Revista Científica
del Centro Universitario
de la Guardia Civil

Revista Lógos Guardia Civil

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

BACKGROUND TO THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN SECURITY ACROSS EUROPE: Technological innovation as a key factor for the Ministry of the Interior

BACKGROUND TO THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN SECURITY ACROSS EUROPE:
Technological innovation as a key factor for the Ministry of the Interior

Summary: 1.- INTRODUCTION. 2.- STATE OF THE ART AI AT THE EUROPEAN LEVEL. 3.- EUROPEAN ACTION PLAN FOR AI IN SECURITY. 3.1 Definition of AI. 3.2 European Strategic Axes (SA) of work on AI. 3.3 Funding mechanisms for AI in Europe. 4.- THE SPANISH MINISTRY OF THE INTERIOR'S INVOLVEMENT IN THE EUROPEAN PROJECTS FOR TECHNOLOGICAL INNOVATION IN THE FIELD OF AI. 5.- CONCLUSIONS, 6- BIBLIOGRAPHY.

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.

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.

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

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

ABBREVIATIONS (Glossary of Terms)

ABC Automated Border Control.
ABC4EU Automated Border Control for the European Union.
GSA General State Administration.
AI Artificial Intelligence.
AIaaS Artificial Intelligence as a Service.
AI-HLEG High Level Experts Group in Artificial Intelligence.
APTs Advanced Persistent Threats.
BI Business Intelligence.
BMVI Border Management and Visa Instrument.
OGCG Official Gazette of the Civil Guard.
CAHAI Ad Hoc Committee on Artificial Intelligence.
AACC Autonomous Communities.
NCC-CERT National Cryptologic Centre / Computer Security Incident Response Team.
CTID Centre for Technological and Industrial Development.
CEPOL European Union Agency for Police Training.
CETSE Security Technology Centre.
CISE Common European Information Sharing Environment.
CITCO Centre for Intelligence against Terrorism and Organised Crime
CLOUD Digital cloud.
NP National Police.
CAP Centre for Analysis and Planning.
NCCIP National Centre for Critical Infrastructure Protection.
DDoS Distributed Denial of Service attacks.
DEP Digital Europe Programme.
DESI Digital Economy and Society Index.
DL Deep Learning.
DG CONNECT Directorate-General for Communication Networks, Content and Technology.
DG HOME Directorate-General for Migration and Home Affairs.
DG REFORM Directorate-General for Support to Structural Reforms.
Digital-DEP Digital Europe Programme.
EES Entry Exit System.
AFSJ Area of Freedom, Security and Justice.
MS Member States.
EMPACT European Multidisciplinary Platform Against Criminal Threats.
NAIS National Artificial Intelligence Strategy.
ENISA European Union Agency for Cyber Security.
ENLETS European Network of Law Enforcement Technology Services.
ESA European Space Agency.
ESMIR Spanish Ministry of the Interior.
Eu-LISA European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice.
EUROJUST European Agency for Judicial Cooperation.
EUROPOL European Union Agency for Law Enforcement Cooperation.
EUROSUR European Border Surveillance System.
SLEA State Law Enforcement Agencies.
ERDF European Regional Development Funds.
FP7 7th Framework Programme

FRONTEX European Border and Coast Guard Agency.
ISF Internal Security Funds.
GC The Guardia Civil.
H2020 Horizon 2020 Programme (8th Framework Programme).
HE Horizon Europe Programme (9th Framework Programme).
HEUROPA Horizon Europe Programme.
RD+I Research, Development and Innovation.
AI Artificial Intelligence.
IoT Internet of Things.
LEA Law Enforcement Agency.
LEAR Legal Entity Appointed Representative.
OLODPGDR Organic Law on Data Protection and Guarantee of Digital Rights.
CEFM Connecting Europe Facility.
MFF Multiannual Financial Framework.
ML Machine Learning.
MSA Micro Services Architecture.
NCP National Contact Point.
NLP Natural Language Processing.
CCO Cyber Coordination Office
OECD Organisation for Economic Cooperation and Development.
SDGs Sustainable Development Goals.
EAFO European Anti-Fraud Office.
UN United Nations.
OSCE Organisation for Security and Co-operation in Europe
OSINT Open Source Intelligence.
NATO North Atlantic Treaty Organisation.
SMEs Small and medium-sized enterprises.
RBI Remote Biometric Identification.
GDPR General Data Protection Regulation.
SSDAI State Secretariat for Digitalisation and Artificial Intelligence
DDSICS Deputy Directorate-General for Security Information and Communications Systems.
ICTs Information and Communication Technologies.
EU European Union.
UNESCO United Nations Educational, Scientific and Cultural Organisation.
PUM Polytechnic University of Madrid.
WGAI Working Group Artificial Intelligence.
CSR Corporate Social Responsibility.

1.- INTRODUCTION

Technology, innovation and digitalisation are the bases of the new global order. There is no denying that technological change has reached all areas of society, the economy and politics, generating a new dimension in international relations and in the field of security.

Scientific knowledge, access to technology, its development and regulation have become essential elements for States and their societies. Power relations are no longer only based on technological excellence, defence and security, but also on the need to achieve hegemony in cyberspace or to build new data spaces.

The new technological revolutions linked to information and communication systems (ICTs) have generated new areas of collaboration and competition. Digitalisation and the creation of global networks for information exchange were initially led by the United States. The second phase, and the one we are currently in, based on 5G networks, the Internet of Things (IoT), quantum technology and Artificial Intelligence (AI), is taking place amidst fierce competition between China and the United States. But other middle powers in these fields, such as the European Union, including Spain, Japan, South Korea and other Asian countries, must be made visible.

Accessing the first generations of new technologies, integrating some of the traditional ones, or designing and maintaining new data network infrastructures, are critical aspects on which the national security of the new societies is based.

Big Data analysis and inference techniques through AI processes have opened the field for new services that are much more personalised and also much more useful in the field of Security. Important concerns are raised about the privacy of individuals and their individual autonomy. Many States are seeking a balance between security and freedom, due to the growing trend of criminal activities relating to cybercrime and identity theft.

The current situation is generating power asymmetries. The *information revolution* associated with new digital technologies has unearthed four fundamental values that are necessary to exert influence in this new environment: *networks, data, information and knowledge*. However, it is the large technology companies that own most of the data and networks and benefit the most from the current situation.

At the same time, societies are facing problems caused by new technologies in their daily use. The possibility of interacting with other people from all over the world and accessing all kinds of information does not only offer advantages for citizens. What is now known as "*Infodemia*", or the overabundance of information accessible from any platform or digital media, can have both positive and negative effects in the field of technological security. It is becoming increasingly difficult to find reliable sources of information, as it is becoming more and more common to find false propaganda for illicit or unreliable purposes (fake news).

The proper management of such potential, at a time when technology is advancing at a dizzying pace, requires an effort to foster the cooperation of all stakeholders involved in researching, developing and implementing AI-assisted solutions. Management that allows maximum performance to be obtained from the information systems, providing real added value to the State Law Enforcement Agencies (SLEA), in their mission to protect the free exercise of rights and freedoms, as well as to guarantee public safety.

Digitisation, availability and access to large volumes of data, as well as high-performance and high-capacity data processing infrastructures, are essential elements for developing AI. Beyond investment in creating new data sets and infrastructures, it is also necessary to ensure the efficient management of existing data and the appropriate use of data along the data value chain according to the principles of availability, integrity, reliability and quality.

The specific objectives, as defined in this study, focus on establishing guiding principles relating to AI for the purpose of security. The aim is to analyse how strategic lines of work in the field of AI have emerged for Spain, thanks to the emerging technologies validated in European projects and discussed in the different expert groups.

Some of the AI projects implemented in recent years will be presented, which will help Spanish agents ensuring the security of citizens (Law Enforcement Agencies, Border Guards, Customs Control and Protection Services, etc.) to benefit from new tools to use during their daily operational work.

On the other hand, and bearing in mind that Europe will continue to develop and improve the mechanisms to develop the ICT services it offers to its citizens, it is essential to place value on technology watch and competitive intelligence. The inclusion of new Artificial Intelligence processes in existing information systems, the design of new secure data spaces and their interoperability is a major challenge.

2.- STATE OF THE ART AI AT THE EUROPEAN LEVEL

Having shown in the introduction Europe's need to be a competitive player in the technology sector, the European Union (EU) is lagging behind in a number of areas. Indeed, the global digital economy is clearly developing around two powers: the United States and China.

To compete with these technological giants, the EU is investing heavily through European funding programmes. It is believed that more pan-European projects, pooling the resources of all Member States, will help to achieve sufficient savings to be more competitive in global markets.

AI is developing rapidly. In the short term, it will arguably change our lives by improving healthcare (e.g. by increasing diagnostic accuracy and enabling better disease prevention), increasing the efficiency of agriculture, contributing to climate change mitigation and adaptation, improving the efficiency of production systems through predictive maintenance, increasing the safety of Europeans, and bringing many other changes that we can only guess at today.

At the same time, AI carries a number of potential risks, such as opacity in decision-making, discrimination, intrusion into our private lives or use for criminal purposes, which need to be taken into account. Although Europe is still in a relatively consolidated position in relation to consumer applications and online platforms (which translates into a competitive disadvantage in terms of data access), important shifts in the value and re-use of data are taking place across different sectors.

In addition, Europe will seek to continue to lead progress in the algorithmic foundations of AI by building on its own scientific excellence. There is a need to build bridges between disciplines currently working independently, such as machine learning and deep learning (characterised by their limited interpretable nature and the need for large volumes of data to train models and learn through correlations) and symbolic approaches (where rules are created through human intervention).

Despite what appear to be multiple advantages, the adoption of AI in the field of security also entails challenges with respect to fundamental rights, so it is vital to find the right balance to harness the benefits of this technology without compromising privacy and the presumption of innocence.

In view of the above, in order to create an ecosystem of excellence that can support the sustainable development and uptake of AI across the economy and public administration of both the EU and its Member States (MS), actions need to be encouraged at several levels: (1) Collaboration between Member States. (2) Focusing the efforts of the research community. (3) AI skills development. (4) Support to SMEs and partnerships with the private sector.

In terms of practical applications, currently AI solutions mainly offer the possibility to automate processes. This applies, for example, to automatic image recognition in the medical field, security or industrial production. Previously a visual inspection of a product was necessary, whereas now sensors and algorithms can be used.

Also, taking an example from the field of automatic natural language processing, it is possible to automate communication with customers and users of a given service through chatbots. In the short term, these developments will reduce costs, optimise processes and help reduce waiting times. Moreover, smart assistants are already a part of everyday life in virtually every developed world.

Thus, on the one hand, we can speak of “Artificial Narrow Intelligence” (ANI), which refers to systems focused on solving specific application problems. Solving the problem is based on mathematical and computational methods, which are developed for specific requirements. Human beings provide the system with the necessary rules so that the algorithm can both train itself and provide results based on specific needs. The resulting system is able to optimise itself. ANI systems operate reactively at a superficial level of intelligence and do not achieve a deeper understanding of the problem solution. ANI focuses primarily on fulfilling clearly defined tasks and does not vary its approach to problems.

On the other hand, there is so-called “strong AI”, also called “superintelligence” or “artificial general intelligence” (AGI), which aims to reach or surpass the intellectual capabilities of humans. Strong AI is not just reactive, but also takes its own initiative, acting intelligently and flexibly. Today, it is very difficult to speak about a full development of strong AI, and there is still debate as to whether developing this type of intelligence is even possible. However, most researchers agree that this milestone will be reached, but there is no consensus on when it will happen.

In this context, we can talk about the following AI technologies applied in the field of security: natural language generation, speech recognition, virtual agents[1], Machine Learning (ML) platforms, AI optimised hardware, Deep Learning (DL) platforms, biometrics, robotic process automation, text analytics and NLP (Natural Language Processing[2]), digital twins/AI models[3], cyber defence, compliance, Peer-to-Peer networks[4], emotion recognition (anomalous behaviour) and image and video recognition.

AI can search for photos on social media platforms and compare them with a wide range of datasets to decide which are most relevant. Image recognition technology can also be used to detect number plates, analyse people and their opinions, and even verify people based on their faces.

With regard to future trends, AI as a Service (Artificial Intelligence as a Service, AIaaS[5]) should be highlighted. AI as a Service, i.e. SaaS-based development tools and resources[6], are increasingly in demand.

3.- EUROPEAN ACTION PLAN FOR AI IN SECURITY

If we just focus on the European Security domain, the key milestone lies in integrating new technologies with traditional systems and creating hybrid systems with improved capabilities, at an affordable cost.

AI can be a tool that manages threats but also augments them. Its use may be extended to accelerate the identification of and response to vulnerabilities and targeted attacks. The use of *the cloud and Big Data* pose new, associated challenges, as being able to access free data in cyberspace increases the possibility of its theft or misuse.

Europe is continuing to develop and improve mechanisms to protect the data and the related services it offers to its citizens. The safe and widespread use of data-driven products and services, the basis for training AI systems, means that establishing a legal framework that meets the interests of both citizens and security authorities must be a priority at the international level.

Another important part of security is protecting data when they are exchanged. Ensuring continuity of access controls across value chains and real-time data portability

[1] Computer agent or a program capable of interacting with humans. (Chatbots are a good example). Virtual agents are currently being used for customer service and support as well as smart home managers).

[2] Technology that uses text analysis to understand sentence structure, meaning and intent through statistical and ML methods. Text analytics and NLP are currently used in security systems, fraud detection or semantic analysis on social networks to identify radicalism. However, they are also used by a wide range of automated wizards and applications to extract unstructured data.

[3] Digital Twin is a software builder that bridges the gap between physical systems and the digital world. It is a virtual model of a physical object in real time.

[4] Two or more PCs connect and share resources without the need for data to pass through a centralised server.

[5] Artificial Intelligence as a Service AIaaS: New Business Model for AI as a Service. AI as a Service (AlaaS) helps organisations to incorporate AI functionality and processes without having technical knowledge or expertise within the organisation.

[6] Software as a Service (SaaS): a software distribution model where the software and the respective data it handles are hosted on a provider's servers, accessed via the Internet. The supplier not only provides the hardware, but also the corresponding software.

is a key requirement that is currently taken into account by European bodies in charge of regulating the use of AI in the security domain.

In 2018, the *European Strategy on AI* was published (European Commission, COM (2018) 237), which showed that AI was moving from being "*science fiction*" to becoming the basis for solving some of the main challenges of today's societies. In 2019, the European Commission's *High Level Expert Group on Artificial Intelligence AI HLEG*[7] published guidelines on trusted AI and an assessment checklist for 2020, based on the common values of all Member States (Area of Freedom, Security and Justice).

These guidelines were not intended to change existing legislation; they were non-binding recommendations, which, after consultation with the various cross-sector stakeholders, set out the key requirements for socially trustworthy AI in areas like security, personal data protection, privacy and environmental protection rules.

At the end of 2018, and revised in 2021, the first European *Coordinated Plan on AI* was published whereby Member States, plus Switzerland and Norway, made a joint commitment to foster the development and use of AI in Europe. This set out the policy changes and investments needed in Member States to strengthen Europe's leadership in AI. Four key areas were considered: increasing investment, making data more available (secure data spaces), fostering talent and ensuring trust.

In this regard, the Council of the European Union, in its 2019 conclusions on the *Coordinated Plan on AI,* stressed the importance of ensuring full respect for the rights of European citizens and called for a review of the relevant existing legislation with a view to ensuring that it is adapted to new opportunities and challenges.

In order to foster a framework of public trust in AI based on respect for the ethical, legal and moral principles of the European space, on 11 September 2019, the Committee of Ministers of the Council of Europe created *the Ad Hoc Committee on Artificial Intelligence (CAHAI).*

The *CAHAI* is unique in that it brings together Member States and observers, as well as members of civil society, academia and the private sector. It works closely with other international institutions, such as UNESCO, OECD and the European Union. The DDGSICS, representing the Spanish Ministry of the Interior, together with the Spanish Ministry of Justice and the Spanish Ministry of Foreign Affairs, are the Spanish members of this Committee.

April 2020 saw the publication of the *European Commission's White Paper* (A European approach to excellence and trust. European Commission Brussels, 19.2.2020 COM2020), preceding a public consultation with high international participation. The *White Paper* was accompanied by a "*Report on the security and liability implications of Artificial Intelligence, the Internet of Things and robotics*" (European Commission, 2020), whose conclusions launched a series of loopholes that the current legislation needed to address in terms of security.

[7] The Spanish NCP National Contact Point for this group is Dr Enrique Belda Esplugues, Deputy Director General for Security Information and Communications Systems (DDGSICS) at the State Secretariat for Security under the Ministry of the Interior.

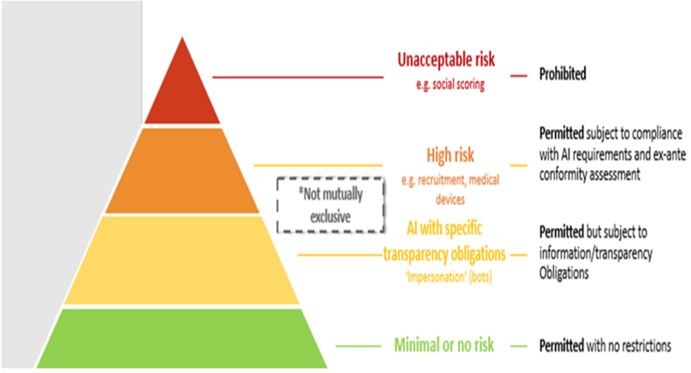
In October 2020, the European Council called for a clearer definition of what uses of AI should be considered high-risk, and urged fort certain issues, such as bias, opacity or a certain degree of unpredictability in partially autonomous behaviour, to be addressed in a way that ensures their compatibility with the application of existing legal rules, thereby safeguarding fundamental rights.

The European Commission, with its publication on 21 April 2021 of its *Proposal for a Regulation of the European Parliament and of the Council* laying down harmonised rules in the field of Artificial Intelligence and amending certain Union legislation, is currently proposing new rules and measures aimed at making Europe the global hub for Artificial Intelligence adapted to the Digital Age.

However, the proposal was very ambitious. The review of the text by the different Member States[8] has been costly. It can be seen in the review of the articles that, on occasions, it aims to develop an *Ad Hoc* data protection regulation for use cases of AI procedures, which, for example, in Spain, would already be covered by the recent General Data Protection Regulation GDPR (Regulation (EU) 2016/679), the national OLDPGDR (Organic Law on Data Protection and Guarantee of Digital Rights), and the national regulations transposing EU Directive 680/2016, giving rise to contradictions, or even potentially generating situations of legal uncertainty.

Among the general objectives of the Regulation, the possibility of responding to the needs imposed by the new technological landscape, in which AI-assisted security systems will have a huge impact in the field of sectors like Security, is codified. If properly designed and used, AI can become a strategic technology, enabling authorities to deal effectively with new challenges and types of crime.

The proposed Regulation takes into account that the way police work is understood will change, both in terms of the organisational effects on planning and resource allocation, as well as the introduction of a new paradigm of prevention and anticipation as opposed to a reactive approach.


Unacceptable risk
e.g. social scoring
Prohibited
High risk
e.g. recruitment, medical devices
Permitted subject to compliance with AI requirements and ex-ante conformity assessment
*Not mutually exclusive
AI with specific transparency obligations
'Impersonation' (bots)
Permitted but subject to information/transparency Obligations
Minimal or no risk
Permitted with no restrictions

Risks uses AI-Strategic Priorities 2019-2024.
Source: ec.europa.eu.

[8] The Spanish Ministry of the Interior is participating in the Review of the Draft of the European AI Regulation through the IXIM group of the European Council on police cooperation. The State Secretariat for Security – DDSICSS, the Directorate General International and European Relations (DGRIE), the Directorate General of the National Police (DGPN) and the Directorate General of the Guardia Civil for the Judicial Police (DGGC-UTPJ) are actively involved in this review.

It is worth noting that when, for example, the use of *RBI (Remote Biometric Identification)* systems by law enforcement authorities is regulated, risk and outcome are not differentiated. An erroneous result can lead to an undesirable physical outcome for citizens, but it is even more serious if the erroneous result violates fundamental rights, such as life or physical integrity, if the risk has not been taken into account by the Law Enforcement Agencies at the European level.

In fact, the live use of RBI systems in publicly accessible spaces for law enforcement purposes is, in principle, prohibited. Strict exceptions are defined and regulated, for example, when their application is necessary to search for a missing child, to prevent a specific and imminent terrorist threat, or to detect, locate, identify or prosecute a perpetrator or suspect of a serious crime. Their use shall be subject to authorisation by a judicial or other independent body and to appropriate limits in terms of duration, geographical scope and databases explored.

Police forces are currently using applications in different fields and specialisations, such as investigation and intelligence gathering, criminalistics, including research gathering, or forecasting. These applications will have an enormous impact on the way police work is understood, both in terms of organisational effects on planning and resource allocation (greater efficiency and improvements in police intelligence) and the introduction of a new paradigm (that of prevention and anticipation) as opposed to the reactive approach of law enforcement.

Some experts believe that policing will be more about predicting and identifying criminal patterns or managing risks arising from criminal acts being committed. In this sense, in the future, the Spanish police will have to take into account some of the challenges of integrating Artificial Intelligence in police work in Spain.

3.1.- Definition of AI

The term “algorithm” is widely used in the context of Big Data, machine learning and AI. In computing, an algorithm is a sequence of commands for a computer to transform an input into an output. A simple example of an algorithm would be a script to sort a random list of people by age. In this example, a computer is provided with a random list (input), a previously designed algorithm is executed (commands) and an age-ordered list is obtained (output).

Algorithms are often used to make predictions, e.g. predictions about the profile of people likely to buy a certain product, weather forecasting, spam detection or the nationalities of the most frequent border crossers. For a specific task, an algorithm is fed with data creating a model that is used in practice for a real-world task. The term machine learning, which has already been referred to, involves having an algorithm in the “raw” (already designed) state and training it successively by feeding it data to finally obtain a model.

The term “Artificial Intelligence” is more difficult to define. It does not refer to something tangible, but to current technological developments and processes in general. Most of what is discussed “under the AI umbrella” refers to increasing automation of tasks through the use of machine learning (supervised AI) and even achieving autonomous decision-making through learning that is not directed by a human (unsupervised AI).

The fact that machines and information and communications systems are capable of self-management, estimating patterns or even taking control of events or occurrences in which they take action, far exceeds human capacity. Ultimately, the capacity for human governance of such “intelligent” systems may be compromised. It is therefore a major challenge not only to interpret them properly, but also how these processes will be implemented in practice.

The Organisation for Economic Cooperation and Development (OECD) defines AI as: “*a system that can make predictions, recommendations or decisions that influence real or virtual environments for a specific set of objectives*”.

On Friday 9 March 2023, representatives of the European Parliament's political groups working on the AI Law (Consolidation of the AI Harmonisation Regulation 2021), reached a political agreement on one of the most sensitive parts of the legal text, the definition of AI: “*A machine-based system that is designed to operate with different levels of autonomy and that can generate results, such as predictions, recommendations or decisions that influence physical health or virtual environments, for explicit or implicit goals*”.

The definition largely overlaps with that of the OECD and is closely aligned with the work of international organisations working on Artificial Intelligence, to ensure legal certainty, harmonisation and broad acceptance, such as the Council of Europe.

A distinction between AI applied to simpler software systems (programming approaches) versus AI systems seeking predictive autonomy applied to specific contexts is broken down from the accompanying text accompanying the EU's updated definition of AI. What has been studied in science for years as the difference between “weak Artificial Intelligence” and “strong Artificial Intelligence” is being regulated.

AI enables the increasingly complex development of *algorithms* and instruction sets to solve a problem. Algorithms have moved from being static (when programmers design the decision-making criteria) to dynamic.

Machine learning algorithms have the ability to learn from data and experiences to make decisions, generating their own instructions, which are no longer the original ones defined by the programmer. Deep learning already emulates complex neural networks (Deep Learning).

Through aggregating and processing large amounts of data generated daily into useful information for Member States’ law enforcement, AI can help prevent crime by recognising patterns, finding anomalies and using predictive analytics to anticipate the future movements of terrorists and criminals, both in the physical and digital realm. It can also be very useful for investigating crimes that have already taken place. Generally, these types of tools are based on historical data, mostly from official sources (time, place and type of crimes committed). They can be complemented by environmental variables (population density).

In this way, researchers use each digital data source to its fullest potential, saving time in reviewing evidence. With Big Data and increasingly sophisticated algorithms, it is possible to make increasingly accurate analyses and predictions in real time. One advantage of algorithms is that, unlike people, algorithms make consistent decisions when faced with the same scenarios (they do not have changes in judgement or mood).

3.2.- European Strategic Axes (SA) of work on AI.

The overall work of the European Commission's Human Leading Expert Group on Artificial Intelligence (HLEG) has been central to developing the Commission's approach to AI. The group's recommendations have served as a basis for policy initiatives taken by the Commission and its MS. The initiatives that have emerged include the following: Communication on building trust in human-centred AI. Contributions to the White Paper on AI: a European approach to excellence and trust and contributions to the updated EC Co-ordinated Plan on AI.

The Strategic Axes (SA) on AI that are being studied as part of this work are:

SA1.- Position the end-user as a key element in developing AI, using European technological potential as a catalyst. AI has the potential to transform the world for the better. Its capabilities could improve healthcare, reduce energy consumption, make cars safer and enable farmers to use water and natural resources more efficiently. AI can be used to predict climate change, improve financial risk management and provide the tools to make products tailored to our needs with less waste. AI could also help detect fraud and cybersecurity threats, and enable law enforcement agencies to fight crime more efficiently.

However, this technological potential also brings with it new challenges for the future of work and raises particularly important ethical and legal questions.

To address these issues, the EC, through its Communication "*Building Trust in Human-Centric Artificial Intelligence"* (European Commission, 2019, COM(168))*,* has highlighted that trust is a prerequisite to ensure a human-centric approach to AI: AI is not an end in itself, but a *tool that has to serve people with the ultimate goal of increasing human well-being.* To achieve this, the reliability of AI must be ensured by integrating the values on which our societies are based into the development of technology.

SA2.- Evaluation of the technological adaptation to the new system of functional and operational needs of the Law Enforcement Agencies in real terms of use (eu-Lisa and EUROPOL).

Due to the relevant role of both eu-LISA, in its mission to provide technological support to Member States for a safer Europe, and EUROPOL, as what could be described as supra-user in technological and operational terms, they are of vital importance in identifying and channelling developments in AI technology that are truly effective for *Law Enforcement Agencies (LEAs*).

It seems advisable, therefore, to have this type of agent to promote the implementation and standardisation of protocols for the acceptance testing of AI-assisted technological solutions, identifying, coordinating and helping to establish the key elements for measuring the performance and suitability of the system to be developed.

SA3.- Fostering a framework of public confidence in AI based on respect for the ethical, legal and moral principles of the European area. To this end, on 11 September 2019, the Committee of Ministers of the Council of Europe established the Ad Hoc Committee on Artificial Intelligence (CAHAI). Established for a period of 2 years, it met for the first time from 18 to 20 November 2019 in Strasbourg.

The CAI (a later incarnation of the CAHAI), is the Council of Europe's Committee on AI for the period 2022-2024, tasked with establishing an international negotiation process to develop a legal framework for developing, designing and implementing AI at the international level.

It is based on Council of Europe standards on human rights, democracy and the Rule of Law. The CAI brings together MS and observers, as well as members of civil society, academia and the private sector. Convinced of the importance of global reflection and joint efforts in this field, the Committee on AI works closely with other international institutions, such as UNESCO (the United Nations Educational, Scientific and Cultural Organisation), the OECD (Organisation for Economic Co-operation and Development) and the EU (European Union).

SA4.- Common Data Strategy – Secure data architectures and spaces for AI (eu-Lisa and Europol). In February 2021, the European Commission published the document "The European Data Strategy" (European Commission, 2020), which consolidated the intention to create a Single Data Market, so that public and private sector stakeholders would have easy access to quality industrial and public data, with the aim of boosting the training of the algorithms underlying certain technologies, among other things.

This is why secure data spaces will be of particular importance in the period from 2021 to 2027, and both their technological infrastructure and governance will need to be addressed.

Several legislative and financial measures have been proposed since the beginning of 2021 to implement these spaces. These include the**Data Governance Act** (European Commission, 2020, 767 final), which was adopted on 25 November 2020 and could be complemented by sectoral legislation for access and use, as well as the necessary mechanisms to implement interoperability of systems.

For reasons of national security and public safety, the Data Governance Act did not regulate accessibility. That is why, in 2021, the European Council declared the need to accelerate the creation of common data spaces, and requested the European Commission to take the remaining measures necessary to implement these.

The problems that the European Union has encountered in tackling this task include, firstly, the fragmentation of the MS. Several had started to develop their own legal framework relating to the processing of data for research purposes, or even the use of privately held data by governmental authorities in accordance with their competence. Other States had not yet started, leading to differences in the internal data market.

Secondly, the availability of data: The value of data lies in its use and re-use. At present, there is not enough data available to be reused and, for example, to train the algorithms underlying AI processes. The issues start with the ownership of the data, continue with identifying the data users, and can go as far as the nature of the data (whether this is personal, non-personal, or a combination of both categories).

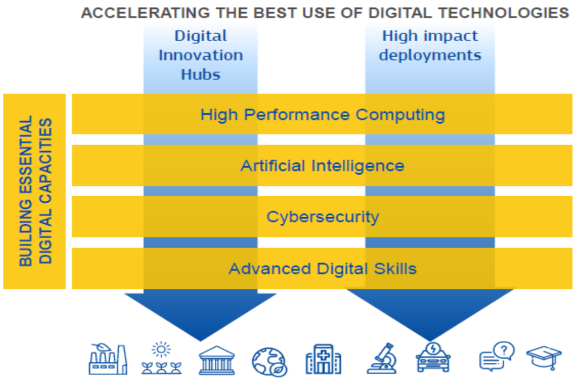
Thirdly, the overall benefit to citizens. Data, which is considered to be public assets, are created in societies by their citizens, and can often be harnessed to address emergency situations and to improve public services. Indeed, if put to good use, they can even ensure a more effective fight against organised crime, terrorism and the protection of external borders.

3.3.- European funding mechanisms for AI.

Countering the power of large technology companies requires reforming markets for goods and services, removing barriers to entry and exit for products and knowledge, and strengthening and modifying defence and security investment policies. The EU's long-term budget, also known as the Multiannual Financial Framework (MFF), drives the development of digital technologies through the different Framework Programmes. Instruments like the Digital Europe Programme (DEP) dovetail with the Internal Security Programmes (ISF and BMVI) and the Horizon Europe and Horizon 2020 Programmes (RD&I). In addition, the European Commission has proposed a new recovery instrument in the wake of the COVID-19 crisis called NextGenerationEU. The main active EU funding programmes in the field of AI, from which law enforcement agencies benefit, are:

a) DIGITAL EUROPE Programme 2021-2027

The Digital Europe Programme *(DEP)* aims to accelerate economic recovery and drive digital transformation across Europe. It will seek to strengthen the Union's Member States with investments in five areas of work, namely: (1) Supercomputing and data processing capabilities. (2) Core Artificial Intelligence (AI) capabilities, such as secure data spaces and AI algorithm libraries**.** (3) Cybersecurity. (4) Improving the use of digital skills in EU society and economy. (5) Support for digitising businesses and public administrations.


ACCELERATING THE BEST USE OF DIGITAL TECHNOLOGIES
Digital Innovation Hubs
High impact deployments
BUILDING ESSENTIAL DIGITAL CAPACITIES
High Performance Computing
Artificial Intelligence
Cybersecurity
Advanced Digital Skills

Structure of the DIGITAL EUROPE Programme. Source: EuropeanCommission.eu.

The DEP Work Programme is designed by DG-CONNECT (the European Commission's Directorate-General for Communication Networks, Content and Technology) to bridge the gap between research and deployment of digital technologies. It will bring research results to the marketplace for the benefit of Europe's citizens and businesses, in particular small and medium-sized enterprises (SMEs). There is a planned investment of 7.6 billion euros.

In Spain, the national authority is the Ministry of Economic Affairs and Digital Transformation, represented through the SSDAI (Secretary of State for Digitalisation and Artificial Intelligence). Work is carried out at inter-ministerial level. The two main lines on the deployment of technologies applied to the field of Security and the LEAs are: (1) Implementing a common European Secure Data Space for testing, training and validation of AI algorithms and developing a reference architecture to collect data that is interoperable. (2) Increasing the technological means and capabilities of European Law Enforcement Agencies in the use of AI and Cybersecurity to manage large amounts of data.

b) HORIZON2020 Programme 2014-2020 (Horizon2020).

Horizon 2020 (H2020) is the European Union's Framework Programme (FP) for Research and Innovation, which was active during the period 2014-2020. It had a total budget of 77.028 billion euros to finance research, technological development, demonstration and innovation initiatives and projects. Horizon 2020 brought together and reinforced the activities that were funded by the 7th Research and Development FP (FP7) during the period 2007-2013, the innovation actions of the Competitiveness and Innovation FP (CIP) and the actions of the European Institute of Innovation and Technology (EIT). It included AI-specific topics and calls.

c) HORIZON EUROPE 2021-2027 Programme (Horizon Europe).

Horizon Europe (the 9th EC Framework Programme) is a seven-year European funding programme (2021-2027) for Research, Development and Innovation (RD&I), which continues the work of the European Horizon 2020 Programme (FP8). Within the European Commission, the 9th Work Programme is designed, coordinated and funded by DG-HOME, in collaboration with other Directorates-General, such as DG-SANTE (European Commission's Directorate-General for Health and Food Safety), DG-REFORM (European Commission's Directorate-General for Support to Structural Reforms) and DG-CONNECT.

Horizon Europe includes a specific budget for "*Digital, Industry and Space*". This budget will develop high-level research and innovation in enabling technologies, such as Artificial Intelligence. The national authority in Spain for the Horizon Europe Programme is the Ministry of Science and Innovation, represented by the Centre for Technological and Industrial Development (CDTI), a body attached to the Ministry of Science and Innovation. It collaborates with the Spanish Ministry of the Interior and its dependent bodies to prepare and develop proposals and projects, supported by the II Pillar, Global Changes and Industrial Competitiveness, Cluster III, "Civil Security for Society", which also includes specific calls for Artificial Intelligence.

d) INTERNAL SECURITY FUNDS. ISF and BMVI financial framework 2021-2027.

The Internal Security Funds ISF (fund for police cooperation, fight against organised crime and terrorism) and BMVI (fund for integrated border and visa management), make up the Multiannual Financial Framework 2021-2027. The ISF-BMVI is jointly managed by the European Commission and the Member States through the approval of Programmes. For the 2021-2027 framework, there is a total budget of 1.931 billion euros and Spain has an initial allocation of 79.5 million euros for the ISF and around 300 million euros for the BMVI. Spain will be able to respond to the European Commission on the economic needs of *technological and security projects*, both in the border area and in the areas of counter-terrorism, radicalism and organised crime.

This fund makes it possible to improve and facilitate the exchange of information between the competent authorities and Union bodies and agencies and, where appropriate, with third countries and international organisations. This is why investments through AI co-financing are evident in numerous large-scale projects currently being worked on by the Spanish Ministry of the Interior, with one of the main beneficiaries being the Guardia Civil.

Some of the objectives that closely touch upon implementing AI processes in the field of security are: the *procurement and acquisition* of Information and Communications Technology (ICT) systems, the associated testing, and the improvement of system interoperability and data quality (e.g. automated processing of biometric and identification data). This also includes support to thematic or cross-cutting networks of specialised national units to improve mutual trust, exchange and dissemination of knowledge, information, experience and best practices, pooling of resources and expertise in joint centres of excellence.

4.- THE SPANISH MINISTRY OF THE INTERIOR'S INVOLVEMENT IN THE EUROPEAN PROJECTS FOR TECHNOLOGICAL INNOVATION IN THE FIELD OF AI

Following the global pandemic of COVID-19, there has been an increase in online crime in recent years[9]. More counterfeits are being created and the goods distributed are generally of inferior quality. New methods of financing organised crime and different types of fraud are being investigated, including cases relating to the field of medicines (medical devices and vaccines).

The *Schengen Strategy* (European Commission, COM (2021) 277 final), emphasises the important role of using technologies for internal and external border control as an alternative to temporary physical border controls in the face of the crises experienced in recent years. Technologies like AI, applied to advanced facial recognition, make it possible to check passengers in vehicles crossing a land (physical border) or maritime (e.g. ferry) border control.

The Entry-Exit System *(EES[10]),* currently funded by the European Commission's Internal Security Funds, Border Protection and Visa Instrument, is expected to be

[9] The Crime Statistics Portal belonging to the Ministry of the Interior for the Government of Spain.

[10] The Entry Exit System EES, an automated computerised system for registering non-Schengen travellers, both short-stay visa holders and visa-exempt travellers, each time they cross an external EU border.

operational by the end of 2023, although the European Commission and its Member States are finding it difficult to strike a balance between a seamless border crossing for travellers while at the same time ensuring the security of traveller information.

Several H2020 research projects have successfully developed solutions for the controlled and secure passage of travellers at external borders, also addressing the challenges that arose at the France-United Kingdom border after the UK's departure from the EU. Authorities in the French region of *Hauts-de-France* used the results of a security research project, called *FastPass15, FP7*, which ended in 2017, to facilitate travel at the France-United Kingdom border.

Reference should be made here to the EU research project *ABC4EU* (FP7-SEC-2012.3.4-6**:** Enhancing the workflow and functionalities of Automated Border Control ABC gates, in which the Spanish Ministry of the Interior participated, DDSICS, 2014 to 2018). This project prepared the capabilities for the forthcoming Passenger Entry-Exit System (EES). There was a pressing need at the time to unify and harmonise technology for external border control in relation to e-passport management, biometrics, gate design, human interface, processes, *PKD* (Public Key Directory) certificate exchange, signalling and interoperability.

On the other hand, the EU's Smart Border Initiative adds a new approach to be taken into account in developing ABC: the inclusion of a Real Time Transport Protocol (RTP) system for the control of third country nationals and a Schengen Entry and Exit System (EES).

ABC4EU identified the requirements for an integrated, interoperable and citizens' rights compliant ABC system, taking into account the experience gained from previous pilots and projects and the future needs arising from the Smart Border initiative[11] and other EU and national initiatives. The project focused on harmonising the design and operational features of ABC Gates, using the EU's second generation passports and other accepted travel documents. In addition, RTP and EES were specifically tested in the project to assess their feasibility and to develop a new *C4I-Computing for Intelligence* concept for border management.

The *CLOSEYE* project is particularly relevant, because it was the first project coordinated by an LEA (Law Enforcement Agency), namely the Spanish Ministry of the Interior, represented by the Guardia Civil (Prosecutor's Office and Border Control). A collaborative assessment of border surveillance technologies in maritime environments was conducted through pre-operational validation of new technological solutions. Innovative solutions worked on as part of the project included platforms, sensors and Information and Communications Technologies (ICT), which promoted more cost-effective surveillance, improved vessel traffic discrimination and supported the decision-making process. They also contributed to improving situational awareness in coordination centres, real-time information exchange between different agencies and reaction times.

The *ANDROMEDA* project, H2020, aimed to extend the scope of the Common European Information Sharing Environment (CISE) also applied between police forces

[11] EU Smart Borders Initiative: easier access and better security in the Schengen area since 2011. Combines EES with PNR (Passenger Name Record). Both projects developed, managed, implemented and maintained at the national level by DDSICS – Ministry of the Interior.

and armed forces and to land borders. It built on the network created by the National Contact Centres, Frontex and EMSA through enhanced capabilities, including transnational exchange of useful and available information and associated procedures and mechanisms, thus supporting the creation of a common information-sharing environment.

The H2020 *COMPASS2020* demonstrator project, coordinated by Portugal, validated underwater drones to prevent cross-border crime through maritime surveillance and the H2020 *FOLDOUT* project (2018-2022) aims to improve the detection of migrant smuggling in densely forested areas. It combines various sensors and technologies and fuses them using *machine learning* into an intelligent sensing platform. Although the Spanish Ministry of the Interior did not participate, Spain was represented in the consortium by *Eticas Research and Consulting S.L.*, an Industrial Partner, whose participation translates into *identifying black box algorithmic vulnerabilities and retraining AI-driven technology with better data and source content.*

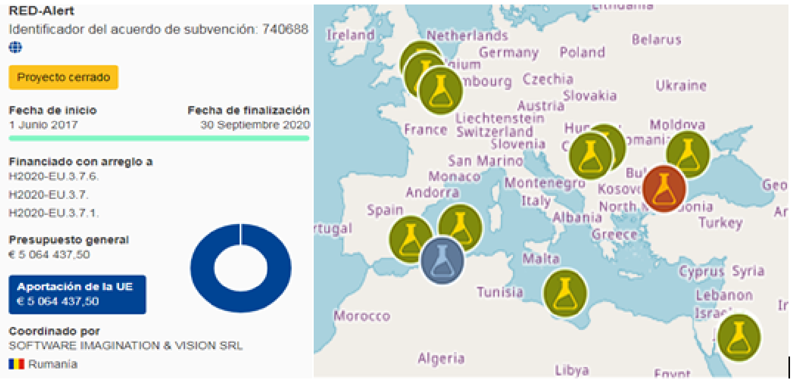
The EU's counter-terrorism agenda, mentioned above, highlights the importance of applied security research for areas like data processing and detecting and analysing terrorist content and violent radicalism online by European Law Enforcement Agencies.

The *RED ALERT* project [12] *H2020-AI* has developed technologies to rapidly detect online radicalisation, supporting global counter-terrorism efforts**.** For extremist or terrorist organisations, the Internet is a means of psychological combat, dissemination of disinformation, malicious propaganda, and recruitment of new members. Social media has become one of the preferred methods of targeting vulnerable individuals.

Without adequate tools to effectively identify terrorist content on the Internet, Law Enforcement Agencies are forced to rely on private *anti-spam* solutions, user reports and human analysis. This can mean that some terrorist activity goes undetected, which, in some cases, can have negative consequences for the full deployment of policing.

It aims to develop tools for semantic, photographic and video analysis of social networks and open sources to detect radicalism by processing large amounts of unstructured data. (Ministry of the Interior-Guardia Civil-Information Service) 2017-2020. The Coordinator is SIVECO, a Romanian IT company.

[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.



RED-Alert

Identificador del acuerdo de subvención: 740688

Proyecto cerrado

Fecha de inicio	Fecha de finalización
1 Junio 2017	30 Septiembre 2020

Financiado con arreglo a
H2020-EU.3.7.6.
H2020-EU.3.7.
H2020-EU.3.7.1.

Presupuesto general
€ 5 064 437,50

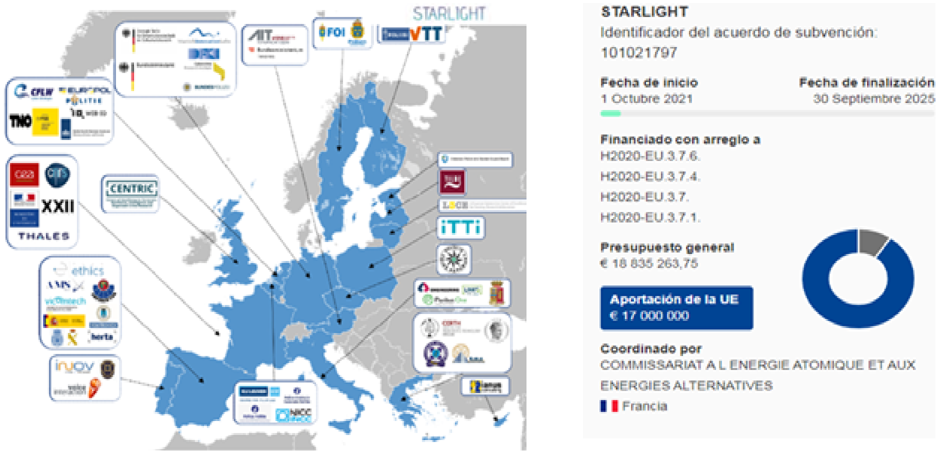
Aportación de la UE
€ 5 064 437,50

Coordinado por
SOFTWARE IMAGINATION & VISION SRL
Rumania

Figure 3-6 H2020 RED ALERT Project Consortium. Source: Cordis.eu

The European project *STARLIGHT*[13] *H2020-AI,* which began on 1 October 2021 for 48 months, *will validate Artificial Intelligence processes* used by European Law Enforcement Agencies. The Spanish Ministry of the Interior will play a relevant role, leading tasks for analysis and specification of operational requirements, use cases and proposed pilots.

Coordinated by the French Ministry of the Interior (Commissariat à l'énergie atomique et aux energies alternatives CEA). In total, 53 partners from 18 countries, 17 European Law Enforcement Agencies and 7 Spanish partners: the Spanish Ministry of the Interior (DDSICS, NP-Special Systems and GC-Operational Support Group), Polytechnic University of Madrid (PUM), Vicomtech, Herta Seguridad SL, Plus Ethics, Ertzaintza and Advanced Model Solutions SL.



STARLIGHT

Identificador del acuerdo de subvención: 101021797

Fecha de inicio	Fecha de finalización
1 Octubre 2021	30 Septiembre 2025

Financiado con arreglo a
H2020-EU.3.7.6.
H2020-EU.3.7.4.
H2020-EU.3.7.
H2020-EU.3.7.1.

Presupuesto general
€ 18 835 263,75

Aportación de la UE
€ 17 000 000

Coordinado por
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES
Francia

STARLIGHT H2020AI Project Consortium Source: Cordis.eu

The overall objective of the project focuses on AI: Development, validation and deployment of secure and resilient AI technologies, tools and solutions in support of law enforcement and citizen protection, cybersecurity operations and the prevention of and protection against adversarial AI actions.

[13] H202 STARLIGHT project: Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats. It will run for 48 months, with a return to Spain of €1,987,073, of which €293,750 corresponds to the Spanish Ministry of the Interior. Total EC-DGHOME funding for the Project: 18M euros

In order to test the applicability of the AI-based solutions offered by *STARLIGHT,* the different beneficiaries or end users, coordinated by EUROPOL, and with their own methodology designed as part of the project, will work on the task of analysing and specifying the following use cases, carrying out the corresponding technical validations: counter-terrorism, child sexual exploitation, border and external security, cybersecurity and cybercrime, addressing the overload and processing of information relating to organised crime and protecting public spaces.

The H2020 *VICTORIA* Project**,** which began in 2017 and ended in 2020, and in which the Spanish Ministry of the Interior participated through the National Police. It aimed to develop a platform for hosting an intelligent video analysis system for crimes or terrorist attacks where large amounts of footage was accumulated. A platform is created that accelerates the task of video analysis through the use of Big Data technologies, complex semantic research, 4D crime scene reconstructions and Artificial Intelligence.

The *AIMARS* project *(Intelligence System for Monitoring, Alert and Response for Security in events*), funded by the *CIEN Programme* under the CDTI (Centre for Technological and Industrial Development, from 2018 to 2022), is an AI system for Monitoring, Alert and Response for Event Security at the national level. The Spanish *AI MARS consortium* is led by RETEVISIÓN (CELLNEX group), includes five other companies (TELEVES, EMERGYA, SNGULAR, SHS and HERTA), and is supported by four public research organisations (University of Granada, Technological Institute of Castile and León, University Carlos III of Madrid and the Polytechnic University of Madrid). The Spanish Ministry of the Interior acts as the technical validator through the Advisory Council, via the Guardia Civil's Information Headquarters.

The objective of the AI MARS project is to research different technologies, techniques, tools and methodologies that help with the surveillance and prevention of terrorist attacks and any other type of incidents that may affect national security, such as crowds or disturbances, large concentrations of people (airports, demonstrations, sporting events, shopping centres, etc.). Other objectives of the project, using Big Data techniques, Machine Learning, Artificial Intelligence and intelligent algorithms, are being able to identify unique profiles of objects or people with information received from various sources. Work on real-time image processing, human-machine interfaces and biometrics (iris, facial, vascular) is also being carried out cooperatively.

5.- CONCLUSIONS

The effort to be made by all stakeholders involved in the field of AI for security at the European and national level is demanding. Far from simply eliminating repetitive tasks, people must be placed at the centre and considered to be an irreplaceable element of any process. Only through cooperation, investment of financial and human resources or identifying the challenges posed by new technologies adjusted to the regulatory systems, both national and European, will it be possible to manage AI correctly at a time of such important and rapid change.

In fact, the development of AI-based solutions must be aligned with the real needs of the Guardia Civil and the LEAs in general, in order for the Spanish Ministry of the Interior to make efficient investments. This requires the development of interdisciplinary officer profiles with experience in security, police investigation and specialised RD&I

units. Without these two requirements, which are necessary but not sufficient, there is a risk of producing applications with no real utility or sustainability over time.

On the one hand, AI can be used to improve response and resilience, e.g. for early detection of threats and other malicious activities in order to identify, prevent and stop attacks more accurately. On the other hand, attackers are increasingly leveraging their tools through the use of AI or manipulation of AI systems.

As this study has shown, the Spanish Ministry of the Interior and the ***SLEA could improve their capabilities for gathering and organising information*** (data science-data quality) by participating in national and European technological innovation projects, with the support of operational units. From what has been worked on so far, it can be concluded that:

- Basic and applied AI research for the security sector needs to create research infrastructures at the national and European level to address the *excessive fragmentation.*
- The use of Artificial Intelligence is at a stage where *it is more important to invest in very expensive and scalable solutions than in improving existing national products.* A model based on large companies is being promoted, with little attention being paid to SMEs. The national model is an obstacle to European competitiveness vis-à-vis other models in the field of police investigation.
- AI knowledge management and transfer cannot be separated from talent management policies and European RD&I funding programmes.

I personally consider that the current investment in training, human resources, equipment and awareness-raising in AI matters, both by the Spanish Ministry of the Interior and the Guardia Civil, is insufficient. This is either due to a lack of awareness of the new opportunities for improvement that this technology offers or of the paradigm shift in the model of police work brought about by the digital era, which is being consolidated at the European level.

Only large companies have the resources to meet the regulatory obligations proposed by European regulations by developing, adapting and deploying supervised AI applications or models at an accelerated pace. In practice, this means that the SLEAs will be forced to significantly slow down or even stop developing dedicated in-house AI tools and will have to rely heavily on commercial tools, using AI systems as a black box.

6.- BIBLIOGRAPHY

- 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 [Accessed on 11 February 2023].
- CDTI Centre for Technological and Industrial Development. Ministry of Science. https://www.cdti.es/ [Accessed on 16 January 2023].
- CETSE Technology Centre for Homeland Security. https://cetse.ses.mir.es/publico/cetse [Accessed on 20 February 2023].

- EUROPEAN COMMISSION, REPORT, EU Digital Decade 2030 Targets, 5/02/2023 https://ec.europa.eu/commission/presscorner/detail/es/ip_23_74 [Accessed on 17 January 2023].
- EUROPEAN COMMISSION, REPORT, May 2019, practical guidance for businesses on how to process datasets. COM(2019) 250 https://ec.europa.eu/digitalsingle-market/en/news/practical-guidance-businesses-how-process-mixed-datasets [Accessed on 01 February 2023].
- EUROPEAN COMMISSION, REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE. Report on the security and liability implications of Artificial Intelligence, the Internet of Things and robotics. EUROPEAN COMMISSION Brussels, 19.2.2020 COM (2020) 64 final https://revistas.uam.es/revistajuridica/article/view/16957 [Accessed on 20 October 2022].
- EUROPEAN COMMISSION, COMMUNICATION, June 2021: "Towards a strategy for a fully functional and resilient Schengen area" COM (2021) 277 final of 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 [Accessed on 28 January 2023].
- EUROPEAN COMMISSION, COMMUNICATION, Brussels, 29.5.2019 COM (2019) 250 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: "Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union". https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52019DC0250&from=en [Accessed on 08 January 2023].
- EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: on the EU Strategy for a Security Union, COM/2020/605 final https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0605 [Accessed on 10 February 2023].
- EUROPEAN COMMISSION, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, European Commission, "A European Data Strategy", Brussels, 19.2.2020 COM (2020) 66 (final), https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066&from=ES [Accessed on 26 February 2023].
- EUROPEAN COMMISSION, Civil Liability Initiative. Adapting liability rules to the Digital Age and Artificial Intelligence, 30 June 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. [Accessed on 15 January 2023].
- COUNCIL OF THE EUROPEAN UNION, COUNCIL CONCLUSIONS (9 JUNE 2020), Shaping Europe's Digital Future, Brussels, 9 June 2020 (OR. en) 8711/20.

https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf [Accessed on 17 December 2022].

- COUNCIL DECISION (EU) 2022/2349 of 21 November 2022. Artificial Intelligence Committee of the Council of Europe. Authorising the opening of negotiations on behalf of the European Union for a Council of Europe Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32022D2349 [Accessed on 10 December 2022].
- EU SPACE. COPERNICUS. European Union Programme. https://www.copernicus.eu/es [Accessed on 21 January 2023].
- EUROPEAN COMMISSION. WHITE PAPER. White Paper on Artificial Intelligence: a 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 [Accessed on 07 October 2022].
- EUROPEAN COMMISSION. CORDIS EU Research Results. https://cordis.europa.eu/ [Accessed on 11 February 2023].
- EUROPEAN COMMISSION. Migration and Home affairs. https://home-affairs.ec.europa.eu/index_en [Accessed on 12 February 2023].
- EUROPEAN COMMISSION. PARTICIPANT PORTAL. Funding and tenders opportunities. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home [Accessed on 30 January 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 [Accessed on 22 February 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 [Accessed on 18 December 2022].
- INTERNAL SECURITY FUNDS. 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 https://fondoseuropeosparaseguridad.interior.gob.es/opencms/es/fondos/fondo-de-seguridad-interior/ [Accessed on 08 March 2023].
- FP7 FRAME PROGRAMME, Seventh EC RD&I Framework Programme. Specific COOPERATION programme: Security Topic 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 [Accessed on 07 February 2023].
- FRONTEX. European Border and Coast Guard Agency. https://frontex.europa.eu/es/ [Accessed on 29 January 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 [Accessed on 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?" ("Artificial intelligence and civil liability: is a change in the legal system really necessary?"), Diario La Ley, no. 47, 29 January 2021. https://diariolaley.laleynext.es/dll/2021/01/29/inteligencia-artificial-y-responsabilidad-civil-es-realmente-necesario-un-cambio-del-ordenamiento-juridico [Accessed on 27/01/2023].
- WEBSITE Spanish Ministry of the Interior, State Secretariat for Security, Internal Security Funds, ISF. https://fondoseuropeosparaseguridad.interior.gob.es/opencms/es/fondos/fondo-de-seguridad-interior/ [Accessed on 2/02/2023].
- Updated statistics from 2012 to 2020. Statistical Portal on Cybercrime. Spanish Ministry of the Interior, State Secretariat for Crime. https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/portal/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, European Commission, Brussels, 25.11.2020 COM (2020) 767 final 2020/0340 (COD). Data Governance Act. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020PC0767&from=EN [Accessed on 20 February 2023].
- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). OJEU Official Journal of the European Union. https://www.boe.es/doue/2016/119/L00001-00088.pdf [Accessed on 21 February 2023].
- TABLADA, F., "Inteligencia artificial: Definición, tipos y aplicaciones" ("Artificial intelligence: definition, types and applications"), Grupo Atico34, Blog 18 June 2020. https://protecciondatos-lopd.com/empresas/inteligenciaartificial/#Memoria_limitada. [Accessed on 20 September 2022].
- EUROPEAN UNION, Public Consultation Report, digital, 28 March 2019. https://wayback.archive-it.org/12090/*/https://ec.europa.eu/digital-single-market/en/news/* [Accessed on 05 November 2022].
- ZURITA MARTÍN, I., "Las propuestas de reforma legislativa del Libro Blanco europeo sobre inteligencia artificial en materia de seguridad y responsabilidad civil" ("The proposals for legislative reform from the European White Paper on Artificial Intelligence in the field of security and civil liability"), Actualidad Jurídica Iberoamericana, no. 14, 2021, pg. 481. https://idibe.org/wp-content/uploads/2021/03/11._Isabel_Zurita_pp._438-487.pdf [Accessed on 28/12/2022]