiación indebida de información estratégica. Más aún, una

potencia extranjera podría tomar el control social de nuestras poblaciones y, por tanto, establecer acciones de desinformación para desestabilizar el orden social.

En el ámbito de la inteligencia, Estados Unidos está desplegando una cantidad considerable de recursos para dominar la inteligencia artificial. Solo la Agencia Central de Inteligencia (CIA) tiene alrededor de 140 proyectos en desarrollo que aprovechan la IA de algún modo para llevar a cabo tareas como el reconocimiento de imágenes y el análisis predictivo. La Actividad de Proyectos de Investigación Avanzada sobre Inteligencia (IARPA), cuya misión es diseñar y dirigir investigaciones de alto riesgo y alto impacto que den lugar a tecnologías innovadoras con importantes beneficios futuros para la inteligencia, patrocina varios proyectos de investigación sobre IA destinados a producir otras herramientas analíticas en los próximos cuatro a cinco años. Algunos ejemplos de esto son el desarrollo de algoritmos para el reconocimiento y la traducción de voz multilingües en ambientes ruidosos, la geolocalización de imágenes sin los metadatos asociados, la fusión de imágenes bidimensionales para crear modelos tridimensionales y la creación de herramientas para inferir el funcionamiento de un edificio a partir del análisis del patrón de vida (Servicio de Investigación del Congreso de EE. UU., 2020). Los estados europeos no tienen acceso a estos medios sin una verdadera cooperación multilateral. El proyecto AIDA, mencionado en la introducción, es el principio de una respuesta europea, pero probablemente carezca de dimensión.

Más allá de las principales potencias estatales, es necesario abordar el entorno económico de la inteligencia artificial. Con respecto a su desarrollo en el mundo, los actores principales son las mayores empresas de tecnología. Las empresas GAFAM (Google, Apple, Facebook-Meta, Amazon, Microsoft) son monstruos económicos, de un tamaño sin precedentes, que a veces se encuentran en una posición casi de monopolio, lo que les otorga un poder enorme (Cazals, Cazals, 2020). La realidad es que la capacidad de influencia de las GAFAM se extiende más allá de las fronteras de Estados Unidos y su poder no se limita a las empresas, sino que se extiende a los Estados, las ONG e incluso los organismos internacionales (Nour, 2019). La hegemonía de las empresas GAFAM en Europa es casi total. En noviembre de 2021, en el punto álgido de la pandemia de la COVID-19, las GAFAM alcanzaron márgenes récord: Microsoft, un 38 %; Meta, un 37 %; Google, casi un 30 %; y Apple 7, más del 26 %. A principios de diciembre, la capitalización bursátil de esta última alcanzó el nivel más alto jamás registrado para una empresa estadounidense, con la asombrosa cifra de 2650 millones de dólares, seguida de Microsoft (2570 millones de dólares), Alphabet (1980 millones de dólares), Amazon (1850 millones de dólares) y Meta (1000 millones de dólares) (Smyrnaios, 2023). Si bien son actores económicos, son y representan a fuerzas extranjeras cuyo *modus operandi* es el siguiente:

- Analizar los objetivos (debilidades psicológicas, debilidades socioeconómicas, funcionamiento, red, entorno familiar y profesional, identificación de las necesidades del territorio).
- Utilizar las vulnerabilidades psicológicas y responder a una necesidad específica del territorio (estrategia a corto plazo).
- Introducirse en los territorios y empobrecerlos (a medio y largo plazo) para absorber mejor al Estado (Decloquement, Luttrin, 2023).

Del lado chino, en su territorio, Pekín obliga a las empresas extranjeras, incluidas las estadounidenses, a colaborar con una homóloga china, a almacenar sus datos de forma

local, incluso los más sensibles, y a transmitir sus patentes tecnológicas, con el riesgo de perder el acceso al mercado de la segunda economía mundial (Nour, 2019). Esta es una de las razones de los enormes progresos de la inteligencia artificial en China. En Estados Unidos, una gran parte de los datos está monopolizada por empresas privadas (Amazon, Facebook y Google), mientras que en China la mayoría de las empresas son públicas o están vinculadas al gobierno de alguna manera. Por tanto, este ascenso chino se ve facilitado por ingredientes como el gran volumen de datos, los miles de empresarios e ingenieros y el apoyo activo del poder político. Actualmente, las empresas BHATX (Baidu, Huawei, Alibaba, Tencent, Xiaomi) poseen en su conjunto más datos que EE UU. y Europa juntos (Nour, 2019). Del mismo modo, uno de los componentes clave de la IA, el aprendizaje automático, que esencialmente se basa en la abundancia de datos, se está desarrollando aún más en China a través de dos líderes mundiales en pagos móviles, AliPay y Tencent. De hecho, por sorprendente que parezca, los chinos realizan 50 veces más compras móviles que los estadounidenses (Nour, 2019).

5.- INTELIGENCIA ARTIFICIAL Y APLICACIÓN DE LA LEY EN EUROPA

Una vez establecidas las raíces del problema, nos gustaría elaborar una breve lista de los elementos específicos de la UE y de cada uno de sus estados miembros, lo que haría simplemente imposible lograr un sistema de IA eficiente al servicio de las fuerzas del orden y la justicia en el ámbito de toda la Unión Europea.

5.1.- La falta de voluntad y medios a corto, medio y largo plazo

Recientemente, el sitio web de una de las principales organizaciones de IA, el Centro para la Gobernanza de la IA, de Oxford, publicó un libro blanco con un título intrigante (Ord, 2022): *Lessons from the Development of the Atomic Bomb (Lecciones del desarrollo de la bomba atómica)*. Este texto, muy oportuno, compara de forma indirecta los recursos que necesitaría cualquier organización estatal que desee poseer la bomba atómica con los que necesitaría para desarrollar su propio sistema operativo de IA.

Las páginas anteriores evocan en gran medida los infinitos poderes de las grandes tecnologías, a los que añadiremos la capacidad (ilegal) de vigilancia global, que recientemente se ha visto reforzada por las constelaciones de satélites StarLink y pronto por las de Amazon. Todos estos aspectos se explican con gran detalle en la obra de referencia sobre este asunto, la obra maestra de Shoshana Zuboff (2019).

Sobre este tema, tanto para el desarrollo de una bomba atómica como para el desarrollo de un sistema de IA completo y soberano, las cuatro condiciones principales que expone Orb (2022) son:

- poseer las materias primas (= lo que Europa no tiene en términos de hardware)
- tener una voluntad política inquebrantable a corto, medio y largo plazo (imposible en la situación actual de la UE y con las prerrogativas nacionales)
- disponer durante décadas de los recursos humanos, tecnológicos y financieros necesarios (Europa nunca ha tenido un solo programa cuantificado en billones de euros, la cantidad necesaria para un sistema de IA. Todo lo que se ha implementado hasta ahora, teniendo en cuenta todos los campos, no supera unos pocos miles de millones) y, por último,

- llevar a cabo un espionaje activo de quienes ya posean la bomba (en este caso, la IA) y mantener el más absoluto secreto sobre el desarrollo del arma en sí (de la IA)

¿La UE espía a las GAFAM/BHATX y mantiene en absoluto secreto la existencia y la actividad del megalaboratorio que desarrolla su propio sistema de IA (incluidos satélites), hardware terrestre (incluidos ordenadores cuánticos y superordenadores), software de reconocimiento individual de fabricación propia y medios de vigilancia capilar en toda la UE? No es necesario ser tan cínico como Emil Cioran para darse cuenta de que, si el desarrollo de una seguridad europea ya es imposible, su extensión a un sistema de IA paneuropeo, así como las continuas operaciones de espionaje, contraespionaje y engaño (preservando el secreto del proyecto) de la UE dejadas en manos de Bruselas son pura ciencia ficción.

5.2.- La eterna elección entre la competencia intereuropea en lugar de una federación...

En el ámbito de un sistema de IA totalmente funcional para la seguridad, la UE necesita comunicaciones fiables y rápidas, así como tecnologías de primer nivel y, por último, pero no por ello menos importante, un centro de competencia único que reciba, analice y envíe las investigaciones a cada miembro de la UE en tiempo real.

Las decisiones tomadas desde el comienzo de la «década digital» de la UE se pueden comparar a una pequeña caja con 27 huecos que da a cada Estado miembro euros por lograr el mismo objetivo que cualquier otro miembro.

Hay dos ejemplos especialmente relevantes: el primero, que, debido a las presiones políticas de EE. UU., la mayoría de los miembros de la UE aún carecen de 5G (por no hablar del 6G, que pronto estará disponible), un elemento fundamental para el buen funcionamiento de la IA. Esta negativa a adoptar la última tecnología inalámbrica está costando miles de millones a la economía de la UE cada año.

¿Cuál ha sido la decisión de la UE? Crear un fondo de 2000 millones de euros que se distribuirá a cada miembro que desee crear una tecnología OpenRAN operativa que, a finales de 2027, compita con las tecnologías desarrolladas por otros miembros. Es inútil mencionar aquí que Francia, España y Alemania ya dominan esta tecnología: una mente empresarial lógica sencillamente habría creado un OpenRAN de la UE combinando lo mejor de cada uno de los resultados obtenidos por estos tres Estados y lo habría propuesto al Parlamento de la UE para su adopción inmediata (Lauhde, 2022).

El segundo elemento, aún más oportuno, es el «Centro Europeo de Ciberseguridad», como se denominó hace diez años, que estará bajo la dirección de un comisariado de la UE recién creado. Al estar ubicado en el Reino Unido, todo tuvo que replantearse tras el Brexit. Hasta 2020, cuando se designó al exjefe de Seguridad del OIEA para diseñar su arquitectura funcional, mientras que Bucarest ganó el concurso para albergar la sede del Centro, seguía habiendo muchas esperanzas.

La entrada en funciones de la presidenta von der Leyen y la eliminación del antiguo método «Spitzenkandidaten» («candidatos principales») para elegir a los comisarios, multiplicada por las consecuencias económicas (y, por tanto, políticas) de la COVID y la crisis energética, provocó que las crecientes disputas entre varios Estados miembros tuvieran un impacto catastrófico en todo el proyecto diseñado para el Centro

de Ciberseguridad, y no únicamente como se puso de manifiesto en diciembre de 2022, con el veto de solo dos miembros que prohibía a Rumanía y Bulgaria unirse al espacio Schengen, mientras la unanimidad de los miembros daba la bienvenida a Croacia.

La recién nacida organización de seguridad sufrió desde sus inicios. Rebautizada como ECCC (Centro Europeo de Competencia en Ciberseguridad), sigue estando dirigida por un comité ejecutivo (y no por un comisario), y sus objetivos son principalmente distribuir fondos y compartir conocimientos a cualquier Estado miembro exigente.

Por tanto, nunca se convertirá en el órgano proactivo de aplicación de la ley e inteligencia deseado por la Unión, siguiendo los pasos de la C-Proc (Oficina del Programa sobre Ciberdelincuencia) del Consejo de Europa, también con sede en Bucarest, reducida por los mismos egos políticos de soberanía nacional a llevar a cabo un desarrollo continuo de capacidades, principalmente en los países del tercer mundo y, a veces, en uno de los miembros de la CE.

5.3.- La identificación digital europea, una herramienta fundamental para una futura IA aprobada por la UE, pero...

En marzo de 2023, una abrumadora mayoría del Parlamento de la UE votó a favor de la implantación de un sistema de identificación digital en la UE. Sería otra herramienta básica para cualquier sistema de IA dedicado a la aplicación de la ley.

Por desgracia, aunque el texto legislativo incluye todas las medidas que garantizan que cada ciudadano de la UE tendrá un derecho permanente de acceso y vigilancia de los datos incluidos en este «pasaporte digital» (que debería o podría en última instancia incluir documentos fiscales, sanitarios, legales y biométricos, etc.), la mayoría de los partidos políticos, de la mayor parte de los países de la UE y, sobre todo, de toda la UE Oriental, se oponen a que sus países participen en la identificación digital, (donde sigue muy presente el recuerdo de la época comunista y la intromisión del Estado en la vida personal, incluso en las generaciones más jóvenes).

Es muy probable que la identificación digital de la UE, cuya implantación y contenido se dejan al libre albedrío de cada Estado miembro, se convierta en una gigantesca carpeta vacía, al menos a corto y medio plazo.

5.4.- La “Ley de IA” europea, un obstáculo ineludible para una IA eficaz en materia de aplicación de la ley...

La ley antes mencionada, finalizada en 2021, pero que aún no se ha sometido a la votación del Parlamento Europeo, es un texto demasiado ético que probablemente impulsará las ventas de IA fabricada en la UE a clientes que desean proteger la privacidad de sus clientes, principalmente en países en los que los ciudadanos desconfían mucho de las actividades de inteligencia de su propio gobierno, como EE. UU. o Canadá tras las revelaciones de Snowden y los abusos de la Patriot Act en EE. UU. y los abusos judiciales durante el período de ley marcial impuesto por el gobierno de Trudeau durante la huelga de camioneros en Canadá (Siegmann, Anderljung, 2022).

Paradójicamente, como podemos ver en EE. UU., donde la IA ya se utiliza con fines policiales y judiciales, esta norma europea, de aplicarse, prohibirá el uso de la IA

por parte de los mismos actores de la UE, ya que no puede llevarse a cabo ninguna investigación completa realizada con la ayuda de un conjunto completo de herramientas de IA sin «daños colaterales» (las interceptaciones ambientales, el estudio de vídeos o imágenes, etc. son elementos en los que aparecen otros ciudadanos, ajenos a los delitos del posible delincuente investigado). Incluso si bien todos estos elementos pueden y deben censurarse y borrarse debidamente antes del juicio, este mismo tema se utilizará profusamente desde la perspectiva política, con ayuda de la «Ley de IA» de la UE, para adoptar posiciones radicales contra el uso de la IA por parte de las fuerzas del orden.

5.5.- El impulso a favor de la IA utilizado por las fuerzas del orden es probablemente el peor de la historia reciente...

Otra fuente indispensable para analizar la IA a través de la percepción de la población y las empresas de la UE son los libros blancos publicados por la IE University – Centro para la Gobernanza del Cambio (ie.edu), con sede en Barcelona, y, concretamente, su informe anual «European Tech Insights». Su versión más extensa, publicada en dos volúmenes en 2021, subraya una especie de «esquizofrenia» en la percepción de cada persona sobre lo que realmente es la IA (Chrzanovki, 2021). De hecho, por un lado, a una gran mayoría de los europeos les gustaría que la UE y sus estados miembros adoptaran medidas legales para reducir la pérdida de puestos de trabajo a causa de la IA y el aprendizaje automático (European Tech Insights, 2021), pero, por otro, la desconfianza hacia la clase política y los gobiernos actuales es total: la mayoría de los europeos desea que sean las redes sociales quienes censuren las noticias falsas, y no las instituciones estatales (European Tech Insights, 2021). Y, lo que es peor, el 51 % de los europeos preferiría que la IA gobernara su país en lugar de los diputados y miembros del gobierno humanos (European Tech Insights, 2021).

En el ámbito que nos atañe, el principal problema es que estamos presenciando el nivel más bajo de confianza hacia los políticos y, por tanto, hacia los gobiernos de la historia contemporánea. Lo más grave es que la consecuencia directa de esta falta de confianza, incluso en países en los que la administración cumple con las expectativas de los ciudadanos, es la creencia de que las fuerzas del orden y, sobre todo, los servicios de inteligencia son tan tóxicos como los políticos, lo que significa que cualquier nueva donación a esas entidades (la IA sería la más importante) se considera de hecho una intrusión en la privacidad de los ciudadanos.

6.- CONCLUSIÓN: ALGO DE LUZ AL FINAL DEL TÚNEL

En Europa existe un interés creciente por los conceptos de «soberanía digital» y «autonomía estratégica en el ciberespacio». Si bien sus significados son diferentes, están estrechamente relacionados y ambos se refieren a la voluntad de los actores políticos y económicos europeos de mantener su autonomía en los procesos de toma de decisiones estratégicas. Para los estados europeos, esto implica adquirir una capacidad autónoma de valoración, decisión y acción para ejercer su soberanía (Dannet, Desforges, 2020). Este es el meollo de la cuestión: ¿cómo defender los intereses nacionales cuando uno se encuentra en una situación de dependencia? Aunque dentro de la Unión Europea se está trabajando, especialmente en materia de normativa, queda mucho por hacer en lo que respecta al desarrollo de sistemas de inteligencia artificial.

Como estamos muy lejos de vislumbrar un borrador de sistema de IA paneuropeo integrado que favorezca los intercambios y el desempeño de las fuerzas del orden (véase la lista de países de la UE que se oponen a un sistema de este tipo en Viscusi, G, Collins, A., Florin, M.-V., 2020), en nuestra opinión, la única manera de seguir es esperar que unos cuantos gobiernos y tribunales supremos valientes permitan que se empiece a utilizar la IA en sus territorios.

Por supuesto, el primer paso es prohibir la temida «IA predictiva», prohibida incluso en EE. UU., ya que podría arrojar resultados como los que se ven en la obra maestra de Steven Spielberg, «Minority Report» (2002). En caso de que se logre dar ese paso y los tribunales introduzcan y admitan progresivamente la IA, ya contamos con una «guía de buenas prácticas» europea: el informe elaborado por el UNICRI y Europol (UNICRI, 2018).

Pero, sobre todo, tenemos la experiencia práctica de los tribunales estadounidenses. Tras algunos años de permitir el uso de la IA, se ha recopilado una lista completa de errores y logros positivos. Como resultado, la propia Casa Blanca aprobó un marco integral, con instrucciones claras que cualquier usuario de IA (empresa o institución) debe seguir (Oficina para Políticas de Ciencia y Tecnología, 2022).

Sin embargo, la mayoría de los países de la UE tienen el *modus vivendi* grecorromano, que exige nuevas leyes antes de aplicar cualquier novedad en un tribunal. En un mundo en el que cada día aparecen nuevas tecnologías, aplicaciones y software, ya no tenemos tiempo para eso.

Se necesitan fases experimentales, con o sin un valor decisivo para los tribunales, si la UE no quiere seguir siendo víctima del inmenso poder de las GAFAM/BATX, que siguen estas palabras pronunciadas en 2011 por Eric Schmidt (entonces director ejecutivo de Google): «*La alta tecnología funciona tres veces más rápido que las empresas normales. Y el gobierno funciona tres veces más lento que las empresas normales. Así que tenemos una diferencia de nueve veces... Por tanto, lo que queremos es asegurarnos de que el gobierno no se interponga y frene las cosas»*.

BIBLIOGRAFÍA

- Cazals, F.; Cazals, C., «GAFAM et BATX contre le reste du monde», en Cazals, F.; Cazals, C., Intelligence artificielle. L'intelligence amplifiée par la technologie, De Boeck Supérieur. 2020.
- Chrzanovski, L., "ML, AI, IoT: why it is important to take the time to reflect", Cybersecurity Trends, Edición Reino Unido, n.º 3/4. 2021.
- Congressional Research Service, Artificial intelligence and National Security. Noviembre de 2020.
- Danet, D.; Desforges, A.), «Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques», Hérodote, vol. 177-178, n.º 2-3. 2020.
- Decloquement F.; Luttrin A., «La souveraineté numérique au fondement de notre performance nationale», en Cercle K2, Les enjeux du big data, Cercle K2. 2023.
- European Tech Inside, Centro para la Gobernanza del Cambio-IE University, vol.1. 2021.
- Ganascie, J.-G.; Germain, E.; Kirchner, C., «La souveraineté à l'ère du numérique. Rester maître de nos choix et de nos valeurs», CERNA. Mayo de 2018.
- Hottois, G., Le signe et la technique. La philosophie à l'épreuve de la technique, Aubier Montaigne, París. 1984.
- Institut Montaigne, Investir l'IA sûre et digne de confiance : un impératif européen, une opportunité française, Note d'action. Abril de 2023.
- Mika Lauhde, M., «Par quel moyens serons-nous espionnés ou, au contraire, plus protégés demain: anciennes et nouvelles normalités des télécoms...», Cybersecurity Trends, Edition Spéciale Cyber-espionnage économique et technologique. Junio de 2022.
- Marcellin, S., «L'intelligence artificielle centrée sur l'humain: droit ou éthique?», Revue de la Gendarmerie Nationale, n.º 268. Enero de 2021.
- Meghani, R.; Essomba, M.; Chrzanovski, L., «The stakes have never been higher…», CyberSecurity Trends, Edición Reino Unido, n.º 1. 2023.
- Mortier, S., «Réflexion sur l'Homme et le cyberespace : le paradoxe de l'oeuf et de la poule», Revue de la Gendarmerie Nationale, n.º 266. Diciembre de 2019.
- Mortier, S., «IA et cyber-sécurité, les instruments de conquête d'un espace non-territorialisé», Droit et Patrimoine, n.º 298. Enero de 2020.
- Nour, M. R., «Géopolitique de l'Intelligence Artificielle : Les enjeux de la rivalité sino-americaine», Paix et Sécurité Internationales, n.ºº7. 2019.
- Office of Science and Technology Policy, The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, The White House. Octubre de 2022.
- Ord, T., Lessons from the Development of the Atomic Bomb, Oxford, Centre for Governance of Artificial Intelligence,. Septiembre de 2022.
- Ponce Del Castillo, A., «La stratégie numérique de l'Europe : centrée sur les personnes, sur les données ou sur les deux ?», Bilan social de l'Union Européenne. 2021
- Radulov, N., «Artificial intelligence and security. Security 4.0», International Scientific Journal – Security & Future, vol.3, n.ºº1. 2019.
- Siegmann, C.; Anderljung, M., The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market, Oxford, Centre for Governance of Artificial Intelligence. Agosto de 2022.

- Smyrnaios, N., «Les GAFAM, entre emprise structurelle et crise d'hégémonie», Pouvoirs – Revue française d'Etudes constitutionnelles et politiques, n.º°185. 2023.
- UNICRI, White paper Artificial Intelligence and Robotics for Law Enforcements, Turín. 2018.
- Viscusi, G.; Collins, A.; Florin, M.-V., «Governments strategic stance toward artificial intelligence: an interpretive display on Europe», en ICEGOV '20: Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance. Septiembre de 2020.
- Zuboff, S., The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York Public Affairs. 2019.