Enrique Belda Esplugues
PhD in Engineering from the Polytechnic University of Valencia.
Deputy Director-General for Security Information and Communications Systems and Director of the Security Technology Centre.
Secretariat of State for Security
Ministry of the Interior.

DIGITAL TRANSFORMATION IN THE MINISTRY OF THE INTERIOR FUTURE CHALLENGES THE SECURITY TECHNOLOGY CENTRE (CETSE)

DIGITAL TRANSFORMATION IN THE MINISTRY OF THE INTERIOR FUTURE CHALLENGES THE SECURITY TECHNOLOGY CENTRE (CETSE).

Abstract: One of the functions entrusted to the Deputy Directorate-General for Security Information and Communications Systems (SGSICS) of the Secretariat of State for Security of the Ministry of the Interior is to manage the Security Technology Centre (CETSE). This body is responsible for multiple technological and digital transformation initiatives designed as support tools for the mission carried out by the Spanish State's law enforcement bodies to safeguard the rights and freedoms of citizens, as well as the Ministry of the Interior itself in the fulfilment of its functions. The CETSE has become a leading digital centre, ideal for attracting technological excellence and providing the Ministry of the Interior with a capacity for innovation in the field of security technologies. Today, the Security Technology Centre (CETSE) manages more than 100 projects, and is able to identify industrial sectors, investigate future trends and motivate stakeholders towards innovative technological actions.

Resumen: Como parte de las funciones encomendadas a la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS) de la Secretaría de Estado de Seguridad del Ministerio del Interior, se encuentra la dirección del Centro Tecnológico de Seguridad (CETSE), desde el que se impulsan múltiples iniciativas tecnológicas y de transformación digital al objeto de servir como herramientas de apoyo a la misión ejercida por las Fuerzas y Cuerpos de Seguridad del Estado de salvaguarda de los derechos y libertades de los ciudadanos, así como al propio Ministerio del Interior en el cumplimiento de sus funciones. El CETSE se ha convertido en un Centro de referencia digital, idóneo para atraer la excelencia tecnológica y dotar al Ministerio del Interior de capacidad de innovación en el ámbito de las tecnologías para la Seguridad. Hoy, el Centro Tecnológico de la Seguridad (CETSE) es una realidad que gestiona más de 100 proyectos. Así pues, desde este Centro, podemos identificar sectores industriales, investigar tendencias de futuro y motivar a los interesados hacia acciones tecnológicas innovadoras.

Keywords: Information and Communications Systems; Digital Transformation; Public Security; Technology Centre.

Palabras clave: Sistemas de Información y Comunicaciones. Transformación Digital. Seguridad Pública. Centro Tecnológico.

1.- INTRODUCTION

In the last ten years, Information Technologies have begun to be used en masse by terrorists and terrorist organisations and in the world of serious and organised crime (such as human trafficking and drugs), making it necessary to provide the Spanish State's law enforcement bodies (known by their Spanish acronym "FFCCSE") with instruments capable of fighting against this phenomenon. The undisputed goal is to make people safer, as only then will they be able to exercise their freedom and individual rights effectively.

In this sense, the size of our law enforcement agencies makes it necessary to carefully consider which technological information and communications systems we acquire to support them in achieving their goals, ensuring their present and future sustainability. The only way to do this is through the joint, scalable and interoperable planning and management of each and every one of the necessary solutions, making it possible to have the latest updates of each of the systems managed available at all times.

To this end, in February 2013, the concept of the Technology Centre was created and thus, the Deputy Directorate-General for Security Information and Communications Systems (SGSICS) of the Secretariat of State for Security, launched the project of the Security Technology Centre (CETSE), which took shape in April 2016 in the new facilities of El Pardo (Madrid). Today, three units of the Secretariat of State for Security are located in the aforementioned premises: the SGSICS itself, the National Centre for the Protection of Critical Infrastructure (CNPIC) and the Office of Cybernetic Coordination (OCC).

Figure 1. Security Technology Centre (El Pardo). Source: Created by the author.

In particular, the SGSICS has been assigned the set of functions aimed at planning, proposing and coordinating the development and implementation of databases, information systems and communications systems for joint or shared use by law enforcement based on their needs, in order to provide them with the capabilities and tools that allow them to carry out their work of safeguarding the rights and freedoms of citizens in the different areas of security (crime prevention in its various forms, investigation, reaction and crisis management, etc.) more efficiently and effectively and adapting to the technological challenges of the future.

2.- NOTEWORTHY PROJECTS

In recent years, the strategy of the SGSICS has included the modernisation and evolution of the following projects:

2.1.- Telecommunications

The SGSICS manages the modernisation of the State Emergency Digital Radiocommunications System (SIRDEE), which currently provides secure voice and data communications management capabilities to law enforcement and other organisations, such as the Military Emergency Unit (UME), municipal police and emergency and crisis management services, through its own communications network with more than 70,000 terminals, preparing it for the next evolution in Communications Technologies—LTE Technology—, the progressive implementation of which is set to begin in 2025.

Likewise, a service model has been implemented for the management of the Legal Interception of Telecommunications and Data Retention System, the purpose of which is the centralised reception and recording of electronic communications intercepted by court order for their subsequent presentation by the National Police or Guardia Civil as evidence in court proceedings relating to investigations of terrorism, drug trafficking and organised crime.

2.2.- Smart Borders

The Smart Borders Project is part of a European initiative to manage air, sea and land borders in an integrated manner. In this regard, the SGSICS led the launch of the implementation of the Automated Border Control System (ABC System), which, based on the biometric and documentary identification of travellers, makes it possible to speed up and implement an unassisted border crossing, as well as the implementation of Border Post Control and Coordination Centres such as the one located in the offices of the General Commissariat for Aliens and Borders of the National Police in Madrid or in the Port of Algeciras.

Figure 2. ABC system at El Prat airport (Barcelona). Source: Created by the author.


Figure 3. National Coordination Centre for Border Crossings (Madrid). Source: Created by the author.

Moreover, by Regulation (EU) 2017/2226, adopted in November 2017, it was decided to establish a new Entry Exit System (EES) to record information on the entry, exit and refusal of entry of Third-Country Nationals (TCNs) crossing the external borders of EU Member States within the Schengen area.

EES will be an automated computerised system to register third-country travellers, both visa holders and visa-exempt travellers, each time they cross an external border of the EU. The system will record data such as the person's name, type of travel document, biometric data (fingerprints and facial images captured) and the date and place of entry and exit, in full respect of fundamental rights and data protection. The EES will also record refusals of entry to third-country nationals and will replace the current system of manual stamping of passports.

This system is part of the European Union (EU) Smart Borders package and, together with other new or revised systems (ETIAS, SIS, VIS, etc.), will form a first building block of the new architecture of the EU's interoperable IT systems, under the responsibility of the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA). With the entry into operation of the EES, it will contribute to:

- Strengthening internal security and the fight against terrorism and cross-border crime, as well as preventing irregular (illegal) migration.
- More effectively identifying overstayers and cases of document and identity fraud.
- Facilitating border crossing for bona fide TCNs through the wider use of automated border controls that are faster and more convenient for the traveller.

At the national level, the Ministry of the Interior, through the SGSICS and the National Police, has proposed an ambitious project that is currently under development for the phased implementation of the EES. This includes the implementation of the national central EES system, manual checkpoints for use by border agents, as well as equipment for automated control at land, airport and port border checkpoints, in close cooperation with AENA, the Spanish National Ports Authority and the other port authorities.

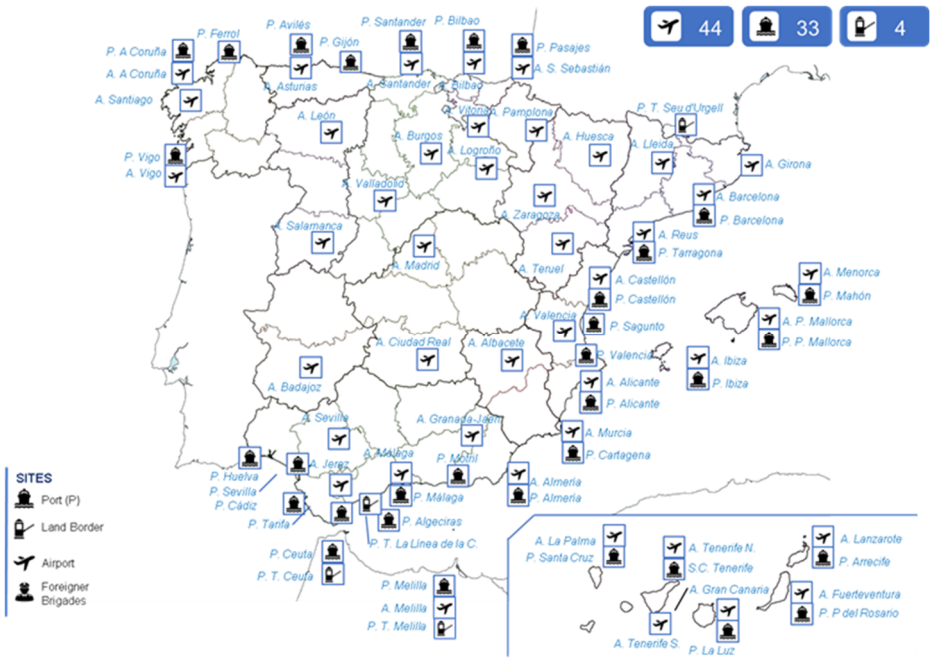

Figure 4. Geographical distribution of border points where EES equipment is planned to be deployed. Source: Created by the author.

With the same goal of further strengthening security at the external borders of the Schengen area, Regulation (EU) 2018/1240 of 12 September 2018 establishes a European Travel Information and Authorisation System (ETIAS) and amends Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.

ETIAS is part of the EU's smart border package and is specifically targeted at third-country nationals exempted from the visa requirement to cross borders, allowing for an assessment of whether the presence of such third-country nationals in the territory of the Member States poses a security risk, a risk of illegal immigration or a high risk of epidemics. To this end, a travel authorisation and the conditions and procedures for issuing or refusing it are laid down. With the implementation of ETIAS, the validity of the travel authorisation that third-country nationals will have to apply for prior to their travel will be checked. The main goals of ETIAS are to:

- Contribute to a high level of security by providing a rigorous security risk assessment of the applicants, prior to their arrival at external border crossing points, in order to determine whether there are concrete indications or reasonable grounds based on concrete indications to conclude that the presence of the person in the territory of the Member States poses a security risk;
- Contribute to the prevention of illegal immigration by providing an assessment of the risk of illegal immigration of applicants prior to their arrival at external border crossing points;
- Contribute to the protection of public health by providing an assessment of whether the applicant poses a high risk of epidemic prior to arrival at external border crossing points;
- Increase the effectiveness of border inspections;
- Support the goals of the SIS relating to alerts on third-country nationals subject to an entry-and-stay ban on persons wanted for arrest for surrender or extradition, on missing persons, on persons wanted to cooperate in judicial proceedings and on persons for discreet or specific checks;
- Contribute to the prevention, detection and investigation of terrorist offences or other serious criminal offences.
- Facilitate inbound and outbound business travel and boost the economy.

With the national implementation of ETIAS, which is currently under development under the leadership of SGSICS and the National Police, technological capabilities for border control officials and third-country nationals will be upgraded. These capabilities will include the necessary mechanisms for the validation of the ETIAS travel authorisation provided by the TCN, thus complementing the controls carried out through the development of the EES system.

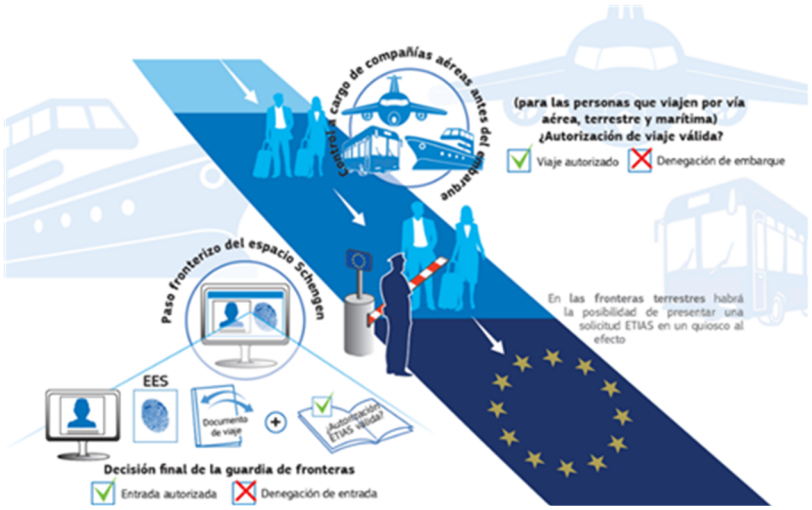

Figure 5. Overview of the ETIAS system. Source: eu-LISA.

2.3.- Other European Systems

The Schengen Information System (SIS RECAST) became operational on 7 March. The SIS system, for which SGSICS is responsible at the national level, and whose users include the National Police, Guardia Civil and regional law enforcement agencies, is the largest information exchange system for border security and management in Europe, as well as for police cooperation. It provides information on wanted or missing persons, third-country nationals without a legal right to stay in the European Union and lost or stolen objects (e.g. cars, firearms, boats and identity documents).

SIS RECAST has been enhanced to include new categories of alerts, biometric data such as palm prints, fingerprints and DNA records of missing persons and additional tools to combat crime and terrorism. The update is important as it will also allow the introduction of preventive alerts to protect vulnerable persons and identify irregular migration. These updates aim to provide national authorities with more comprehensive and reliable information to improve border security and border management in Europe. Enhanced features include:

- Increased information sharing and cooperation: new categories of alerts and more data will be shared through the SIS, ensuring that more complete and reliable information is available to national authorities. Clearer rules and improved structures for the exchange of information through the national contact points (SIRENE bureaux) have been introduced.
- New possibilities to locate and identify wanted persons and to strengthen controls at external borders: in addition to photographs and fingerprints, the SIS will contain new types of biometric data (such as palm prints, fingerprints and palm marks, as well as DNA records, but only in relation to missing persons).
- Additional tools to combat crime and terrorism: new alerts on investigative controls will allow national authorities to collect specific information on suspects of serious crime or terrorism.
- There will be "unknown wanted persons" alerts, containing only the fingerprints of unknown perpetrators discovered at scenes of terrorist offences or serious crimes.
- New functionalities to protect missing and vulnerable persons: National authorities may issue preventive alerts in the system to protect certain categories of vulnerable

persons (children at risk of abduction or possible victims of terrorism, human trafficking, gender-based violence, or armed conflict/hostilities), in addition to existing alerts on missing persons.

- Improvements to prevent and identify irregular migration: Feedback decisions will be part of the information shared in the system to improve the effective implementation of these decisions.
- Improved use of the SIS by EU agencies: Europol and national immigration authorities now have access to all alert categories in the SIS. Operational teams of the European Border and Coast Guard Agency (Frontex) have gained access to the SIS.

In order to provide consistency and obtain maximum performance from the different systems developed, the European Commission is developing the *Interoperability* project. In general terms, it is seen as the ability of information systems to exchange data and enable information sharing, in this case for both effective border security management and the internal security of the European Union. It is based on the management and use of large centralised European information systems and databases.

These include existing systems: Schengen Information System (SIS), Eurodac and Visa Information System (VIS), as well as systems currently under development, being implemented and soon to come into operation:

- ECRIS-TCN: Centralised system with the necessary data to identify third-country nationals with information relating to criminal sanctions.
- EES: System for registering third-country travellers, both short-stay visa holders and visa-exempt travellers, each time they cross—entry or exit—an external border of the EU.
- ETIAS: Scheme for citizens of countries that are currently exempt from visa requirements to visit the Schengen Area, who wish to travel to Europe for tourism, transit or for business.

Interoperability between them being a key requirement, four basic elements have been incorporated to make this possible:

- ESP (European Search Portal): a European search portal that will allow authorised users to perform a single search in all the systems mentioned above and receive results from all the systems they are authorised to access.
- SBMS (Shared Biometric Matching Service): a repository shared by all systems collecting biometrics that will allow users to search and cross-reference biometric data jointly.
- CIR (Common Identity Repository): common repository of identities that will allow the biographical information of non-EU citizens. It shall store biographical data from all systems except the SIS.
- MID (Multiple-Identity Detector): a system for the detection of multiple identities with the dual goal of ensuring the correct identification of bona fide individuals, as well as combating identity fraud.

Ensuring all systems are interoperable and effectively managed and used, the aim is to achieve an improvement in security, border and migration management, address structural deficiencies and share information that is currently in "silos", improving the

deficiencies that hamper the work of national authorities and ensuring that police officers, both border and citizen security, customs and judicial authorities have at their disposal the information they need to carry out their work efficiently and effectively.

Lastly, the SGSICS continues to work on the ongoing updating of the Passenger Name Record (PNR) system, which enables the collection, analysis and establishment of relationships and patterns of information on flight passengers, as a means of preventing terrorist actions and organised crime at our borders.

2.4.- Biometrics

In this area, the update of the ABIS project, Automatic Biometric Identification System (formerly SAID—Sistema Automático de Identificación Dactilar—, started in 2007), where latent fingerprints collected at crime scenes are recorded, as well as the fingerprints of the detainees reported. During 2023, ABIS will also store facial images of detainees for the development of investigations when there are images or videos of criminal offences.

The National Police, the Guardia Civil, the Mossos d'Esquadra and the Policía Foral de Navarra share this database, which is managed and coordinated by the SGSICS, as well as the related information existing in the respective criminal databases. The Ertzaintza has its own system, which has been exchanging data with the Central system since the beginning of 2015.

These fingerprints stored in Spain are also exchanged within the framework of the Prüm Treaty with 21 European countries for the same purpose as genetic profiles.

2.5.- Drones/anti-drones

The SGSICS manages the development of the SIGLO-CD system. The best way to describe it is to break it down into its acronym, Global Counter Drone System, i.e. a system made up of different interoperable solutions, independent of the manufacturer, to detect, identify, monitor and, if necessary, neutralise most commercial drones on the market.

Based on client-server architecture and avoiding proprietary or 'stand-alone' solutions, a national network of detection and neutralisation systems is being created, managed from a Command and Control Centre, which will be able to operate depending on the assigned permissions.

The SGSICS initiated the project, following a resolution of the Secretariat of State for Security, in 2019, to protect the highest State Institutions. The system is currently in Phase 1 and detects over the urban areas of Madrid and Valencia, being able to neutralise commercial drones if they approach certain areas of special protection. As a reference, in 2022 alone, 14,000 commercial drones were detected flying over the urban area of Madrid.

The next phase of the project, currently under tender, will be implemented during the years 2023 to 2025. During this period, a total of 32 fixed detection antennas will be deployed, of which 15 will also be accompanied by neutralisation capability, together

with 86 portable detection cases and 15 portable neutralisation cases. The aim is to cover the most populated cities in the country, with the network to be expanded in subsequent phases.

The current users of the SIGLO-CD system are the National Police, the Guardia Civil, the Royal Household Security Service, the Security Service of the Presidency of the Government and the Ministry of Defence. There is also a collaboration agreement with LaLiga de Fútbol Profesional.

Moreover, the mode of operation of commercial drones coming onto the market and possible solutions for their detection and, if necessary, neutralisation continue to be analysed.

2.6.- Mobility platforms

In this field, the **AlertCops** platform has set a milestone in the provision of public services for citizen security and constitutes an innovative channel for interacting with Spanish law enforcement (a direct communication channel between the public and law enforcement). The capabilities of today's smartphones have made it possible to improve both the effectiveness of the police response for citizens and collaboration in communicating risk situations.

AlertCops, developed by SGSICS, provides a comprehensive and universal public citizen security service through an application (APP), which was completed in early 2015. It is a direct, discreet, effective and complementary channel to the existing ones, to communicate a dangerous situation that someone has suffered or witnessed. The key features of AlertCops are:

- Enabling geo-positioned calls and alerts for immediate attention.
- Enabling a direct chat (similar to WhatsApp) with the nearest law enforcement service centre and enabling the exchange of photos and videos.
- It is integrated into the existing infrastructure and does not affect the action protocols of the SSCDF.
- The entire service is provided and maintained from the technological infrastructure of the Secretariat of State for Security and 100% of the ownership of the development and its components belongs to the Ministry of the Interior.
- Since its deployment to date, many more functionalities have been added, at the request of citizens, working groups of law enforcement and public agencies (Civil Protection, Health, etc.). The most significant are:
- Sending security or collaboration alerts to certain areas.
- Increased presence in groups with new types of alerts: Gender violence, deaf people, hate crimes, squatting and animal abuse.
- “Public Guardian” zones, where citizens can share their position with rescue services, for example for pilgrims on the Way of St James (Camino de Santiago).
- S.O.S. button for gender violence groups (Viogen) and health with law enforcement and S.O.S. button between individuals.
- Systems for locating missing persons in areas without coverage through the smartphone’s WiFi signal.
- Integration of alarm reception centres of private security companies.
- AML, service for the localisation of emergency calls to 091 and 062.

AlertCops provides service to more than 1,200,000 registered users in 6,993 municipalities, and has attended to more than 130,000 risk situations from 100 National Police and Guardia Civil call centres. Many success stories have been reported in the media.

Figure 6. AlertCops system. Source: Created by the author.

AlertCops, as an effective and innovative service, has received multiple international and national awards.

A completely revamped version of AlertCops is currently in the works. As a result of the analysis and feedback from users and law enforcement, the most valuable functionalities (such as the Acompáñame [Accompany Me] service) and the most suitable design lines and usability criteria were identified. The aim is for AlertCops to be perceived as a simple and user-friendly application with valuable capabilities for citizens and law enforcement, not only for requesting police attention but also for obtaining information. As a result of this analysis, a comprehensive redesign of the entire platform has been carried out and will be deployed in AlertCops v7 during 2023.

3.- STRATEGY

The recognition of these projects at both the national and international (EU) levels makes it necessary to continue with the effort in technological matters and, to this end, the SGSICS has designed a Strategic Plan that includes the actions to be developed over the next five years, thus continuing with the goals of technological modernisation of our law enforcement agencies. In this plan, the following lines of action are highlighted:

- The permanent updating of all projects in service and the development of new projects necessary to maintain the safety standards required at the international level.
- The consolidation of the Security Technology Centre, as a technological tool to support operations and exchange information between law enforcement agencies, including the following initiatives:
- Establishment the new Data Processing Centre (CPD) for Security at the CETSE facilities in El Pardo, designed from the perspective of efficiency within the framework of energy savings and respect for the environment, as well as with a systems, storage and communications architecture that is compatible with the

infrastructure currently in place in the DPCs of the SGSICS, National Police and Guardia Civil, allowing for active-active operation as a Backup Centre for the former.

- Development of a Supercomputing Centre for Security to provide capacity for the implementation of new high-level developments for law enforcement in a harmonised manner, resulting in a clear improvement in the efficiency, both technical and economic, of present and future investments.
- Design of a Systems Monitoring Centre (Fusion Centre), which will improve the fusion of information between systems and the exchange of data between different sources (including law enforcement, the public sector and the private sector) and the control of the activity of technological systems through the monitoring of their indicators.

4.- THE IMPACT OF ARTIFICIAL INTELLIGENCE ON OUR ENVIRONMENT

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

In our case, the definition of AI should be as neutral as possible, in order to encompass all the technologies that the term encompasses and those yet to be developed. The aim is to cover all AI, including everything from machine learning to deep learning and hybrid systems.

In the European framework, the European Commission's Directorate-General for Migration and Home Affairs (DG HOME) is also currently discussing, together with the Directorate-General for Communication Networks, Content and Technologies (DG CONNECT), EUROPOL, the eu-LISA Agency and the Member States (MS), the different architecture options for secure data spaces and the technical requirements based on existing legal principles for the implementation of IA. Proof of this was the creation in 2019 of the eu-LISA AI Working Group (WGAI Working Group Artificial Intelligence), in which the Ministry of the Interior participates through the SGSICS.

In 2018, the European Commission set up the High Level Expert Group on Artificial Intelligence (AI HLEG)[1]to develop AI strategies and recommendations. In 2019, the European Commission published guidelines on reliable AI and an assessment check-list for 2020, based on the common values of all Member States in the Area of Freedom, Security and Justice (AFSJ). They were not intended to change existing legislation; they were non-binding recommendations, which, after consultation with the various stakeholders, will set out the key requirements for a socially trustworthy AI in areas such as security, personal data protection, privacy or environmental protection rules.

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, and to examine the feasibility and elements, on the basis of multi-stakeholder consultations, of a legal framework for the development, design and application of artificial intelligence, based on Council of Europe standards on human rights, democracy and the rule of law, the Committee of Ministers of the Council of Europe established the Ad Hoc Committee on Artificial Intelligence

[1] The representative of Spain is from the Ministry of the Interior.

(CAHAI) on 11 September 2019. The CAHAI is unique in that it brings together MS and observers, as well as members of civil society, academia and the private sector.

It works closely with other international institutions, such as UNESCO (United Nations Educational, Scientific and Cultural Organisation), the OECD and the European Union. The SGSICS, representing the Ministry of the Interior, together with the Ministry of Justice and the Ministry of Foreign Affairs, are the Spanish members of this Committee.

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 the development, design and implementation of AI at the international level.

In strategic terms, SGSICS is aligned with the EU Strategy for the Security Union and with the strategic lines set by the European Commission for the Digital Decade and, therefore, contributes to meeting the digital objectives for 2030 from a security perspective. This framework should ensure that AI technology can be developed and implemented in Europe and Spain, while at the same time ensuring that AI technology is not used inappropriately.

In order to address these issues, the SGSICS has defined an internal AI strategy applied to new technologies to be implemented in the Ministry of the Interior, aligned with both the National Artificial Intelligence Strategy (ENIA) and the Spanish AI R&D&I Strategy of the Ministry of Science, Innovation and Universities. The following Strategic Axes for the area of Security and IA aim to address this objective:

- Positioning law enforcement and other bodies dependent on the Secretariat of State for Security as a key element in the development of AI, using the technological potential as a catalyst for their knowledge and experience.
- Promoting the assessment of the technological adequacy of the new system with the functional and operational needs under real conditions of use.
- Promoting a framework of trust and confidence in AI-derived technologies, through legal, ethical and safe use, protection of civil liberties, privacy and citizens' values, fully exploiting the security potential of new technologies.
- Formulating a common data and interoperability strategy, adapted to European standards and large-scale European projects coordinated by both the European Commission and the European Agencies, eu-LISA and Europol.
- Sourcing and nurturing talent, training and development of AI skills and competencies within the Ministry of the Interior.
- Promoting technological advances in AI through public-private collaboration and joint work established by the Government, in order to promote competitiveness and National Security.
- Promoting and actively participating in national and international fora, supporting AI research, development, innovation, implementation and procurement.

5.- RESEARCH, DEVELOPMENT AND INNOVATION

With regard to the Research, Development and Innovation (R&D&I) activity, in accordance with Royal Decree 734/2020 of 4 August, which develops the basic organic

structure of the Ministry of the Interior and Royal Decree 146/ 2021, of 9 March, which amends Royal Decree 139/2020, of 28 January, which establishes the basic organic structure of the ministerial departments, and Royal Decree 734/2020, of 4 August, by which the basic organic structure of the Ministry of the Interior is developed, the SGSICS is responsible for "Agreeing, coordinating, executing and carrying out any other necessary activities relating to participation in European research, development and innovation projects (R&D&I) in matters of security" in accordance with the instructions of the Secretary of State, as well as "Directing the Security Technology Center (CETSE) as the body for implementing the specific functions of this Deputy Directorate and R&D&I policies of the Governing Body".

Specifically, one of the functions of the CETSE's R&D&I Department is to coordinate the Ministry of the Interior's participation in innovation projects. This department currently manages more than 80 international projects from different European funding programmes, including Horizon Europe, the Internal Security Fund (ISF), the Citizens, Equality, Rights and Values Programme (CERV), the European Defence Fund (EDF) and Innovative Public Procurement, among others, providing support in their management to all the bodies dependent on the Ministry of the Interior, such as: National Police, Guardia Civil, Penitentiary Institutions, Civil Protection, the National Office for the Fight against Hate Crimes (ONDOD), the Directorate-General for the Support of Victims of Terrorism, OCC, CNPIC or the Intelligence Centre against Terrorism and Organised Crime (CITCO).

It is also working on the development of national R&D&I projects, according to the needs of the end users of the Ministry of the Interior.

It also actively participates in different international networks and working groups, being national points of contact. Examples include: ENLETS (European Network of Law Enforcement Technology Services), IFAFRI (International Forum to Promote Innovation in First Aid), I-LEAD (Innovation – Law Enforcement Agencies Dialogue) and AHEAD (TowArd sustainable foresigHt capabilitiEs for increAseD Civil Security).

Another major activity of the department is the direction and management of the user community (COU Spain). This initiative brings together academia, industry and end users—law enforcement, Regional Police, Local Police, Emergency Corps, etc., at the national, regional and local levels—, with the aim of carrying out projects of interest to all. The COU is in constant contact and collaboration with the European User Community (CERIS), as well as with other international networks in the field of security with which it maintains close cooperation.

Work is currently underway on the development and implementation of the EACTDA (European Anti-Cybercrime Technology Development Association) National Node through the COU, with the aim of making the tools developed in European projects available to Spanish end users.

6.- DIGITAL TRANSFORMATION

In order to comply with Laws 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations and 40/2015, of 1 October, on the Legal Regime of the Public Sector and aligned with the guiding principles of the Digital Transformation

Plan 2015-2020 of the General State Administration and its Public Bodies, the SGSICS is implementing a new architecture based on microservices technology in the Ministry of the Interior, which will make it possible to offer highly available services with the capacity to adapt to change, necessary for the electronic processing of administrative procedures.

The central part of this platform will be the Digital Administration Services (DAS) Platform, the main goal of which will be to ensure and simplify the integration of all applications and processing systems of the Ministry of the Interior with the main Digital Administration services. This platform will provide uniformity in the Ministry's projects, ensuring the use of electronic files, electronic signature systems and priority electronic communication with citizens. Part of this architecture will also be the Third-Party Integration Platform, which will concentrate electronic interaction with other administrations and national and international organisations in the civil sphere in a communication node.

Furthermore, in order to meet the International Protection demands of the Asylum and Refugee Office (OAR), it is necessary to have a highly secure application that manages the complete life cycle of international protection, statelessness and refugee application files. Currently, the OAR uses the "Asilo" application, developed in 2006. The needs and technology that existed in 2006 are a far cry from what they are today. The application was developed for a very limited number of users, taking into account the sharp increase in recent times.

During 2022, the development of the new application for the Integrated System for the Management of Applications for International Protection, called LARES, has continued. In an environment of exponential growth in applications, this year the number of applications has been exceeded, reaching 118,842. This new application includes enhancements that allow for greater processing capacity. Improvements are being implemented at various levels:

- The day-to-day management of International Protection applications and decisions is being redesigned, creating a new way of working that is automated and adaptable to the context of each country.
- At the technical level, some key technical aspects are taking shape, such as the use of a microservices-oriented architecture, which represents a paradigm shift in the way new developments will be tackled in the future.
- From a usability point of view, a new interface has been created, offering a more user-friendly environment for the application's users. The new interface is designed to be the main point of data entry, which will assist in the flow of information between the different sources, both Police and SG International Protection.
- In addition, the work methodology has been innovated. A "User eXperience Design" methodology has been used to create, together with the users, boards with post-it notes on which all the defined functionality is collected.
- At the strategic level, the system continues to evolve to allow for dynamic and interactive reporting with daily updated information. These reports are customisable and accessible, both for the management units and for the senior managers responsible for these units.

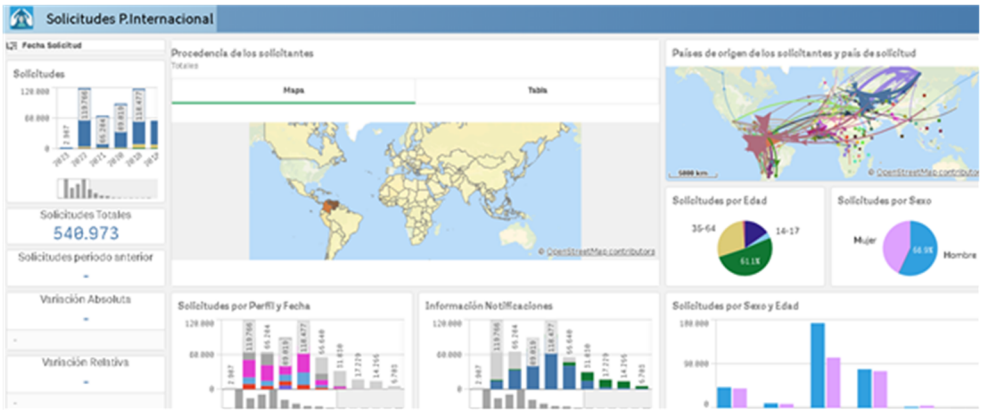

Figure 7. LARES Management Scorecard. Source: Created by the author.

In this area, we should note the implementation of the process of temporary protection resolutions in a maximum of 24 hours, as per Order PCM/169/2022, of 9 March, which develops the procedure for the recognition of temporary protection for persons affected by the conflict in Ukraine.

This procedure has processed more than 150,000 applications for temporary protection since it began on 11 March 2022. In addition, a quick and easy mechanism has been prepared that allows Ukrainian citizens to download their temporary protection order directly from the website of the Ministry of the Interior.

Another example of the use of synergies between the members of the CETSE is the capacity to ensure the security and proper functioning of the electoral scrutiny processes, an area in which Spain is a world leader. The joint work of civil servants and law enforcement is making it possible to gradually reduce technological dependence in this area, which will result in considerable cost savings and improved quality in the medium term. In this process, multiple tasks are carried out to ensure the correct functioning of the computer systems that carry out the vote count on election night.

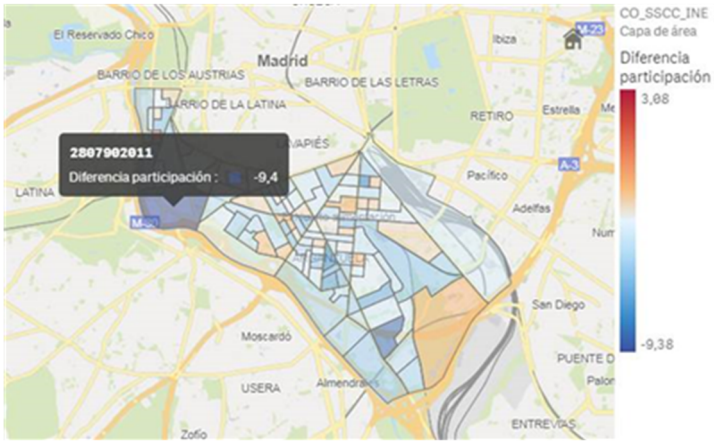

Figure 8. Detail of the election results visualisation tool. Source: Created by the author.

The computer systems, servers and communications are audited at all levels, the tests carried out by the successful tenderer are supervised and additional tests are carried out to ensure the correct functioning of the election count, from the collection of political

party candidacies to the publication in the BOE of the final count, including the provisional dissemination of the Election Day results.

New lines of work have also been initiated, such as the implementation of an electoral results visualisation system. With this system, an evolutionary analysis of the details of the vote or of the turnout can be obtained within a few hours of the general election, down to the polling station level.

7.- CONCLUSIONS

In short, the set of actions described above, as well as the numerous transversal developments to support them, carried out within the scope of the Security Technology Centre of the Secretariat of State for Security, allow us to quickly and securely adapt the functioning of the Ministry to the digital reality of the social environment through the provision of increasingly effective and efficient services of value, ensuring the fundamental rights of citizens at all times in an area of freedom, security and justice.

Glossary

ABC	Automated Border Control.
ABIS	Automatic Biometric Identification System.
AENA	Spanish Airports and Air Navigation (*Aeropuertos Españoles y Navegación Aérea*).
AML	Advanced Mobile Location.
CAHAI	Ad hoc Committee on Artificial Intelligence.
CERIS	Community for European Research and Innovation for Security.
CERV	Citizens, Equality, Rights and Values Programme.
CETSE	Security Technology Centre (*Centro Tecnológico de Seguridad*).
CITCO	Centre for Intelligence against Terrorism and Organised Crime (*Centro de Inteligencia contra el Terrorismo y el Crimen Organizado*).
CIR	Common Identity Repository.
CNPIC	National Centre for Critical Infrastructure Protection (*Centro Nacional para la Protección de Infraestructuras Críticas*).
COU	Community of Users.
CPD	Data Processing Centre (*Centro de Proceso de Datos*).
EACTDA	European Anti-Cybercrime Technology Development Association.
ECRIS-TCN	European Criminal Records Information System - Third-Country Nationals.
MS	Member States.
EES	Entry/Exit System.
ELSJ	Area of Freedom, Security and Justice (*Espacio de Libertad, Seguridad y Justicia*).
ENIA	National Artificial Intelligence Strategy (*Estrategia Nacional de Inteligencia Artificial*).
ENLETS	European Network of Law Enforcement Technology Services.
ESP	European Search Portal.
ETIAS	European Travel Information and Authorisation System.
eu-LISA	European Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice.
Eurodac	European Dactyloscopy (the European system for the comparison of fingerprints of asylum seekers).
FFCCSE	Law enforcement (*Fuerzas y Cuerpos de Seguridad del Estado*).
ISD	Internal Security Fund
HLEG	High-Level Expert Group.
R&D&I	Research, Development and Innovation.
AI	Artificial Intelligence.
IFAFRI	International Forum to Advance First Responder Innovation.
MID	Multiple-Identity Detector.
OAR	Asylum and Refugee Office (*Oficina de Asilo y Refugio*).
OCC	Cyber Coordination Office (*Oficina de Coordinación Cibernética*).
OECD	Organisation for Economic Cooperation and Development.
ONDOD	National Office for Combating Hate Crimes (*Oficina Nacional de Lucha Contra los Delitos de Odio*).
PNR	Passenger Name Record.
SAD	Digital Administration Services (*Servicios de Administración Digital*).

SAID	Automatic Fingerprint Identification System (*Sistema Automático de Identificación Dactilar*).
SBMS	Shared Biometric Matching Service.
SGSICS	Deputy Directorate-General for Security Information and Communications Systems (*Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad*).
SIGLO-CD	Global Counter Drone System (*Sistema Global Contra Drones*).
SIRDEE	State Emergency Digital Radiocommunications System (*Sistema de Radiocomunicaciones Digitales de Emergencia del Estado*).
SIS	Schengen Information System.
TCN	Third-Country Nationals.
EU	European Union
UNESCO	United Nations Educational, Scientific and Cultural Organization.
VIS	Visa Information System.
WGAI	Working Group Artificial Intelligence.