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

Rosalía Machín Prieto
Capitán Guardia Civil
Jefe de Proyectos TIC-IA /Jefe de Departamento Fondos Europeos SES-SGSICS
Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (CETSE-SGSICS)

ANTECEDENTES PARA LA IMPLANTACIÓN DE LA IA EN SEGURIDAD A TRAVÉS DE EUROPA: La innovación tecnológica como factor clave para el Ministerio del Interior

ANTECEDENTES PARA LA IMPLANTACIÓN DE LA INTELIGENCIA ARTIFICAL EN SEGURIDAD A TRAVÉS DE EUROPA: La innovación tecnológica como factor clave para el Ministerio del Interior

Resumen: Actualmente, Europa facilita a sus Estados Miembros (EM), el acceso a importantes inversiones en investigación y nuevas tecnologías de información y comunicaciones, claves, entre las que destaca la Inteligencia Artificial (IA).

La cantidad de información que debe tratarse y procesarse en el ámbito de la seguridad, ha aumentado enormemente ante la aparición de nuevas modalidades de criminalidad, sobre todo en los últimos veinte años, debido a la proliferación y extensión de Internet en prácticamente todos los ámbitos de la actividad cotidiana.

La digitalización, la disponibilidad y el acceso a grandes volúmenes de datos, son elementos esenciales para el desarrollo de la IA. Supone para el Ministerio del Interior Español, las Fuerzas y Cuerpos de Seguridad del Estado, entre ellas la Guardia Civil, y demás organismos dependientes de la Secretaría de Estado de Seguridad, apostar y participar en el desarrollo de nuevas tecnologías y sus aplicaciones con la finalidad de mejorar la función pública y mantener la seguridad de la ciudadanía española.

La Comisión Europea respalda la importancia de reforzar la innovación y la cooperación público-privada para responder adecuadamente a las amenazas globales, cada vez más especializadas, como el ciberdelito, el crimen organizado y el terrorismo. Con el presente trabajo, se pretende dar valor añadido y demostrar que la cooperación público-privada a través de proyectos de corte europeo, es vital para garantizar el acceso al talento, al conocimiento, y a nuevos mercados nacionales e internacionales, y de este modo abordar eficazmente los desafíos de utilización de IA en seguridad.

Abstract: Europe is currently providing its member states with access to major investments in research and new key information and communications technologies, including Artificial Intelligence (AI).

The amount of information to be handled and processed in the field of security has increased enormously with the emergence of new forms of crime, especially in the last twenty years, due to the proliferation and extension of the Internet in practically all areas of daily activity.

Digitization, availability and access to large volumes of data are essential elements for the development of AI. For the Spanish Ministry of the Interior, the State Security Forces and Corps, including the Civil Guard, and other agencies under the Secretary of State for Security, it means betting and participating in the *development of new technologies and their applications in order to improve the* public service and maintain the safety of Spanish citizens.

The European Commission supports the importance of strengthening innovation and public-private cooperation to adequately respond to increasingly specialized global threats such as cybercrime, organized crime and terrorism. This paper aims to add value and demonstrate that public-private cooperation is vital to ensure access to talent, knowledge, and new national and international markets, and thus effectively address the challenges of using AI in security.

Palabras clave: IA Supervisada, Algoritmo, Dato, Innovación, Sistema de información.

Keywords: Supervised AI, Algorithm, Data, Innovation, Information System.

ABREVIATURAS (GLOSARIO DE TÉRMINOS)

ABC Control Automatizado de Fronteras. (Automated Border Control).
ABC4EU Control Automatizado de Fronteras para la Unión Europea (Automated Border Control for the European Union).
AGE Administración General del Estado.
AI Inteligencia Artificial (Artificial Intelligence).
AIaaS Inteligencia Artificial como Servicio.
AI-HLEG Grupo de expertos de alto nivel en Inteligencia Artificial (High Level Experts Group in Artificial Intelligence).
APTs Amenaza Persistente Avanzada.
BI Inteligencia de Negocio. (Business Intelligence)
BMVI Instrumento de Gestión para Fronteras y Visados (Border Management and Visa Instrument).
BOGC Boletín Oficial de la Guardia Civil.
CAHAI Comité Ad Hoc sobre Inteligencia Artificial.
CCAA Comunidades Autónomas.
CCN-CERT Centro Criptológico Nacional / Equipo de Respuesta a Incidentes de Seguridad Informática.
CDTI Centro para el Desarrollo Tecnológico e Industrial.
CEPOL Agencia de la Unión Europea para la formación policial.
CETSE Centro Tecnológico de Seguridad.
CISE Entorno Común de Intercambio de información Europeo.
CITCO Centro de Inteligencia contra el Terrorismo y el Crimen Organizado.
CLOUD Nube digital.
PN Policía Nacional.
CAP Centro de Análisis y Prospectiva.
CNPIC Centro Nacional de Protección de Infraestructuras Críticas.
DDoS Ataques Distribuidos de Denegación de Servicio.
DEP Programa Europa Digital (Digital Europe Programme).
DESI Índice de Economía y Sociedad Digitales (Digital Economy and Society Index).
DL Aprendizaje Profundo (Deep Learning).
DG CONNECT Dirección General de Redes de Comunicación, Contenido y Tecnología.
DG HOME Dirección General de Migración y Asuntos de Interior.
DG REFORM Dirección General de Apoyo a las Reformas Estructurales.
Digital-DEP Programa Europa Digital (Digital Europe Programme).
EES Sistema de Entrada y Salida (Entry Exit System).
ELSJ Espacio de Libertad, Seguridad y Justicia.
EM Estados Miembros
EMPACT Plataforma Multidisciplinaria contra Amenazas Criminales (European Multidisciplinary Platform Against Criminal Threats).
ENIA Estrategia Nacional Inteligencia Artificial.
ENISA Agencia de la Unión Europea para la Ciberseguridad.
ENLETS Red Europea de Aplicación de la Ley a Servicios Tecnológicos (European Network of Law Enforcement Technology Services).
ESA European Space Agency (Agencia Espacial Europea).
ESMIR Ministerio del Interior España.
Eu-LISA Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia.
EUROJUST Agencia Europea de cooperación judicial.

EUROPOL Agencia de la Unión Europea para la Cooperación en materia de Aplicación de la Ley.
EUROSUR Sistema Europeo de Vigilancia de Fronteras (European Border Suveillance System).
FCSE Fuerzas y Cuerpos de Seguridad del Estado.
FEDER Fondos Europeos de Desarrollo Regional.
FP7 7º Programa Marco
FRONTEX Agencia Europea de la Guardia de Fronteras y Costas.
FSI Fondos para la Seguridad Interior.
GC Guardia Civil.
H2020 Programa Horizonte 2020 (8º Programa Marco).
HE Programa Horizonte Europa (9º Programa Marco).
HEUROPA Programa Horizonte Europa.
I+D+i Investigación, Desarrollo e Innovación.
IA Inteligencia Artificial.
IoT Internet de las Cosas (Internet of Things).
LEA Law Enforcement Agency (Agencia de Aplicación de la Ley o Fuerzas de Seguridad).
LEAR Legal Entity Appointed Representative (Autoridad Representativa Legal).
LOPDGDD Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.
MCE Mecanismo CONECTAR EUROPA.
MFP Marco Financiero Plurianual.
ML Machine Learning (Aprendizaje de Máquina).
MSA Micro Services Architecture (Arquitectura de Mircoservicios)
NCP Punto Nacional de Contacto.
NLP Procesamiento de Lenguaje Natural.
OCC Oficina de Coordinación Cibernética.
OCDE Organización para la Cooperación y Desarrollo Económico.
ODS Objetivos de Desarrollo Sostenible.
OLAF Oficina Europea de Lucha contra el Fraude.
ONU Organización de las Naciones Unidas.
OSCE Organización para la Seguridad y la Cooperación en Europa
OSINT Inteligencia de fuentes abiertas. Open Source INTelligence
OTAN Organización del Tratado del Atlántico Norte.
PYME Pequeña y Mediana Empresa.
RBI Identificación Biométrica Remota. Remote Biometric Identification.
RGPD Reglamento General de Protección de Datos.
SEDIA Secretaría de Estado de Digitalización e Inteligencia Artificial
SGSICS Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad.
TICs Tecnologías de la Información y Comunicación.
UE Unión Europea.
UNESCO Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.
UPM Universidad Politécnica de Madrid.
WGAI Working Group Artificial Intelligence (Grupo de Trabajo en Inteligencia Artificial).
RSC Responsabilidad Social Corporativa

1.- INTRODUCCIÓN

La tecnología, la innovación y la digitalización son la base del nuevo orden global. No se puede negar que el cambio tecnológico ha llegado a todos los ámbitos de la sociedad, la economía y la política, generando una nueva dimensión en las relaciones internacionales y en el campo de la seguridad.

El conocimiento científico, el acceso a la tecnología, su desarrollo y regulación, se han convertido en elementos imprescindibles para los Estados y para sus sociedades. Las relaciones de poder ya no sólo se basan en la excelencia tecnológica, la defensa y la seguridad, sino también en la necesidad de alcanzar la hegemonía en el ciberespacio o en construir nuevos espacios de datos.

Las nuevas revoluciones tecnológicas vinculadas con los sistemas de información y de comunicación (TICs), han generado nuevas áreas de colaboración y competición. La digitalización y la creación de redes globales para el intercambio de información fueron lideradas en un primer momento por Estados Unidos. La segunda fase, y en la que actualmente nos encontramos, basada en las redes 5G, el Internet de las Cosas (IoT), la tecnología cuántica y la Inteligencia Artificial (IA), se está desarrollando entre una aguerrida competición entre China y Estados Unidos. Pero se deben visibilizar otras potencias medias en dichos campos como son la Unión Europea, España incluida, Japón, Corea del Sur y otros países asiáticos.

El poder acceder a las primeras generaciones de nuevas tecnologías, integrar algunas de las tradicionales o diseñar y mantener las nuevas infraestructuras de las redes de datos, son aspectos críticos en los que se basa la seguridad nacional de las nuevas sociedades.

El análisis de Big Data y las técnicas de inferencia a través de procesos de IA, han abierto el campo para nuevos servicios, mucho más personalizados y también mucho más útiles en el ámbito de la Seguridad. Se plantean importantes preocupaciones en cuanto a la privacidad del individuo y su autonomía individual. Muchos Estados buscan el equilibrio entre seguridad y libertad, debido a la creciente tendencia de actividades delictivas relacionadas con el cibercrimen y el robo de identidades.

La presente situación está generando asimetrías de poder. La *revolución de la información* asociada a las nuevas tecnologías digitales, ha marcado cuatro valores fundamentales que son necesarios para ejercer influencia en este nuevo entorno: *redes, datos, información y conocimiento*. Sin embargo, son las grandes compañías tecnológicas las que poseen la mayor parte de los datos y de las redes, beneficiándose mayoritariamente de la presente situación.

En paralelo, las sociedades se enfrentan a problemáticas generadas por las nuevas tecnologías en su uso diario. La posibilidad de interaccionar con otras personas de todo el mundo y acceder a todo tipo de información, no sólo ofrece ventajas para los ciudadanos. Lo que actualmente se conoce como "*Infodemia*" o sobreabundancia de información accesible desde cualquier plataforma o medios digitales, puede tener efectos tanto positivos como negativos en el ámbito de la seguridad tecnológica. Se hace costoso entre tal cantidad de datos encontrar fuentes fiables de información, ya que, cada vez es más habitual encontrar falsas propagandas con fines ilícitos o no fiables (fake news).

La correcta gestión de tal potencial, en un momento en el que la tecnología avanza a un ritmo vertiginoso, exige un esfuerzo para fomentar la cooperación de todos los actores involucrados en la investigación, desarrollo e implementación, de soluciones asistidas por IA. Una gestión que permita obtener el máximo rendimiento de los sistemas de información, aportando verdadero valor añadido a las Fuerzas y Cuerpos de Seguridad del Estado (FCSE), en su misión de proteger el libre ejercicio de los derechos y libertades, así como garantizar la seguridad ciudadana.

La digitalización, la disponibilidad y el acceso a grandes volúmenes de datos, así como la existencia de infraestructuras de procesamiento de datos de alto rendimiento y capacidad, son elementos esenciales para el desarrollo de la IA. Más allá de la inversión en la generación de nuevos conjuntos de datos e infraestructuras, también hay que garantizar la gestión eficiente de los existentes y el uso adecuado de los datos a lo largo de su cadena de valor según los principios de disponibilidad, integridad, fiabilidad y calidad.

Los objetivos específicos, definidos en el presente estudio, se centran en la definición de los principios orientadores en materia IA para la seguridad. Se pretende analizar cómo, gracias a las tecnologías emergentes validadas en proyectos de corte europeo y tratadas en los diferentes grupos de expertos, han surgido líneas de trabajo estratégicas en materia de IA para España.

Se van a presentar algunos de los proyectos de IA de los últimos años que ayudan a que los agentes españoles que velan por la seguridad de los ciudadanos (Fuerzas y Cuerpos de Seguridad, Guardias de Fronteras, Servicios de Control y Protección de Aduanas, etc.), se beneficien de nuevas herramientas para su trabajo operativo diario.

Por otro lado, y teniendo en cuenta que Europa seguirá desarrollando y mejorando los mecanismos para desarrollar los servicios TIC que ofrece a sus ciudadanos, es esencial poner en valor la vigilancia tecnológica y la inteligencia competitiva. La inclusión de nuevos procesos de Inteligencia Artificial en los sistemas de información existentes, el diseño de los nuevos espacios seguros de datos y la interoperabilidad de los mismos, supone un gran desafío.

2.- ESTADO DEL ARTE IA EN ÁMBITO EUROPEO

Mostrada en la introducción la necesidad de Europa de ser un actor competitivo en el sector tecnológico, la Unión Europea (UE) se está quedando atrás en varios ámbitos. De hecho, la economía digital global se está desarrollando, claramente, alrededor de dos potencias: Estados Unidos y China.

Para competir con estos gigantes tecnológicos, la UE está realizando grandes inversiones a través de Programas de financiación europeos. Se considera, que un mayor número de proyectos paneuropeos, en los que se ponen en común los recursos de todos los Estados Miembros, ayudará a alcanzar economías suficientes para ser más competitivos en los mercados globales.

La IA se está desarrollando de forma rápida. Se podría decir que a corto plazo cambiará nuestras vidas, pues mejorará la atención sanitaria (por ejemplo, incrementando la precisión de los diagnósticos y permitiendo una mejor prevención de las enfermedades), aumentará la eficiencia de la agricultura, contribuirá a la mitigación del cambio climático y a la correspondiente adaptación, mejorará la eficiencia de los sistemas de producción a través de un mantenimiento predictivo, aumentará la seguridad de los europeos y nos aportará otros muchos cambios que a día de hoy solo podemos intuir.

Al mismo tiempo, la IA conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, las discriminaciones, la intromisión en nuestras vidas privadas o su uso con fines delictivos, que deben ser tenidos en cuenta. Aunque Europa todavía se encuentra en una posición relativamente consolidada en relación a las aplicaciones de consumidores y plataformas on-line (lo que se traduce en una desventaja competitiva en lo que al acceso de datos se refiere), se están experimentando cambios importantes en el valor y la reutilización de los datos en distintos sectores.

Adicionalmente, Europa intentará seguir liderando el progreso de los fundamentos algorítmicos de la IA a partir de su propia excelencia científica. Existe la necesidad de tender puentes entre disciplinas que actualmente trabajan de manera independiente, tales como el aprendizaje automático y el aprendizaje profundo (caracterizados por su naturaleza interpretable limitada y por la necesidad de un gran volumen de datos para entrenar los modelos y aprender mediante correlaciones) y los enfoques simbólicos (en los que las normas se crean mediante intervención humana).

A pesar de lo que parecen múltiples ventajas, la adopción de IA en el ámbito de la seguridad también implica retos con respecto a derechos fundamentales, por lo que es vital encontrar el equilibrio adecuado para aprovechar los beneficios de esta tecnología sin poner en riesgo la privacidad y la presunción de inocencia.

Teniendo en cuenta todo lo anterior, para crear un ecosistema de excelencia que pueda respaldar el desarrollo sostenible y la adopción de la IA en el conjunto de la economía y la administración pública tanto de la UE como de sus Estados Miembros (EM), es necesario fomentar acciones en varios niveles: (1) Colaboración entre los Estados Miembros, (2) Centrar los esfuerzos de la comunidad investigadora. (3) Desarrollo de habilidades en el ámbito de la IA. (4) Apoyo a las PYMES y asociaciones con el sector privado.

Respecto a las aplicaciones prácticas, en la actualidad, las soluciones de IA ofrecen sobre todo la posibilidad de automatizar procesos. Esto se aplica, por ejemplo, al reconocimiento automático de imágenes en el ámbito médico, la seguridad o en la producción industrial. Antes era necesario realizar una inspección visual de un producto, ahora se pueden utilizar sensores y algoritmos.

También, tomando un ejemplo en el campo del procesamiento automático del lenguaje natural, se puede automatizar la comunicación, con clientes y usuarios de un determinado servicio a través de "chatbots". A corto plazo, estos avances reducirán los costes, optimizarán los procesos y contribuirán a reducir los tiempos de espera. Además, los asistentes inteligentes ya forman parte de la vida cotidiana de prácticamente todo el mundo desarrollado.

Así pues, por un lado, podemos hablar de "IA débil" o "IA supervisada" (Artificial Narrow Intelligence, ANI), que se refiere a los sistemas centrados en la resolución de problemas de aplicación concretos. La solución del problema se basa en métodos matemáticos e informáticos, que se desarrollan para unos requisitos específicos. El ser humano dota al sistema de las reglas necesarias para que el algoritmo pueda tanto entrenarse como proveer de unos resultados en base a las necesidades específicas. El sistema resultante es capaz de optimizarse a sí mismo. Los sistemas ANI funcionan reactivamente en un nivel de inteligencia superficial y no logran una comprensión más profunda de la solución del problema. ANI se centra principalmente en el cumplimiento de tareas claramente definidas y no varía su enfoque de los problemas.

Por otro lado, está la denominada "IA fuerte", también llamada "superinteligencia" o "inteligencia general artificial" (AGI), cuyo objetivo es alcanzar o superar las capacidades intelectuales de los humanos. La IA fuerte no sólo actúa de forma reactiva, sino también por iniciativa propia, actuando de forma inteligente y flexible. A día de hoy, es muy difícil hablar de un desarrollo pleno de la IA fuerte y se sigue discutiendo sobre si el desarrollo de una inteligencia de este tipo es siquiera posible. Sin embargo, la mayoría de los investigadores están de acuerdo en que este hito se alcanzará, pero no hay consenso sobre cuándo ocurrirá.

En este contexto, podemos hablar de las siguientes tecnologías de IA aplicadas en el ámbito de la seguridad: Generación de lenguaje natural, reconocimiento de voz, agentes virtuales[1], plataformas Machine Learning (ML), hardware optimizado con IA, plataformas de aprendizaje profundo (Deep Learning DL), biométricos, automatización de procesos robóticos, analíticas de texto y NLP (Procesamiento de Lenguaje Natural[2]), gemelos Digitales/Modelos de IA[3], defensa Cibernética, compliance (cumplimiento), redes Peer-to-Peer[4], reconocimiento de emociones (comportamientos anómalos) y reconocimiento de imagen y video.

La IA puede buscar fotos en las plataformas de redes sociales y compararlas con una amplia gama de conjuntos de datos para decidir cuáles son más relevantes. La tecnología de reconocimiento de imágenes también se puede utilizar para detectar matrículas, analizar a personas y sus opiniones, incluso verificar a las mismas basándose en su rostro.

[1] Agente informático o un programa capaz de interactuar con humanos. (Los chatbots son un buen ejemplo). Los agentes virtuales se están utilizando actualmente para el servicio al cliente y soporte, así como administradores de hogares inteligentes).

[2] Tecnología que utiliza el análisis de texto para comprender tanto la estructura de las oraciones, como su significado e intención, a través de métodos estadísticos y ML. El análisis de texto y NLP se utilizan actualmente en sistemas de seguridad, detección de fraudes o en análisis semánticos en redes sociales para identificar radicalismos. Aunque también se utilizan por una amplia gama de asistentes y aplicaciones automatizadas para extraer datos no estructurados.

[3] Digital Twin o gemelo digital es un constructor de software que cierra la brecha entre los sistemas físicos y el mundo digital. Es un modelo virtual de un objeto físico en tiempo real.

[4] Dos o más PC's se conectan y comparten recursos sin necesidad de que los datos pasen por un servidor centralizado

Respecto a futuras tendencias, cabe destacar la IA como Servicio (Artificial Intelligence as a Service, AIaaS[5]). IA como servicio, es decir, recursos y herramientas de desarrollo basados en SaaS[6], son cada vez más demandados.

3.- PLAN DE ACCIÓN EUROPEO PARA LA IA EN SEGURIDAD

Si nos centramos únicamente en el ámbito de la Seguridad Europea, el hito fundamental radica en la integración de las nuevas tecnologías con los sistemas tradicionales y la creación de sistemas híbridos con mejores capacidades, a un coste asumible.

La IA, puede ser una herramienta tanto para manejar las amenazas, como para aumentarlas. Su uso podrá ser extendido para acelerar la identificación y respuesta ante las vulnerabilidades y ataques dirigidos. El uso *de la nube y el Big Data*, suponen nuevos desafíos relacionados, ya que la navegación de los datos libres en el ciberespacio, aumenta la posibilidad de su robo o de su uso indebido.

Europa sigue desarrollando y mejorando los mecanismos para proteger los datos y los servicios conexos que ofrece a sus ciudadanos. El uso seguro y generalizado de productos y servicios basados en datos, base para el entrenamiento de los sistemas IA, supone establecer como prioridad a nivel internacional la definición de un marco jurídico que cumpla con los intereses tanto de los ciudadanos como los de las autoridades que velan por la seguridad.

Otra parte importante de la seguridad es la protección de los datos cuando estos se intercambian. Garantizar la continuidad de los controles de acceso a través de las cadenas de valor y la portabilidad de los datos en tiempo real, es un requisito fundamental tenido en cuenta actualmente por los organismos europeos que se encargan de regular el uso de la IA en el ámbito de la seguridad.

En el año 2018, se publicó la *Estrategia Europea sobre IA* (Comisión Europea, COM(2018) 237), donde evidenciaba que la IA pasaba de ser "*ciencia ficción*" a ser la base para resolver algunos de los principales retos de las sociedades actuales. En 2019 el *Grupo de Expertos de Alto Nivel*[7] (High Level Expert Group on Artificial Intelligence IA HLEG) sobre Inteligencia Artificial de la Comisión Europea publicó unas directrices sobre una IA fiable y una lista de evaluación para 2020, basándose en los valores comunes de todos los Estados Miembros (Espacio de Libertad, Seguridad y Justicia).

No se pretendía cambiar a legislación existente, eran recomendaciones no vinculantes, que previa consulta de los stakeholders (partes interesadas de corte industrial), marcarían los requisitos claves para una IA confiable socialmente en ámbitos

[5] Artificial Intelligence as a Service AIaaS: Nuevo Modelo de negocio de la IA como servicio. La IA como servicio (AlaaS) ayuda a las organizaciones a incorporar la funcionalidad y procesos de IA sin tener conocimiento o experiencia técnica dentro de la organización.

[6] Software as a Service (SaaS) o Software como Servicio: modelo de distribución de software donde el soporte lógico y los respectivos datos que maneja se alojan en los servidores de un proveedor, cuyo acceso es a través de Internet. El proveedor no solo proporciona el hardware, sino también el software correspondiente.

[7] El Punto Nacional de Contacto NCP de España para dicho grupo es el Dr. Enrique Belda Esplugues, Subdirector General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS), Secretaría de Estado de Seguridad, Ministerio del Interior.

como el de la seguridad, la protección de datos de carácter personal, la privacidad o las reglas de protección medioambiental.

A finales de 2018, y revisado en el año 2021, se publicó el primer *Plan Coordinado sobre IA* europeo donde los Estados Miembros, además de Suiza y Noruega, adquirían un compromiso conjunto para fomentar el desarrollo y la utilización de la IA en Europa. Exponía los cambios de política y las inversiones necesarias en los Estados miembros para reforzar el liderazgo de Europa en materia de IA. Fueron cuatro los ámbitos clave que se tuvieron en cuenta: aumento de la inversión, mayor disposición de los datos (espacios seguros de datos), fomento del talento y garantizar la confianza.

Al respecto, el Consejo de la Unión Europea, en sus conclusiones de 2019 relativas al *Plan Coordinado sobre IA*, destacó la importancia de garantizar el pleno respeto de los derechos de los ciudadanos europeos y pidió que se revisase la legislación pertinente en vigor con vistas a garantizar su adaptación a las nuevas oportunidades y retos.

Con el propósito de fomentar un marco de confianza de la ciudadanía en IA basado en el respeto de los principios éticos, legales y morales del espacio europeo, el 11 de septiembre de 2019, el Comité de Ministros del Consejo de Europa creó *el Comité Ad Hoc sobre Inteligencia Artificial (CAHAI).*

El *CAHAI* tiene una composición única ya que reúne a EM y observadores, así como integrantes de la sociedad civil, el mundo académico y el sector privado. Trabaja en estrecha colaboración con otras instituciones internacionales, como la UNESCO, OCDE y la Unión Europea. La SGSICS en representación del Ministerio del Interior junto con el Ministerio de Justicia, son los representantes españoles en dicho Comité.

En abril de 2020 fue publicado el *Libro Blanco de la Comisión Europea* (A European approach to excellence and trust. European Commission Brussels, 19.2.2020 COM2020), antecedente de una consulta pública que contó con una alta participación internacional. El "*White Paper*" fue acompañado de un "*Informe sobre las implicaciones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*" (Comisión Europea, 2020), cuyas conclusiones lanzaban una serie de lagunas que la legislación vigente debía subsanar en materia de seguridad.

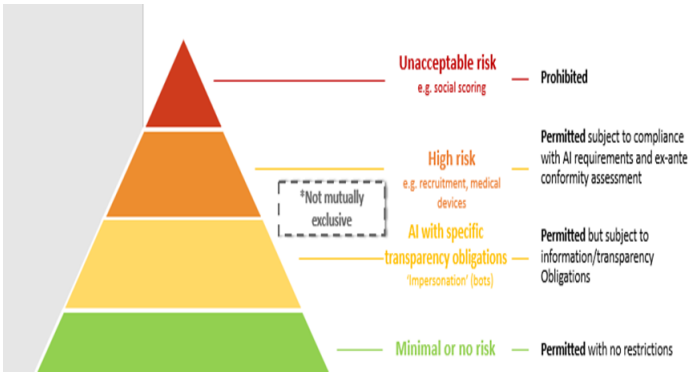
El Consejo Europeo solicitó en octubre de 2020 una definición más clara sobre los usos de IA que debían ser considerados de alto riesgo, instando además a afrontar determinadas problemáticas como el sesgo, la opacidad o el cierto grado de imprevisibilidad en comportamientos parcialmente autónomos, de manera que se garantizase su compatibilidad con la aplicación de las normas jurídicas vigentes, y consecuente salvaguarda de los derechos fundamentales.

Actualmente la Comisión Europea, con su publicación el 21 de abril de 2021 de su *Propuesta de Reglamento del Parlamento Europeo y del Consejo* por el que se establecen normas armonizadas en materia de Inteligencia Artificial y se modifican determinados actos legislativos de la Unión, propone nuevas normas y medidas destinadas a convertir a Europa en el centro mundial de Inteligencia Artificial adaptada a la Era Digital.

No obstante, la propuesta era muy ambiciosa. La revisión del texto por los diferentes Estados Miembros[8] ha sido costosa. Se puede ver en la revisión del articulado, que en ocasiones, pretende desarrollar una normativa de protección de datos *Ad Hoc* para casos de usos de procedimientos de IA, que por ejemplo, en España, se encontraría ya cubierta por el reciente Reglamento General de Protección de Datos RGPD (Reglamento (UE) 2016/679), la LOPDGDD (Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales) nacional, y las normas nacionales de trasposición de la Directiva UE 680/2016, dando pie a contradicciones, o incluso pudiendo llegar a generar situaciones de inseguridad jurídica.

Entre los objetivos generales del Reglamento, se codifica la posibilidad de dar respuesta a las necesidades impuestas por el nuevo panorama tecnológico, en el que los sistemas aplicados a la seguridad asistidos por IA tendrán un impacto enorme en el ámbito de sectores como la Seguridad. Si se diseña y utiliza adecuadamente la IA puede convertirse en una tecnología estratégica, que permita a las autoridades enfrentarse eficazmente a nuevos desafíos y modalidades de delincuencia.

La propuesta de Reglamento si tiene en cuenta que la forma de entender el trabajo policial va a ir cambiando, tanto por los efectos organizativos en el planeamiento y asignación de recursos, como por la introducción de un nuevo paradigma de prevención y anticipación frente al enfoque reactivo.



Riesgos usos IA-Prioridades Estratégicas 2019-2024.
Fuente: ec.europa.eu.

Se considera de interés señalar, cuando por ejemplo, se regula la utilización de sistemas biométricos *RBI* (Remote Biometric Identification) *"Identificación Biométrica Remota en tiempo real"* por parte de las autoridades policiales, riesgo y resultado no se diferencian. Y es que, un resultado erróneo, puede provocar un resultado físico no deseado para los ciudadanos, pero todavía es mucho más grave que dicha errata atente contra derechos fundamentales, como la vida o la integridad física, si no se ha tenido en cuenta el riesgo por parte de las Fuerzas y Cuerpos de Seguridad del ámbito europeo.

De hecho, el uso en directo de sistemas RBI en espacios de acceso público con fines policiales está prohibido, en principio. Se definen y regulan excepciones estrictas, por

[8] El Ministerio del Interior España, participa en la Revisión del Draft del Reglamento Europeo de IA a través del grupo IXIM del Consejo Europeo, en materia de cooperación policial. En dicha revisión trabajan activamente la Secretaría de Estado de Seguridad -SGSICS, la DGRIE, la DGPN y la DGGC-UTPJ.

ejemplo, cuando sea necesaria su aplicación para la búsqueda de un menor desaparecido, para prevenir una amenaza terrorista concreta e inminente, o para detectar, localizar, identificar o enjuiciar a un autor o sospechoso de un delito grave. Su uso estará sujeto a la autorización de un órgano judicial u otro organismo independiente y a los límites adecuados desde el punto de vista de la duración, el alcance geográfico y las bases de datos exploradas.

Actualmente los cuerpos policiales están utilizando aplicaciones en diferentes ámbitos y especialidades como la investigación y la obtención de información, la criminalística, incluyendo la obtención de investigación, o la prospectiva. Dichas aplicaciones tendrán un impacto enorme en la forma de entender el trabajo policial tanto por los efectos organizativos en el planeamiento y asignación de recursos (mayor eficacia y mejoras de la inteligencia policial) como por la introducción de un nuevo paradigma (el de la prevención y anticipación) frente al enfoque reactivo propio de las fuerzas y cuerpos de seguridad.

Algunos expertos consideran que el trabajo policial tendrá más que ver con la predicción e identificación de patrones criminales o la gestión de riesgos derivados de la comisión de actos delictivos. En este sentido las policías, a futuro tendrán que tener en cuenta algunos retos de la integración de la Inteligencia Artificial en el trabajo policial en España.

3.1.- Definición de IA

El término "algoritmo" se usa ampliamente en el contexto de Big Data, aprendizaje automático e IA. En informática, un algoritmo es una secuencia de comandos para que una computadora transforme una entrada en una salida. Un ejemplo sencillo de algoritmo sería una secuencia de comandos para ordenar una lista aleatoria de personas según la edad. En dicho ejemplo, se proporciona a una computadora una la lista aleatoria (entrada), se ejecuta un algoritmo diseñado previamente (comandos) y se obtiene una lista ordenada por edad (salida).

Los algoritmos se utilizan a menudo para hacer predicciones, por ejemplo, predicciones sobre el perfil de las personas que probablemente comprarán un determinado producto, el pronóstico del tiempo, la detección de correo no deseado o las nacionalidades de las personas que cruzan una frontera con más frecuencia. Para una tarea específica, se alimenta un algoritmo con datos creando un modelo que se utiliza en la práctica para una tarea del mundo real. El término aprendizaje automático, al que ya se ha hecho referencia, supone contar con un algoritmo en el estado “sin procesar” (ya diseñado) y entrenarlo sucesivamente con la ingesta de datos para obtener finalmente un modelo.

El término “inteligencia artificial” es más difícil de definir. No se refiere a algo tangible, sino a los desarrollos y procesos tecnológicos actuales en general. La mayor parte de lo que se discute “bajo el paraguas de IA” se refiere al aumento automatización de tareas mediante el uso de aprendizaje automático (IA supervisada) e incluso alcanzar la toma de decisiones de manera autónoma a través de aprendizaje no dirigido por un humano (IA no supervisada).

El hecho de que máquinas y sistemas de información y comunicaciones tengan capacidad de autogestión, llegando a estimar patrones o incluso a tomar el control de

eventos o acontecimientos en los que interviene, supera con creces la capacidad humana. Y en último término, la capacidad de gobernanza humana sobre dichos sistemas "inteligentes" puede llegar a verse comprometida. Constituye, por tanto, un reto de gran magnitud no sólo su adecuada interpretación, si no también, cómo se van a implementar dichos procesos en la práctica.

La Organización para la Cooperación y el Desarrollo Económicos, OCDE, define la IA como: "*un sistema que puede, para un conjunto de objetivos específicos, realizar predicciones, recomendaciones o decisiones que influyan en entornos reales o virtuales"*.

El viernes 9 de Marzo de 2023, los representantes de los grupos políticos del Parlamento Europeo que trabajan en la Ley de IA (Consolidación del Reglamento de armonización en materia de IA 2021), llegaron a un acuerdo político sobre una de las partes más sensibles del texto legal, la definición de IA: "*Sistema basado en una máquina que está diseñado para operar con diferentes niveles de autonomía y que puede, para objetivos explícitos o implícitos, generar resultados tales como predicciones, recomendaciones o decisiones que influyen en la salud física o entornos virtuales*".

La definición se superpone en gran medida con la de la OCDE y está estrechamente alineada con el trabajo de las organizaciones internacionales que trabajan en inteligencia artificial, para garantizar la seguridad jurídica, la armonización y la amplia aceptación como el Consejo de Europa.

Se desglosa del texto adjunto que acompaña a la definición de IA actualizada por la UE, la distinción entre la IA aplicada a sistemas de software más simples (enfoques de programación) frente a aquellos sistemas IA que buscan la autonomía predictiva aplicada a determinados contextos específicos. Se está regulando, lo que en ámbito científico se estudia desde hace años como la diferencia entre "inteligencia artificial débil" e "inteligencia artificial fuerte".

La IA permite el desarrollo cada vez más complejo de **algoritmos** y conjuntos de instrucciones para resolver un problema. Los algoritmos han pasado de ser estáticos (cuando los programadores y programadoras diseñan los criterios de toma de decisiones) a dinámicos.

Los algoritmos de aprendizaje automático tienen la capacidad de aprender de datos y experiencias para tomar decisiones, generando sus propias instrucciones, que ya no son las originales definidas por la persona que lo programa. El aprendizaje profundo ya emula redes neuronales complejas (*Deep Learning*).

A través de agregar y procesar grandes cantidades de datos que se generan diariamente, convirtiéndolos en información útil para las fuerzas y cuerpos de seguridad de los EM, la IA puede ayudar a prevenir el crimen reconociendo patrones, encontrando anomalías y utilizando el análisis predictivo para anticipar los futuros movimientos de terroristas y criminales, tanto en el ámbito físico como en el digital. También puede ser de gran utilidad en investigaciones sobre delitos que ya han tenido lugar. Generalmente, este tipo de herramientas, se alimentan de datos históricos, en gran parte de fuentes oficiales (tiempo, lugar y tipo de delitos cometidos). Se pueden complementar con variables ambientales (densidad de población).

De esta manera, los investigadores utilizan cada fuente de datos digital a su máximo potencial ahorrando tiempo en la revisión de evidencias. Con Big Data y algoritmos cada vez más sofisticados es posible hacer análisis y predicciones cada vez más precisas en tiempo real. Una ventaja de los algoritmos es que estos, a diferencia de las personas, toman decisiones consistentes cuando se enfrentan a los mismos escenarios (no tienen cambios de criterio o humor).

3.2.- Ejes Estratégicos Europeos (EE) de trabajo en materia de IA.

El trabajo global del Grupo de Expertos en Inteligencia Artificial de Comisión Europea (HLEG) ha sido fundamental para el desarrollo del enfoque de la Comisión relativo a la IA. Las recomendaciones del grupo han servido de base para las iniciativas políticas adoptadas por la Comisión y sus EM. Entre las iniciativas surgidas se pueden destacar: La comunicación sobre el fomento de la confianza en la IA centrada en el ser humano. Las aportaciones al Libro Blanco sobre IA: un enfoque europeo de la excelencia y la confianza y los aportes al Plan coordinado actualizado sobre IA de CE.

Los Ejes Estratégicos en materia IA (EE) objetos de estudio en el presente trabajo son:

EE1.- Posicionar al usuario final como elemento primordial del desarrollo de IA, utilizando potencial tecnológico europeo como catalizador. La IA tiene podría tener el potencial suficiente para transformar el mundo a mejor. Sus capacidades podrían mejorar la atención sanitaria, reducir el consumo de energía, hacer más seguros los coches y permitir a los agricultores utilizar agua y los recursos naturales de forma más eficiente. La IA puede utilizarse para predecir el cambio climático, mejorar la gestión del riesgo financiero y proporcionar las herramientas para fabricar con menos residuos, productos adaptados a nuestras necesidades. La IA también podría ayudar a detectar fraudes y amenazas de ciberseguridad, y permitir a las fuerzas y cuerpos de seguridad luchar contra la delincuencia de forma más eficiente.

Sin embargo, este potencial tecnológico también trae consigo nuevos retos para el futuro del trabajo y plantea cuestiones éticas y legales de especial relevancia.

Para afrontar estas cuestiones, la CE a través de su comunicado "*Building Trust in Human-Centric Artificial Intelligence"* (Comisión Europea, 2019, COM(168)), ha puesto de manifiesto que la confianza es un requisito previo para garantizar un enfoque de la IA centrado en el ser humano: la IA no es un fin en sí misma, sino una ***herramienta que tiene que servir a las personas con el objetivo final de aumentar el bienestar humano***. Para lograrlo, debe garantizarse la fiabilidad de la IA, integrando en el desarrollo de la tecnología los valores en los que se basan nuestras sociedades.

EE2.- Evaluación de la adecuación tecnológica al nuevo sistema de necesidades funcionales y operativas de las Fuerzas y Cuerpos de Seguridad en condiciones reales de uso (Eu-Lisa y EUROPOL).

Debido al relevante papel tanto de eu-LISA, en su misión de dar apoyo tecnológico a los estados miembros para una Europa más segura, como de EUROPOL en calidad de lo que podría calificarse como supra usuario en términos tecnológicos y operativos, resultan de vital importancia a la hora de identificar y canalizar los avances en tecnología

IA que resulten realmente efectivos para las Fuerzas y Cuerpos de seguridad *(Law Enforcenment Agencies LEAs*).

Parece recomendable, por tanto, contar con este tipo de agentes que sirvan para fomentar la realización y estandarización de protocolos de pruebas de aceptación de soluciones tecnológicas asistidas por IA, identificando, coordinando y ayudando a definir los elementos clave que permitan medir el desempeño y adecuación del sistema que se pretende desarrollar.

EE3.- Fomentar un marco de confianza de la ciudadanía en IA basado en el respeto de los principios éticos, legales y morales del espacio europeo. Con este propósito el 11 de septiembre de 2019, el Comité de Ministros del Consejo de Europa creó el Comité Ad Hoc sobre Inteligencia Artificial (CAHAI). Establecido por un período de 2 años, se reunió por primera vez del 18 al 20 de noviembre de 2019 en Estrasburgo.

El CAI (evolución del CAHAI), es el Comité sobre IA del Consejo de Europa para el período 2022-2024, encargado de establecer un proceso de negociación internacional que permita elaborar un marco jurídico para el desarrollo, la concepción y la aplicación de la IA.

Se basa en las normas del Consejo de Europa en materia de derechos humanos, democracia y Estado de Derecho. El CAI reúne a los estados miembros y a observadores, así como integrantes de la sociedad civil, el mundo académico y el sector privado. Convencido de la importancia de una reflexión global y de aunar esfuerzos en este ámbito, el Comité sobre IA, trabaja en estrecha colaboración con otras instituciones internacionales, como la UNESCO (La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura), la OCDE (Organización para la Cooperación y el Desarrollo Económicos) y la UE (Unión Europea).

EE4.- Estrategia Común de Datos – Arquitecturas y espacios seguros de datos para la IA (Eu-Lisa y Europol). La Comisión Europea publicó en febrero de 2021 el documento: "La Estrategia Europea de Datos" (Comisión Europea, 2020) en la que consolidó la intención de crear un Mercado Único de Datos, para que los actores del sector público y privado tuviesen fácil acceso a datos industriales y públicos de calidad, con la finalidad de impulsar, en otros puntos, el entrenamiento de los algoritmos base de determinadas tecnologías.

Es por lo que los espacios seguros de datos van a cobrar especial importancia durante el período 2021- 2027, y habrá que atender tanto a su infraestructura de carácter tecnológico como a la gobernanza de los mismos.

Se han ido proponiendo desde principios del año 2021 varias medidas de tipo legislativo y financiero para implementar dichos espacios. Entre ellas, el 25 de noviembre de 2020 se adoptó a *Ley de Gobernanza de Datos* (Comisión Europea, 2020, 767 final) que podía ser complementada por legislaciones sectoriales para su acceso y uso, además de los mecanismos necesarios para implantar la interoperabilidad de los sistemas.

Por motivos de seguridad nacional y seguridad pública, la Ley de Gobernanza de Datos no regulaba la accesibilidad. Ese es el motivo por el qué en el año 2021, el Consejo Europeo, declaraba la necesidad de acelerar la creación de espacios comunes de datos, y

solicitaba de la Comisión Europea, las restantes medidas necesarias para la implantación de los mismos.

Las problemáticas que se ha encontrado la Unión Europea para afrontar esta tarea son, en primer lugar, la fragmentación de los EM. Varios habían empezado a desarrollar su propio marco jurídico en relación con el tratamiento de datos con fines de investigación, o incluso, el uso de datos de titularidad privada por parte de autoridades gubernamentales en función de su competencia. Otros Estados, no habían empezado todavía, generando diferencias en el mercado interior de datos.

En segundo lugar, la disponibilidad de los datos: El valor de los datos reside en su uso y reutilización. En la actualidad, no hay suficientes datos disponibles para que sean reutilizados y, por ejemplo, sean destinados para el entrenamiento los algoritmos base de los procesos de IA. Las problemáticas empiezan por la titularidad de los datos, siguen por la identificación de los usuarios de los datos, y pueden llegar hasta la naturaleza que tienen los mismos. (Si tienen carácter personal, no personal, o se combinan ambas categorías).

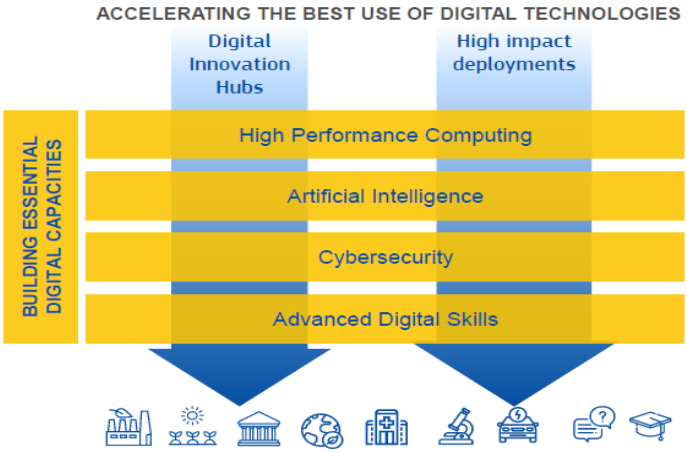
En tercer lugar, el beneficio general para la ciudadanía. Los datos, considerados como bienes de tipo de público, se crean en las sociedades por sus ciudadanos, y pueden ser aprovechados en muchas ocasiones para hacer frente a situaciones de emergencia y para mejorar los servicios públicos. De hecho, pueden llegar incluso, haciendo un buen uso de los mismos, a garantizar una lucha más eficaz contra el crimen organizado, el terrorismo y la protección de fronteras exteriores.

3.3.- Mecanismos financiación europeos para IA.

Para contrarrestar el poder de las grandes empresas tecnológicas es necesario reformar los mercados de bienes y servicios, eliminar las barreras de entrada y salida de los productos y el conocimiento, así como fortalecer y modificar las políticas de defensa y seguridad en materia de inversión. El presupuesto de la UE a largo plazo, también conocido como Marco Financiero Plurianual (MFP), impulsa el desarrollo de las tecnologías digitales, a través de los diferentes Programas Marco. Instrumentos como el Programa Europa Digital (DEP) hacen de engranaje con los Programas de Seguridad Interior (FSI y BMVI) y los Programas Horizonte Europa y Horizonte 2020 (I+D+i). Además, la Comisión Europea ha propuesto un nuevo instrumento de recuperación, tras la crisis de la COVID-19 denominado Next Generation EU. Los principales Programas de Financiación activos de la UE en materia de IA, de los que las Fuerzas y Cuerpos de Seguridad del estado se benefician, son:

a) Programa EUROPA DIGITAL 2021-2027 (Digital Europe Programme)

El Programa Europa Digital *(DEP)* tiene por objetivo acelerar la recuperación económica e impulsar la transformación digital en Europa. Intentará fortalecer a los Estados Miembros de la Unión con inversiones en cinco áreas de trabajo, que son: (1) Capacidades de supercomputación y procesamiento de datos. (2) Capacidades centrales de inteligencia artificial (IA), como espacios seguros de datos y bibliotecas de algoritmos de IA**.** (3) Ciberseguridad. (4) Mejora en el uso de las competencias digitales en la sociedad y la economía de la UE. (5) Apoyo a la digitalización de empresas y administraciones públicas.



Estructura Programa EUROPA DIGITAL. Fuente: EuropeanComission.eu.

El Programa de trabajo DEP está diseñado por DG-CONNECT (Dirección General de Redes de Comunicación, Contenido y Tecnología de Comisión Europea) para llenar el vacío entre la investigación y el despliegue de tecnologías digitales. Llevará los resultados de la investigación al mercado en beneficio de los ciudadanos y las empresas de Europa, en particular las pequeñas y medianas empresas (PYME). Inversión prevista de 7.600 millones de euros.

En España, la autoridad nacional es el Ministerio de Asuntos Económicos y Transformación Digital, representado a través de la SEDIA (Secretaría de Estado de Digitalización e Inteligencia Artificial). Se trabaja a nivel Interministerial. Las dos líneas principales sobre el despliegue de tecnologías aplicadas al ámbito de la Seguridad y de las FCSE son: (1) Implementar un Espacio Seguro de Datos Europeo**,** común, para poder realizar pruebas, capacitación y validación de algoritmos IA y desarrollar una arquitectura de referencia, para recopilar datos que sean interoperables. (2) Aumentar los medios tecnológicos y las capacidades de las Fuerzas y Cuerpos de Seguridad europeas, en el uso de la IA y la Ciberseguridad, para la gestión de grandes cantidades de datos.

b) Programa HORIZONTE2020 2014-2020 (Horizon2020).

Horizonte 2020 (H2020) es el Programa Marco (PM) de Investigación e Innovación de la Unión Europea que estuvo activo durante el periodo 2014-2020. Contó con un presupuesto total de 77.028 millones de euros, para financiar iniciativas y proyectos de investigación, desarrollo tecnológico, demostración e innovación. Horizonte 2020 agrupó y reforzó las actividades que durante el periodo 2007-2013 eran financiadas por el 7º PM de Investigación y Desarrollo (FP7), las acciones de innovación del PM para la Innovación y la Competitividad (CIP) y las acciones del Instituto Europeo de Innovación y Tecnología (EIT). Incluyó *topics* y llamadas específicas para IA.

c) Programa HORIZONTE EUROPA 2021-2027 (Horizon Europe).

Horizonte Europa (9º Programa Marco CE) es un Programa de financiación europeo de siete años de duración (2021-2027), para la Investigación, el Desarrollo y la Innovación (I+D+i), que continua el trabajo del Programa Europeo Horizonte 2020 (8º PM). Dentro de la Comisión Europea, el 9º Programa de Trabajo está diseñado, coordinado y

financiado por la DG-HOME, en colaboración con otras Direcciones Generales como DG-SANTE (Dirección General de Salud y Seguridad Alimentaria de Comisión Europea), DG-REFORM (Dirección General de Apoyo a las Reformas Estructurales de Comisión Europea) o DG-CONNECT.

Horizonte Europa incluye un presupuesto específico para "*Digital, industria y espacio*". Este presupuesto desarrollará la investigación y la innovación de alto nivel en tecnologías habilitadoras, tales como la Inteligencia artificial. La autoridad nacional en España para el Programa Horizonte Europa es el Ministerio de Ciencia e Innovación, representado por el Centro para el Desarrollo Tecnológico e Industrial (CDTI), órgano adscrito al mencionado Ministerio. Colabora con el Ministerio del Interior España y sus organismos dependientes para la preparación y desarrollo de las propuestas y proyectos, subvencionadas dentro del II Pilar, Cambios Globales y Competitividad Industrial, Cluster III, "Seguridad Civil para la Sociedad", donde se incluye también llamadas específicas para Inteligencia Artificial.

d) Fondos de Seguridad Interior. Marco financiero ISF (FSI) Y BMVI 2021-2027.

Los Fondos de Seguridad Interior FSI (Fondo para la cooperación policial, lucha contra crimen organizado y terrorismo) y BMVI (Fondo para la gestión integrada de las fronteras y visados), conforman el Marco Financiero Plurianual 2021-2027. El FSI-BMVI se gestiona conjuntamente por la Comisión Europea y los Estados Miembros a través de la aprobación de Programas. Para el marco 2021-2027 se tiene un presupuesto total de 1.931 millones de euros y España cuenta con una asignación inicial de 79.5 M de euros para FSI y unos 300M para BMVI. España podrá dar una respuesta a la Comisión Europea acerca de las necesidades económicas sobre los *proyectos tecnológicos y de seguridad,* tanto en el ámbito fronterizo como en los ámbitos antiterrorista, radicalismos y crimen organizado.

Gracias a este fondo es posible mejorar y facilitar el intercambio de información entre las autoridades competentes y los órganos y organismos de la Unión y, en su caso, con terceros países y organizaciones internacionales. Es por ello, que las inversiones a través de la co-financiación en materia IA se hacen evidentes en numerosos proyectos de gran magnitud en los que trabaja actualmente el Ministerio del Interior España, para los que uno de los principales beneficiarios es la Guardia Civil.

Algunos de los objetivos que tocan de cerca la implementación de procesos IA en el campo de la seguridad son: la *compra y adquisición* de sistemas de Tecnologías de Información y Comunicaciones (TIC), las pruebas asociadas, así como mejora de interoperabilidad de los sistemas y la calidad de los datos. (procesamiento automatizado de datos biométricos e identificativos, por ejemplo). También apoyo a redes temáticas o transversales de unidades nacionales especializadas para mejorar la confianza mutua, intercambio y difusión de conocimientos, información, experiencias y mejores prácticas, puesta en común de recursos y conocimientos en centros de excelencia conjuntos.

4.- EL MINISTERIO DEL INTERIOR ESPAÑA EN LOS PROYECTOS EUROPEOS DE INNOVACIÓN TECNOLÓGICA EN MATERIA IA

Con la pandemia mundial de COVID-19, se ha producido en los últimos años, un aumento en la delincuencia online[9]. Se generan mayor número de falsificaciones y los bienes que se distribuyen, en general, son de calidad inferior. Se investigan nuevos métodos para financiar la delincuencia organizada y los diferentes tipos de fraude, incluso en aquellos casos que tienen relación con el campo de los medicamentos (dispositivos médicos y vacunas).

La *Estrategia de Schengen* (Comisión Europea, COM (2021) 277 final), subraya el importante papel del uso de tecnologías para control en las fronteras interiores y exteriores, como alternativa a los controles físicos fronterizos de carácter temporal ante las crisis sufridas en los últimos años. Tecnologías como la IA, aplicada al reconocimiento facial avanzado, permiten controlar a los pasajeros de los vehículos que traspasan un control fronterizo terrestre (frontera física) o marítimo (por ejemplo, ferry).

El Sistema de Entrada-Salida (*EES*[10]), actualmente financiado con Fondos de Seguridad Interior de Comisión Europea, Instrumento de Protección de Fronteras y Visados, se espera que entre en funcionamiento a finales del año 2023, aunque para la Comisión Europea y para sus Estados miembros es difícil encontrar el equilibrio entre un paso fronterizo sin interrupciones para viajeros y al mismo tiempo velar por la seguridad de la información sobre los mismos.

Varios proyectos de investigación H2020 han desarrollado con éxito soluciones para el paso controlado y seguro de viajeros en fronteras exteriores, abordando también los desafíos que se dieron en las fronteras franco-británicas después de la retirada del Reino Unido de la UE. Las autoridades de la región francesa de *Hauts-de-France* utilizaron los resultados de un proyecto de investigación en seguridad, llamado *FastPass15, FP7*, que terminó en 2017, y cuya finalidad consistía en facilitar los viajes en la frontera franco-británica.

Se debe hacer mención al proyecto de investigación *ABC4EU* de la UE (FP7-SEC-2012.3.4-6**:** Enhancing the workflow and functionalities of Automated Border Control ABC gates, en el que participó el Ministerio del Interior Español, SGSICS, 2014 a 2018). En dicho proyecto se prepararon las capacidades para el próximo Sistema de Entrada-Salida de pasajeros (EES). Se estaba produciendo una necesidad imperiosa en ese momento de unificar y armonizar tecnología para el control de fronteras exteriores en relación con la gestión de pasaportes electrónicos, biometría, diseño de puertas, interfaz humana, procesos, intercambio de certificados *PKD* (Directorio de Claves Públicas), señalización e interoperabilidad.

Por otro lado, la Iniciativa de Frontera Inteligente de la UE agrega un nuevo enfoque al tenerse en cuenta en el desarrollo de ABC: La inclusión de un sistema de protocolo de

[9] Portal Estadístico de Criminalidad perteneciente al Ministerio del Interior del Gobierno de España.
[10] El Entry Exit System EES, Sistema informático automatizado para registrar viajeros de países no pertenecientes al espacio Schengen, tanto titulares de visados de corta duración y viajeros exentos de visado, cada vez que crucen una frontera exterior de la UE.

transporte en tiempo real RTP, para control de nacionales de terceros países y un Sistema para poder entrar y salir del espacio Schengen (EES).

ABC4EU identificó los requisitos para un sistema ABC integrado, interoperable y respetuoso de los derechos de los ciudadanos, teniendo en cuenta la experiencia obtenida de los pilotos y proyectos anteriores y las necesidades futuras derivadas de la iniciativa Frontera Inteligente[11] y otras iniciativas nacionales y de la UE. El proyecto se centró en armonizar el diseño y las características operativas de ABC Gates, utilizando los pasaportes de segunda generación de la UE y otros documentos de viaje aceptados. Además, RTP y EES se probaron específicamente en el proyecto para evaluar su viabilidad y desarrollar un nuevo concepto *C4I-Computering for Intelligence* de gestión de fronteras.

El proyecto *CLOSEYE*, tiene especial relevancia porque fue el primer proyecto coordinado por un LEA (Law Enforcenment Agency) en concreto, el Ministerio del Interior de España, representado por la Guardia Civil (Jefatura de Fiscal y Fronteras). Se realizó una evaluación colaborativa de tecnologías de vigilancia de fronteras en entornos marítimos mediante la validación pre-operativa de nuevas soluciones tecnológicas. Las soluciones innovadoras con las que se trabajó en el proyecto abarcaron plataformas, sensores y tecnologías de Información y Comunicaciones (TIC), que promovían una vigilancia más rentable, mejoraban la discriminación del tráfico de embarcaciones y respaldan el proceso de toma de decisiones. Contribuyeron también a mejorar el conocimiento de la situación en los centros de coordinación, el intercambio de información en tiempo real entre diferentes organismos y los tiempos de reacción.

El proyecto *ANDROMEDA*, H2020, tuvo por objetivo ampliar el alcance del Entorno Común de Intercambio de Información Europeo (CISE) aplicado también entre fuerzas policiales y fuerzas armadas y a las fronteras terrestres. Se apoyaba en la red creada por los Centros Nacionales de Contacto, Frontex y EMSA a través de mayores capacidades, incluido el intercambio transnacional de información útil y disponible, y los procedimientos y mecanismos asociados, apoyando así la creación de un entorno común de intercambio de información.

El proyecto demostrador H2020 *COMPASS2020*, coordinado por Portugal, validó drones submarinos para prevenir la delincuencia transfronteriza a través de la vigilancia marítima y el proyecto H2020 *FOLDOUT (2018-2022),* cuyo objetivo consiste en mejorar la detección del tráfico de emigrantes en áreas densamente boscosas. Combina varios sensores y tecnologías y los fusiona de forma a través de *machine learning* en una plataforma de detección inteligente. Aunque no participó el Ministerio del Interior español, sí que España estuvo representada en el consorcio por *Eticas Research and Consulting S.L*. Socio Industrial, cuya participación se traduce en *identificar vulnerabilidades algorítmicas de caja negra y reentrenar la tecnología impulsada por IA con mejores datos y contenido de origen.*

La agenda de lucha contra el terrorismo de la UE, anteriormente mencionada, marca la importancia de la investigación aplicada a seguridad para ámbitos como el

[11] Iniciativa Fronteras Inteligentes de la UE: acceso más fácil y una mayor seguridad en el espacio Schengen desde 2011. Combina EES con PNR (Passenger Name Record). Ambos proyectos desarrollados, gestionados, implementados y mantenidos a nivel nacional por la SGSICS-Ministerio del Interior.

procesamiento de datos y la detección y análisis de contenido terrorista y radicalismos violentos on-line por parte de las Fuerzas y Cuerpos de Seguridad Europeos.

El proyecto *RED ALERT*[12] *H2020-IA* ha desarrollado tecnologías para detectar con rapidez la radicalización on-line, sirviendo de apoyo a los esfuerzos globales en la lucha contra el terrorismo**.** Para las organizaciones extremistas o terroristas, internet es un medio de combate psicológico, difusión de desinformación, propaganda maliciosa, y reclutamiento de nuevos miembros. Las redes sociales se han convertido en uno de los métodos preferidos para captar a individuos vulnerables.

Al no disponer de las herramientas adecuadas para identificar eficazmente el contenido terrorista en internet, las fuerzas y cuerpos de seguridad se ven obligadas a depender de soluciones "*antispam*" privadas, informes de usuarios y análisis humano. Esto puede significar que parte de la actividad terrorista quede sin detectar, lo que, en algunos casos, puede llegar a tener consecuencias negativas para el pleno desarrollo de la función policial.

Tiene como objeto el desarrollo de herramientas de análisis semántico, fotográfico y de vídeo en redes sociales y fuentes abiertas, para detectar radicalismos a través del procesamiento de grandes cantidades de datos desestructurados. (Ministerio del Interior-Guardia Civil-Servicio de Información) 2017-2020. El Coordinador es SIVECO, empresa informática de Rumanía.

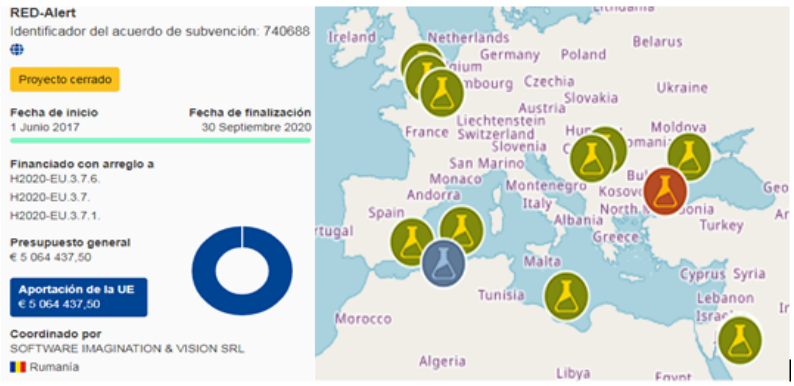


Figura 3-6 Consorcio Proyecto H2020 RED ALERT. Fuente: Cordis.eu

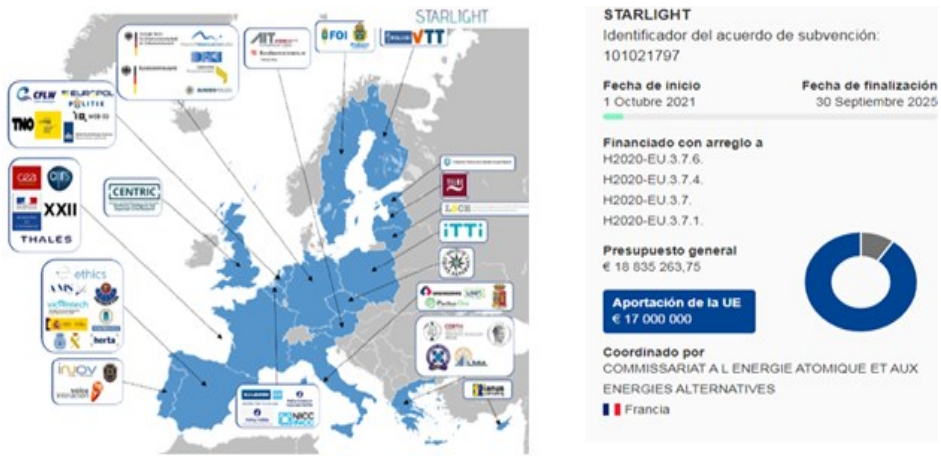
El proyecto europeo *STARLIGHT*[13] *H2020-AI,* que comenzó en 1 de Octubre de 2021, durante 48 meses, *validará procesos de Inteligencia Artificial*, por parte de las Fuerzas y Cuerpos de Seguridad Europeas. El Ministerio del Interior de España tendrá un

[12] *RED ALERT* Real-time Early Detection and Alert System for Online Terrorist Content based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing. SEC-12-FCT-2016-2017 - Technologies for prevention, investigation, and mitigation in the context of fight against crime and terrorism.

[13] *Proyecto H202 STARLIGHT*: Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats. Su duración es de 48 meses revirtiendo en España 1.987.073 €, siendo 293.750 € la ayuda correspondiente al Ministerio del Interior España. Financiación total CE-DGHOME para el Proyecto: 18M de euros

papel relevante, liderando tareas de análisis y especificación de requisitos operativos, casos de uso y pilotos propuestos.

Coordinado por Ministerio Interior Fracés (Commissariat a l'Energie Atomique et aux energies alternatives CEA). En total 53 socios de 18 países, 17 Fuerzas y Cuerpos de Seguridad europeos y 7 socios españoles: Ministerio del Interior (SGSICS, PN-Sistemas Especiales y GC-Grupo de Apoyo Operativo), Universidad Politécnica de Madrid (UPM), Vicomtech, Herta Seguridad SL, Plus Ethics, Ertzaintza y Advanced Model Solutions SL.



Consorcio Proyecto H2020IA STARLIGHT Fuente: Cordis.eu

El objetivo general del Proyecto versa en la IA: Desarrollo, validación e implantación de tecnologías, herramientas y soluciones de IA seguras y resilientes en apoyo de la aplicación de la ley y la protección de los ciudadanos, las operaciones de ciberseguridad y la prevención y protección contra las acciones adversarias de inteligencia artificial.

Con el objetivo de comprobar la aplicabilidad de las soluciones basadas en IA que ofrece *STARLIGHT* los diferentes beneficiarios o usuarios finales, coordinados por EUROPOL, y con una metodología propia diseñada en el proyecto, trabajarán en la tarea de análisis y especificación de los siguientes casos de uso, realizando las correspondientes validaciones técnicas: contra-terrorismo, explotación sexual infantil, seguridad fronteriza y externa, ciberseguridad y cibercrimen, abordar la sobrecarga y tratamiento de información relacionada con la delincuencia organizada y la protección de espacios públicos.

El Proyecto H2020 *VICTORIA***,** que comenzó en el año 2017 y finalizó en el año 2020, y en el que el Ministerio del Interior participó a través de la Policía Nacional. Pretendía desarrollar una plataforma para alojar un sistema de análisis de video inteligente sobre delitos o atentados terroristas en los que se acumulan gran cantidad de horas de grabación. Se crea una plataforma que acelera la tarea de análisis de video mediante el uso de tecnologías Big Data, investigación semántica compleja, reconstrucciones 4D de escenas de delito e inteligencia artificial.

El proyecto *AIMARS* (*Intelligence System for Monitoring, Alert and Response for Security in events*), financiado con el *Programa CIEN* del CDTI (Centro de Desarrollo Tecnológico e Industrial, de 2018 a 2022, es un sistema de IA para la Vigilancia, Alerta y Respuesta para la Seguridad en eventos a nivel nacional. El *consorcio* español *AI MARS* está liderado por RETEVISIÓN (grupo CELLNEX), incluye otras cinco empresas (TELEVES, EMERGYA, SNGULAR, SHS y HERTA), y cuenta con el apoyo de cuatro organismos públicos de investigación (Universidad de Granada, Instituto Tecnológico de Castilla y León, Universidad Carlos III de Madrid y Universidad Politécnica de Madrid). El Ministerio del Interior, actúa como validador técnico desde el Consejo de asesoramiento, a través de la Jefatura de Información de la Guardia Civil.

El objetivo del proyecto AI MARS es investigar en diversas tecnologías, técnicas, herramientas y metodologías que ayuden a la vigilancia y prevención de atentados terroristas y cualquier otro tipo de incidencias que pueden afectar a la seguridad nacional como aglomeraciones o disturbios, grandes concentraciones de personas (aeropuertos, manifestaciones, eventos deportivos, centros comerciales..etc). Otros objetivos del proyecto, utilizando técnicas de Big Data, Machine Learning, son la inteligencia artificial y algoritmos inteligentes, la identificación de perfiles únicos de objetos o de personas con la información recibida de varias fuentes. Igualmente, de forma cooperativa se trabaja también, en el procesamiento de imagen en tiempo real, interfaces hombre-máquina y biometría (iris, facial, vascular).

5.- CONCLUSIONES

El esfuerzo que deben hacer todos los actores involucrados en el ámbito de la IA para la seguridad a nivel europeo y nacional es exigente. Lejos simplemente de eliminar tareas repetitivas, se debe ubicar a las personas como elemento central e insustituible de cualquier proceso. Sólo a través de la cooperación, la inversión de recursos financieros y humanos o la identificación de los retos que plantean las nuevas tecnologías ajustadas a los sistemas normativos, tanto nacionales como europeos, vaticinará una correcta gestión en un momento de cambio tan importante y tan rápido.

De hecho, el desarrollo de soluciones basadas en IA deben estar alineadas con las necesidades reales de la Guardia Civil y en general las FCS, para hacer inversiones eficientes por parte del Ministerio del Interior. Ello requiere desarrollar perfiles interdisciplinares de agentes con experiencia en seguridad, en investigación policial y unidades especializadas en I+D+i. Sin esos dos requisitos, necesarios, pero no suficientes, se corre el riesgo de producir aplicaciones sin utilidad real o sin sostenibilidad en el tiempo.

Por un lado, la IA se puede utilizar para mejorar la respuesta y la resiliencia, por ejemplo, para la detección temprana de amenazas y otras actividades maliciosas con el objetivo de identificar, prevenir y detener los ataques con mayor precisión. Por otro lado, los atacantes potencian cada vez más sus herramientas mediante el uso de IA o la manipulación de sistemas de IA.

Según se ha demostrado con el presente estudio, el Ministerio del Interior y las FCSE *podrían mejorar sus capacidades en la recolección y organización de la información* (ciencia de datos-calidad de los datos) apostando por la participación en

proyectos de innovación tecnológica de corte nacional y europeo, con el apoyo de unidades operativas. Con lo trabajado hasta el momento se puede concluir:

- La investigación básica y aplicada en IA para el sector de Seguridad necesita crear infraestructuras de investigación a nivel nacional y europeo que resuelvan la excesiva fragmentación.
- El uso de la Inteligencia Artificial se encuentra en una fase dónde es más importante invertir en soluciones muy costosas y escalables, que en mejorar los productos actuales de corte nacional. Se impulsa un modelo basado en las grandes empresas, con poca atención a las PYMES. El modelo nacional es un obstáculo para la competitividad europea frente a otros modelos en el ámbito de la investigación policial.
- La gestión y transferencia de conocimiento en materia de IA no se puede desligar de las políticas de gestión de talento ni de los programas de financiación europeos de I+D+i.

Personalmente se considera que la inversión actual en formación, recursos humanos, materiales y de concienciación, en materia IA, tanto del Ministerio del Interior como de la Guardia Civil, es insuficiente. Bien por desconocimiento de las nuevas oportunidades de mejora que brinda esta tecnología o bien por el desconocimiento del cambio del paradigma en el modelo de trabajo policial que conlleva la era Digital y que se está consolidando a nivel europeo.

Solo las grandes empresas tienen los recursos necesarios para cumplir con las obligaciones reglamentarias, propuestas por la normativa europea, al desarrollar, adaptar e implementar aplicaciones o modelos de IA supervisada a un ritmo acelerado. En la práctica, esto significa qué en las FCSE, se ralentizarán significativamente o incluso se verán obligados a dejar de desarrollar herramientas internas de IA dedicadas y tendrán que depender en gran medida de herramientas comerciales, utilizando los sistemas de IA como una caja negra.

6.- BIBLIOGRAFÍA

- BUILDING TRUST IN HUMAN CENTRIC ARTIFICIAL INTELLIGENCE. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Building Trust in Human Centric Artificial Intelligence (COM(2019)168) https://digitalstrategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence[Consultado el 11/02/2023].
- CDTI CEntro de Desarrollo Tecnológico e Industrial. Ministerio de Ciencia. https://www.cdti.es/ [Consultado el 16/01/2023].
- CETSE CEntro Tecnológico para la SEguridad Interior. https://cetse.ses.mir.es/publico/cetse [Consultado el 20/02/2023].
- COMISIÓN EUROPEA, INFORME, Objetivos de la Década Digital 2030 de la UE, 5/02/2023 https://ec.europa.eu/commission/presscorner/detail/es/ip_23_74 [Consultado el 17/01/2023].
- COMISIÓN EUROPEA, INFORME, mayo de 2019, orientaciones prácticas para las empresas sobre cómo procesar los conjuntos de datos. COM(2019) 250 https://ec.europa.eu/digitalsingle-market/en/news/practical-guidance-businesses-how-process-mixed-datasets [Consultado el 1/02/2023].

- COMISIÓN EUROPEA, INFORME DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO Y AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO. Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica. COMISIÓN EUROPEA Bruselas, 19.2.2020 COM (2020) 64 final https://revistas.uam.es/revistajuridica/article/view/16957 [Consultado el 20/10/2022].
- COMISIÓN EUROPEA, COMUNICACIÓN, Junio de 2021: "Hacia una estrategia para un espacio Schengen plenamente funcional y resiliente" COM (2021) 277 final de 2.6.2021 https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:277:FIN https://eur-lex.europa.eu/legal content/ES/TXT/PDF/?uri=CELEX:52021DC0277&from=ES [Consultado el 28/01/2023].
- COMISIÓN EUROPEA, COMUNICACIÓN, Bruselas, 29.5.2019 COM (2019) 250 final COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO: "Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea". https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52019DC0250&from=en [Consultado el 8/1/2023].
- COMISIÓN EUROPEA, COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES: sobre la Estrategia de la UE para una Unión de la Seguridad, COM/2020/605 final https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0605 [Consultado el 10/02/2023].
- COMISIÓN EUROPEA, COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES, Comisión Europea, "Una Estrategia Europea de Datos", Bruselas, 19.2.2020 COM (2020) 66 (final), https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066&from=ES [Consultado el 26/02/2023].
- COMISIÓN EUROPEA, Iniciativa sobre Responsabilidad Civil. Adaptación de las normas de responsabilidad a la Era digital y a la Inteligencia Artificial, 30 de junio de 2021. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Responsabilidad-civil-Adaptacion-de-las-normas-de-responsabilidad-a-la-era-digital-y-a-la-inteligencia-artificial_es. [Consultado el 15/01/2023].
- CONSEJO DE LA UNIÓN EUROPEA, CONCLUSIONES DEL CONSEJO (9 DE JUNIO DE 2020), La Configuración del futuro digital de Europa, Bruselas, 9 de junio de 2020 (OR. en) 8711/20. https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf [Consultado el 17/12/2022].
- DECISIÓN (UE) 2022/2349 DEL CONSEJO de 21 de noviembre de 2022. Comité de Inteligencia Artificial del Consejo de Europa. Por la que se autoriza la apertura de negociaciones en nombre de la Unión Europea con vistas a un Convenio del Consejo de Europa sobre inteligencia artificial, derechos humanos, democracia y Estado de Derecho.

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022D2349 [Consultado el 10/12/2022].
- EU SPACE. COPERNICUS. Programa de la Unión Europea. https://www.copernicus.eu/es [Consultado el 21/01/2023].
- EUROPEAN COMMISSION. WHITE PAPER.
- White Paper on Artificial Intelligence: an European approach to excellence and trust. Brussels, 19.2.2020 COM(2020) 65 final. https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf [Consultado el 7/10/2022].
- EUROPEAN COMMISSION. CORDIS EU Research Results. https://cordis.europa.eu/ [Consultado el 11/02/2023].
- EUROPEAN COMMISSION. Migration y Home affairs. https://home-affairs.ec.europa.eu/index_en [Consultado el 12/02/2023].
- EUROPEAN COMMISION. PARTICIPANT PORTAL. Funding and tenders opportunities. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home [Consultado el 30/01/2023].
- EUROPEAN COMMISSION. Report. Data governance and data policies at the European Commission, Secretariat-General July 2020. https://commission.europa.eu/system/files/2020-07/summary-data-governance-data-policies_en.pdf [Consultado el 22/02/2023].
- EU-LISA. PROGRAMMING DOCUMENT 2020-323 REV 2. SINGLE PROGRAMMING DOCUMENT. European union agency for the operational management of large scale it systems in the area of freedom, security and justice. https://www.eulisa.europa.eu/Publications/Corporate/SPD%202022-2024.pdf [Consultado el 18/12/2022].
- FONDOS DE SEGURIDAD INTERIOR. Internal Security Funds (ISF) y Border Management and Visa Instrument (BMVI). https://home-affairs.ec.europa.eu/funding/internal-security-funds/internal-security-fund-2021-2027_en https://fondoseuropeosparaseguridad.interior.gob.es/opencms/es/fondos/fondo-de-seguridad-interior/ [Consultado el 8/03/2023].
- FP7 FRAME PROGRAMME, Séptimo Programa Marco I+D+I de CE.
- Programa específico de COOPERACIÓN: Topic de Seguridad SEC-2012.3.4-6: Enhancing the workflow and functionalities of Automated Border Control (ABC) gates (Integration Project). https://cordis.europa.eu/project/id/312583 [Consultado el 7/02/2023].
- FRONTEX. Agencia Europea e la Guardia de Fronteras y Costas. https://frontex.europa.eu/es/ [Consultado el 29/01/2023].
- INTERNAL SECURITY FUNDS (ISF) and BORDER MANAGEMENT AND VISA INSTRUMENT (BMVI). https://home-affairs.ec.europa.eu/funding/internal-security-funds/internal-security-fund-2021-2027_en [Consultado el 18/01/2023].
- LÓPEZ DEL MORAL, M. QUESADA LÓPEZ, I. M. ANTÓN SANCHO, "Inteligencia artificial y responsabilidad civil: ¿es realmente necesario un cambio del Ordenamiento Jurídico?", Diario La Ley, núm. 47, 29 de enero de 202. https://diariolaley.laleynext.es/dll/2021/01/29/inteligencia-artificial-y-responsabilidad-civil-es-realmente-necesario-un-cambio-del-ordenamiento-juridico [Consultado el 27/01/2023].

- PÁGINA WEB Ministerio del Interior, Secretaría de Estado de Seguridad, Fondos de Seguridad Interior, FESI. https://fondoseuropeosparaseguridad.interior.gob.es/opencms/es/fondos/fondo-de-seguridad-interior/ [Consultado el 2/02/2023].
- Estadísticas actualizadas desde el año 2012 al año 2020. Portal Estadístico de Cibercriminalidad. Ministerio del Interior, Secretaría de Estado de Criminalidad. https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis
- Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO, Comisión Europea, Bruselas, 25.11.2020 COM (2020) 767 final 2020/0340 (COD). Ley de Gobernanza de Datos. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020PC0767&from=EN [Consultado el 20/02/2023].
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). DOUE Diario Oficial de la Unión Europea. https://www.boe.es/doue/2016/119/L00001-00088.pdf [Consultado el 21/02/2023].
- TABLADA, F., "Inteligencia artificial: Definición, tipos y aplicaciones", Grupo Atico34, Blog 18 de junio de 2020. https://protecciondatos-lopd.com/empresas/inteligenciaartificial/#Memoria_limitada. [Consultado el 20/09/2022].
- UNIÓN EUROPEA, Informe Consulta Pública, digital, 28 de Marzo 2019. https://wayback.archive-it.org/12090/*/https://ec.europa.eu/digital-single-market/en/news/* [Consultado el 5/11/2022].
- ZURITA MARTÍN, I., "Las propuestas de reforma legislativa del Libro Blanco europeo sobre inteligencia artificial en materia de seguridad y responsabilidad civil", Actualidad Jurídica Iberoamericana, núm. 14, 2021, p. 481. https://idibe.org/wp-content/uploads/2021/03/11._Isabel_Zurita_pp._438-487.pdf [Consultado el 28/12/2022]