Miguel Fayos Mestre
Lieutenant Colonel of the Guardia Civil
Master's Degree in Security
Master's Degree in Data Protection

THE NEW SCHENGEN INFORMATION SYSTEM

THE NEW SCHENGEN INFORMATION SYSTEM

Resumen: El 7 de marzo de 2023 entró en funcionamiento el Sistema de Información Schengen (SIS) de nueva generación, conocido también como "SIS recast" o "SIS II+". Las negociaciones se iniciaron en noviembre de 2016 y, en diciembre, la Comisión Europea presentó las tres propuestas de reglamento, con tres fines claramente determinados: cooperación policial y judicial; protección de fronteras; y retorno de ciudadanos de terceros estados; dichas negociaciones en el Consejo abarcaron todo el año 2017 y los trílogos con la Comisión y el Parlamento se extendieron durante gran parte de 2018, hasta su aprobación a finales de noviembre de ese año. Entre sus novedades principales destaca un mayor uso de datos biométricos, la mejora de los señalamientos existentes, mayor información para los agentes actuantes, introducción de señalamientos preventivos para impedir el viaje de menores y mayores de edad, y los señalamientos sobre personas desconocidas.

Abstract: On March 7, 2023, the new generation Schengen Information System (SIS), also known as "SIS recast" or "SIS II+", came into operation. Negotiations began in November 2016 and, in December, the European Commission presented the three proposals for regulations, with three clearly determined purposes: police and judicial cooperation; border protection; and return of citizens of third states. The negotiations in the Council covered the entire year of 2017 and the trilogues with the Commission and Parliament lasted for much of 2018, until its approval at the end of November of that year. Among its main novelties is the greater use of biometric data, the improvement of existing alerts, more information for the agents involved, the introduction of preventive alerts to prevent the travel of minors and adults, and alerts about unknown people.

Palabras clave: Sistema de Información Schengen, cooperación policial, cooperación judicial, protección de fronteras, retorno de ciudadanos, señalamiento, dato biométrico.

Keywords: Schengen Information System, police cooperation, judicial cooperation, border protection, return of citizens, alert, biometric data.

ABBREVIATIONS

Art.: Article

MS: Member State

eu-LISA. EU Agency for the Operational Management of Large-Scale IT Systems

JHA: Justice and Home Affairs

EAW: European Arrest Warrant

SGSICS: Subdirectorate-General for Information and Communications Systems for Security

SIGO: Integrated Operational Management System

SIRENE: Supplementary information request at the national entries

SIS: Schengen Information System

1. INTRODUCTION

The entry into force of the Schengen Information System (SIS[1]) dates back to the provisions of Title IV of the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the Gradual Abolition of Checks at their Common Borders, which was signed on 19 June 1990. In June 2024, the Schengen Area will comprise 25 of the 27 EU Member States (with the exception of Ireland and Cyprus) plus Iceland, Liechtenstein, Norway and Switzerland.

This first Schengen Information System became operational on 26 March 1995. However, the European Parliament did have some doubts when creating it, according to Benzo and García (1996), "numerous European Parliament Resolutions [...] consider the Schengen information system risky for individual freedoms" (p. 331).

Subsequently, and with EC Regulation 2424/2021 and Decision 2001/886/JHA, the Commission was entrusted with the development of the second generation Schengen Information System, or SIS II, developed by Regulation 1987/2006 and Decision 2007/533/JHA, which took effect on 9 April 2013.

Following the terrorist attacks in Paris from 7 to 9 January 2015, during which 17 people were murdered, the Ministers of the Interior and Justice of eleven EU Member States, including Spain, issued a joint declaration with a commitment to fight terrorism and strengthen cooperation between the competent services of EU Member States and their relevant partners (the United States and Canada), as well as to improve law enforcement cooperation to prevent and detect early radicalisation. As part of the measures to be implemented, one of the actions taken was the modification of the regulations within the Schengen Borders Code. This amendment aimed to facilitate improved collaboration and communication within the SIS II system at border checkpoints.

In December of 2016, just one month following the commencement of discussions to revise the legal framework for SIS II, a computer graphic was released by the European Commission outlining the existing and anticipated future features. In addition, he argued that the SIS II had proven to be an incredibly useful law enforcement tool for police, border and customs officers. According to recital 1 of Regulation 2018/1862, it is an essential instrument for implementing the provisions of the Schengen acquis, as one of the main compensatory measures contributing to the maintenance of a high level of security within the area of freedom, security and justice of the European Union, in line with the Commission.

According to the Council of the European Union (2018), "the SIS is the EU's most widely used and efficient information system in the area of freedom, security and justice". The evolution of usage statistics shows this. As of 31 December 2013 and 28 Member

[1] Hereafter, in this article the SIS will be referred to as the current Schengen Information System.

States (MS), there were more than 50 million alerts[2], more than 12.8 billion logins to search and update alerts, and more than 80,000 hits from other MS after a search. Four years later, at the end of 2017 and 30 MS, there were more than 76 million alerts from all types of entities, more than 5100 million logins by authorities to perform searches and updates, and more than 240,000 hits. As of 31 December 2023, with 31 MS and the new SIS in place, the statistics showed more than 91 million hits, 15 billion searches and updates, and 357,000 hits.

Pulido Catalán (2022) highlights the importance of the SIS within the new EU information systems architecture, as it interacts with five other major information systems: the Entry/Exit System, the Visa Information System, the European Travel Information and Authorisation System, the European Criminal Records Information System for third country nationals and EURODAC.

It has been a year since the introduction of the new SIS (commonly known as "SIS RECAST"[3]). As one of the numerous contributors to the development of the three legal documents forming the regulatory framework, and having participated in its implementation at both national and European levels, the author finds it worthwhile to highlight the capabilities it provides to the Security Forces personnel.

Most of the documentation used for this article comes from open sources listed in the "normative" section, although technical documentation from the eu-LISA Agency, not available from open sources, has been used for some specific details.

2. THE SIS IN DETAIL

This section describes the points which, the author considers most significant for readers: the current legal basis of the SIS, the components of the SIS at central and national level, the data to be contained in an alert and the SIRENE Bureau.

2.1. LEGAL ARCHITECTURE OF THE CURRENT SIS

The current legal framework of the SIS consists of the following three Regulations:

- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 *on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU.*
- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the *establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and*

[2] Persons, means of transport, banknotes, blank documents, vessel engines, containers, firearms, industrial equipment, documents issued, registration plates, non-cash means of payment and vehicle documents.

[3] "Changed" or "modified".

amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006

- Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 *on the use of the Schengen Information System for the return of illegally staying third-country nationals*

Informally, the three Regulations are known, among SIS users and at Schengen Area level, as the "police and judicial cooperation regulation", the "border regulation" and the "return regulation", respectively.

The choice of this order of presentation, a priori random because it does contradicts the logic of the numbering of the regulations, is entirely intentional and with the following explanation: the first two regulations modify existing regulations (Regulation 1987/2006, related to border checks, and Decision 2007/533/JHA, related to police and judicial cooperation), while the return regulation is a completely new use case. It is also justified by the number of articles, being higher in the police and judicial cooperation regulation with 79 articles, compared to 66 in the border regulation and 20 in the return regulation).

Although there are three regulations, there is just one system and there is no "police and judicial cooperation SIS, border SIS or return SIS". However, there are minor differences as to what kind of alerts can be created, what data they contain, what personal data can be uploaded and which authorities can create or consult alerts. Deliberately, and based on the author's experience over the last ten years in dealing with SIS with non-security force personnel, it has been decided to replace the term "description" in the translations by "alert"; in the French version the term is *signalement* and, in Spanish, "*señalamiento"*. The term "description" is not a translation used by the police in the Security Forces and Corps in Spain, nor in operational texts, nor is it used in the meetings that are held periodically within the Secretariat of State for Security, while "alert" is widely used without causing confusion or misunderstandings.

2.2. SIS COMPONENTS

According to Art. 4 of Regulations 2018/1861 and 1862[4], the SIS is composed of:

- A central system (referred to as Central SIS) comprises a technical support function (referred to as CS SIS), with a database and backup, and a uniform national interface (referred to as NI SIS). The database is in Strasbourg and the backup is in Sankt Johann im Pongau (Austria). As for the NI SIS components, these are in each Member State (MS); in the case of Spain it is located in the Subdirectorate-General for Information and Communications Systems for Security (SGSICS).
- A national system (called N SIS) in each MS consists of the national data systems communicating with the central SIS. The Spanish N SIS is made

[4] Regulation 2018/1860 lacks an article describing the architecture of the SIS. According to Article 19, several articles of 2018/1861 apply, but there is no mention of Article 4 of the latter regulation.

up of the infrastructure located in the SGSICS and the five[5] systems that interact with it. In the case of the Guardia Civil, the system that interacts with the N SIS for consultation, creation, modification and termination of alerts is the Integrated Operational Management System (SIGO). As an interesting detail, it is foreseen that copies of the N SIS can be shared between several Member States.

- A communication infrastructure between the CS SIS, its backup and the NI SIS
- A secure communication infrastructure between the CS SIS and the central infrastructures of the following components of the EU information systems interoperability architecture: the European search portal, the shared biometric matching service and the multiple identity detector.

The main difference from the previous SIS architecture is the last point, as it is directly related to the two EU information systems interoperability regulations: Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 *on establishing a framework for interoperability between EU information systems in the field of borders and visa* and *Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration.*

2.3. ELEMENTS OF AN ALERT SYSTEM

All alerts in the SIS must have at least the following elements: an **entity** (known or unknown person or object[6]); a **reason** for the alert (arrest warrant, missing person, etc.); a **conduct** to be followed in case the alerted entity is found (this can be arrest, protection, whereabouts, etc.); an **authority** creating the alert and a **reference** to the reason for creating the alert (an arrest number, an investigation number, etc.).

However, there are cases where additional data (such as the type of offence or the categorisation of the alert for as an alert under the Police and Judicial Cooperation Regulation, or the grounds for refusal of entry due to alerts under the Border Regulation) need to be entered, which will be specified on a case-by-case basis.

On the other hand, there can only be one SIS alert per MS and there is a hierarchy between the alerts in this and the other two regulations, meaning that, if there are several alerts from several MS, the acting officer must take this order of priority into account. This also applies to the creation of alerts, so if a higher priority alert needs to be created than an existing alert, the existing alert will have to remain at a national level or be discontinued in order for the new higher priority alert to be upgraded to the SIS. This aspect is covered in the Guardia Civil's training on the operation of the SIS.

[5] Systems belonging to the Guardia Civil, National Police, Ertzaintza, Mossos de Escuadra and Policía Foral de Navarra.

[6] For these purposes, an "object" includes means of transport, weapons, containers, blank official documents or identity documents, among others, which is explained in the relevant alert.

2.4. THE SIRENE BUREAU

Among the responsibilities of the MS is the need to designate a national authority, called the "SIRENE Bureau[7]", which must have the following characteristics:

- It must be operational 24 hours a day.
- It must ensure the exchange and availability of information complementary to the alert, contacting the alerting MS when there is a confirmed match and a course of action has been taken.
- It is the single point of contact for each MS for the exchange of complementary information and for facilitating the adoption of measures requested in an alert.
- It coordinates the verification of the quality of the information entered into the SIS and the compatibility of the alerts.
- It validates alerts for persons subject to arrest warrants.
- Contacting the issuing MS when the response requested in the alert cannot be carried out.

The SIRENE Office in Spain is organically part of the International Cooperation Division of the National Police, made up solely of Spanish National Police personnel.

The importance of this SIRENE Bureau is significant, as it is the indirect link between law enforcement officers anywhere in the Schengen area. Thus, an officer of MS A, after conducting a search and confirming that the person or object in question is listed in the SIS and on which he has to take action, must call his SIRENE Bureau; this SIRENE Bureau of MS A must contact the SIRENE Bureau of MS B that created the alert, which in turn shall contact the authority issuing the alert so that it is aware of its finding. The SIRENE Manual, of which there is a version for the police and judicial cooperation regulation and others for the border and return regulations, details the functioning of these offices, the priorities of the alert and essential aspects of the alert, among others.

3. REGULATION ON POLICE AND JUDICIAL COOPERATION AND DIFFERENCES WITH DECISION 2007/533/JHA

Regulation 2018/1862 might be considered as an evolution of Decision 2007/533/JHA, in some cases maintaining the same numbering of the articles for the alerts, it can be considered as the main one within the regulatory architecture of the new SIS. The choice is not arbitrary, but follows the criterion of the highest number of possible alerts (seven) and allows the creation of alerts not only on persons:

- Persons wanted for arrest for surrender purposes and wanted for arrest for extradition purposes, corresponding to Art. 26. This type of alert already existed with the 2007 Decision.
- Missing persons (to be reported or protected) and vulnerable persons (both adults and minors) to be prevented from travelling, corresponding to Art. 32. These types of alerts have several subcategories. Missing persons

[7] This acronym stands for " *Supplementary information request at the national entries*".

already existed with the Decision, while the reference to vulnerable persons is new.

- Persons wanted for judicial procedure, corresponding to Art. 34. This includes witnesses, persons summoned to appear for alleged offences, persons who are served with a summons in order to report to serve a penalty involving deprivation of liberty. This type of alert already existed with the Decision.
- Persons and objects for discreet checks or specific checks[8] or in the interest of the Union concerning third-country nationals, corresponding to Art. 36 and 37 bis. Specific checks and discreet surveillance already existed under the Decision, although they have been improved; investigative checks and checks on third country nationals in the interest of the Union are new.
- Objects for seizure or use as evidence in criminal proceedings, corresponding to Art. 38. This type of alert already existed with the Decision, although there are modifications in the type of objects that can be alerted.
- Unknown persons being sought for identification under national law, corresponding to Art. 40; this type of alert is new.

The main differences with the Police and Judicial Cooperation Regulation in terms of personal data, the possible types of alert, specific rules on biometric data and connections between alerts are mentioned below.

3.1. PERSONAL DATA

The data set covered by the 2007 Decision has increased, providing end-users with more information to enable appropriate law enforcement actions. Regarding personal data, the main data that allow identification are kept, such as name and surname, both current and previous, aliases, objective physical features (height, eye colour, hair, among others), place, date of birth, sex and nationality/s The person's registration number in a national register can also be added, as well as details of their identity document/s (number, type, country and date of issue) and even photographs, preferably in colour.

In terms of biometric data, photographs of the person (full body, significant scars, tattoos, etc.) can be added, not just facial images, as well as full fingerprint data, not just fingerprints. In case of missing persons, and in the absence of other biometric data and with the express consent of relatives, DNA profiles can be included.

Three further indications about the person can also be added; the Decision only considered whether the person was armed, violent or had escaped, whereas the current Regulation adds whether the person is a suicide risk, a threat to public security or involved in terrorist activities. Several indications can also be selected at simultaneously. Finally, in case of missing and vulnerable persons, the case classification must be added.

[8] In the Spanish version of the Regulation, the term "control" is used for all three types (specific, investigative and discreet), although for operational purposes it was decided to use the term "discreet surveillance" because the terms "control" and "discreet" can be contradictory.

As regards the quality of the individual's data, the use of any database (law enforcement - subject to the Data Protection Directive 2016/680[9]- or not - subject to the General Data Protection Regulation 2016/679[10]) is of particular relevance to have quality data which, on the other hand, must be entered whenever available. In the case of Spain, the main ones are ADDNIFIL data processing operations (management of the national identity card) and ADEXTTRA (administrative actions related to foreign, EU and stateless citizens), both of which are the responsibility of the National Police, and which expressly provide for the transfer of data to the SIS. In this way, and with the correct use of such data processing, quality biographical and biometric data (of Spanish citizens and residents in Spain) can be made available, reducing the possibility of errors being made when verifying the identity of persons whose fingerprints have been recorded. For example, according to Bellanova and Glouftsios (2020, p. 12), "*it is precisely because of the bad quality of alert data that queries in the SIS II can result in hundreds of false positives*".

Concluding with data protection regulations, art. 66 of the Regulation on police and judicial cooperation provides that EU Directive 2016/680 on the protection of personal data shall apply, provided that the processing is carried out by the competent national authorities for the purposes of the prevention, investigation, detection or prosecution of terrorist offences or other serious criminal offences. This Directive was transposed into Spanish law in Organic Law 7/2021[11]. Citizens may exercise their rights of access, rectification and deletion, although these rights may be limited in accordance with the provisions of the aforementioned European and Spanish regulations, in arts. 15 and 16, and 24, respectively.

3.2. ALERT DATA

In point 3, a list of the alerts was shown, specifying whether they were new or existing; in the case of those existing in the 2007 Decision, it was indicated whether they had been modified by the new Regulation to a greater or lesser extent. The clause that they are valid for as long as they are necessary for the purposes for which they were created was also maintained, however, in the new wording specific time limits were established that are better defined than in the Decision. The basic data of the alert remains unchanged (reason, authority creating the alert, reference to the decision giving rise to the alert, measures to be taken, connection(s) with other alerts and type of offence).

---

[9] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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).

[11] Organic law 7/2021, of 26 May, for the protection of personal data processed for prevention, detection, investigation and prosecution of criminal offences and the execution of criminal procedure.

In common with all the designations of persons, with the exception of Art. 40 (unknown persons), at least one surname and the year of birth of the person must be available. In the case of object alerts, at least one number must be available to identify the object (number plate, serial or chassis number, or similar).

3.2.1. Persons wanted for arrest for surrender or extradition purposes - Article 26

The main difference with the Decision is that there is now the option for the issuing MS to deactivate the validity of the arrest warrant for a period of 48 hours, extendable in periods of 48 hours, in order not to prejudice an ongoing operation. This requires judicial authorisation and all SIRENE Bureaux must be notified. In addition to the other alerts, in this type of alert, it is compulsory to enter one of the offences listed in Framework Decision 2002/584/JHA, summarised in 26 options to be completed, and that the European Arrest Warrant (EAW) is available in the alert for viewing.

The possibility is also maintained that, if the summons cannot be executed in a MS, it may be replaced by an address and whereabouts enquiry.

Its validity was increased from three to five years, with reviews every five years.

3.2.2. Missing and vulnerable persons - Article 32

This article has been amended to allow for additional cases. The regulation retains the cases of missing persons who must be placed under protection for their own safety or to prevent threats, as well as those who do not require protection, and adds:

- Children at risk of abduction by a parent, family member or guardian and who should be prevented from travelling.
- Children who are to be prevented from travelling because there is a specific, evident risk that they will leave or be taken from the MS and become victims of trafficking, forced marriage, female genital mutilation or other forms of gender-based violence; be victims of or involved in terrorist offences; or be recruited or enlisted into armed groups or forced to take an active part in hostilities.
- Vulnerable persons of legal age who must be prevented from travelling for their own protection, due to a specific and evident risk of leaving the territory of a MS or being taken outside the territory of a MS and becoming victims of trafficking or gender-based violence.
- All sub-types related to children and adults at risk should be entered when creating the alert to provide useful information for officers who need to intervene following a search in the SIS.

Other amendments compared to the 2007 Decision include:

- Notification from the CS SIS to the issuing MS that a minor has four months left to reach the age of majority to modify the alert and adapt it to the age of majority, or to cancel it.
- The designation of vulnerable persons must be supported by a decision of a competent authority or a judicial authority.

The valid term was amended from three to five years, with reviews every five years, in the case of missing persons, with reviews every five years; for vulnerable persons (both adults and minors), the term is one year, with annual reviews.

3.2.3. Persons wanted for the purpose of judicial proceedings - Article 34

The only change relates to the express mention of the use of connections between signs, with no new categories of persons. In contrast to the indications in Art. 26, the introduction of the type of offence is optional.

The three-year period remained unchanged, with reviews every three years.

3.2.4. Controls and Surveillance - Article 36

The main amendments to these articles, which regulate controls and surveillance, can be summarised as those directly related to the characteristics of alert, the types of alert and the entities on which such alert can be issued.

With regard to the characteristics of the alert, the 2007 Decision envisaged two situations for its creation: where there are clear indications that a person intends to commit or is committing a serious criminal offence, as referred to in Art. 2(2) of Framework Decision 2002/584/JHA[12]; or where the overall assessment of a person, particularly on the basis of previous criminal acts, suggests that they will continue to commit serious criminal offences, as referred to in Art. 2(2) of Framework Decision 2002/584/JHA, in the future.

The current Regulation replaces the terminology "serious criminal offence" with "offence" in the two cases already existing under the Directive, but includes in each of the above cases Article 2(1)[13] of Framework Decision 2002/584/JHA and includes a third case: where the information referred to in Article 37(1) is necessary for the execution of a custodial sentence or detention order in relation to a person convicted of any of the offences referred to in Article 2(1) and (2) of Framework Decision 2002/584/JHA.

In relation to the types of alert, the inclusion of the "investigative check" should be highlighted; since there are Member States where the legal system does not provide for a "specific check", which implies the search of a person and their property, and that "discreet surveillance" should involve obtaining information implying minimal interaction (or lack thereof) with the targeted person, vehicle or object, it was decided to introduce the so-called "investigative check". This measure provides for an interview with the person reported or found with a reported object or vehicle and is at an intermediate level in terms of information-gathering capacity. As can be deduced, the ability to obtain

[12] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JAI)

[13] A European Arrest Warrant may be issued for acts for which the law of the issuing Member State prescribes a custodial sentence or detention order for a maximum period of at least 12 months or, where the purpose of the request is to impose a custodial sentence or detention order of not less than four months' imprisonment.

information is directly proportional to the degree of interaction with the entity concerned, although this may compromise the discretion to act.

One aspect to consider in this type of alert is that the targeted person, or the person found with a object, should not be informed that such an alert exists. In the discussions of the various drafts, it was considered that the identified person should be informed, which required the intervention of several delegations (including the Spanish delegation) to eliminate this possibility, which would undermine the effectiveness of this measure for law enforcement and jeopardise the very functioning of the SIS.

Although the type of offence can be optionally included in such alerts, it should be made compulsory so as not to jeopardise the safety of the officers involved. For example, it is not the same to have to carry out a specific check on a person in connection with the commission of cybercrime as with the commission of a homicide. Having this information in advance allows security measures to be taken. This important aspect is emphasised in the training given in the Guardia Civil on the use of the SIS, so that the future issuer of a SIS signal sees the importance of entering all the corresponding information for their own benefit and for the benefit of the acting agent.

In terms of action in the event of such a tip-off, there are no major differences from the Decision in that the acting officer should gather basic information about the person or object found, including:

- That the person or object has been located.
- Place, time and reason for the check.
- Itinerary and destination of the journey.
- Accompanying persons of the reported person; occupants of the vehicle, vessel or aircraft, and those who may be presumed to be related to the reported person. In the case of object alerts, any identity revealed.
- Objects carried, including travel documents.
- Circumstances in which the reported person or object has been located.

However, in this type of alert, the possibility is given to enter "other information requested". This new section makes it possible for the MS to select from a set of 15 graded options (of which up to five can be selected) and one with the ability to enter free text (only available for viewing in the SIRENE Bureau). The options include whether works of art or jewellery or false documents related to the purchase and sale of objects, etc are being carried. It should be noted that the first version of the technical documentation submitted by the eu-LISA Agency to SGSICS included more than 45 different options, which would have been difficult to manage. Information obtained from a control or surveillance must be communicated through the exchange of supplementary information via the relevant SIRENE Bureau by means of forms with specific information fields.

As in the Decision, immediate notification is maintained for serious cases or cases which, without being serious, justify this measure. The measure must be duly justified when generating the alert, as it may involve communication at any time of the day from the SIRENE Bureau in the event that the reported entity is found at any point in the Schengen area. Again, this aspect is dealt with in the training courses provided, as the SIRENE Bureau does not validate the reports in which this justification has not been provided.

Regarding the entities that can be marked on the basis of this Article, the Decision allowed the creation of alerts only for persons, vehicles, vessels, aircraft and containers. The Regulation additionally allows for the creation of control and surveillance alerts for the following objects:

- Trailers with an unladen mass exceeding 750 kg.
- Firearms.
- Blank official documents that have been stolen, misappropriated or lost, or are presented as such but are forged.
- Issued identity documents (passports, identity cards, residence permits, travel documents and driving licences) which have been stolen, misappropriated, lost or invalidated, or which are represented as such but are false.
- Non-cash means of payment (such as a credit card).

The retention period for this type of alert, in the case of persons, was kept at one year, with annual reviews. However, for objects it was increased from three to ten years, with reviews every ten years.

3.2.5. Alerts regarding third country nationals in the Union's interest - Article 37 bis

This article, which was introduced following the publication of Regulation 2022/1190 of 6 July 2022, allows Member States to introduce alerts on third country nationals on the basis of a proposal from EUROPOL, the origin of which is information received from third country authorities or international organisations. However, it is not yet operationally implemented. Does this mean that it is not possible to create an alert about a citizen of a third state? No, because this particular case would only be used if the information comes from a third state and has been provided to EUROPOL.

This type of alert enables an officer to know that the person is suspected of involvement in a serious crime or other forms of serious delinquency listed in Annex I of Regulation 2016/794[14], known in the law enforcement community as the EUROPOL Regulation.

In a quick overview, this article allows for the creation of an alert similar to Art. 36 (checks and surveillance), but differs in that there are only two cases for its introduction, namely when there are objective indications that a person intends to commit or is committing any of the offences in Annex I of the Europol Regulation, or when the overall assessment of a person, in particular on the basis of criminal acts committed in the past, suggests that this person could commit any of the offences in Annex I of the Europol Regulation.

In addition, EUROPOL will only propose the creation of such a alert when the information is reliable and at least one of the above conditions is met, and that there are no existing alerts in the SIS for the same person. An alert may be created for the same type of objects as those referred to in Art. 36, with the exception of issued identity

[14] The offences in this list coincide almost entirely with those in Framework Decision 2002/584/JHA.

documents, provided that there are clear indications that they are related to the person being alerted.

When this type of alert is operational, its operation shall be similar to discreet surveillance, taking into account that the field "other information sought" cannot be included when generating the alert.

It is valid for one year, with annual reviews.

3.2.6. Objects to be seized or used as evidence - Article 38

There are differences between the objects that can be identified between the 2007 Decision and the current Regulation. With the exception of transferable securities and non-cash means of payment, which under the new Regulation can no longer be identified as objects to be seized or used as evidence in criminal proceedings, the range of options increases:

- All motor vehicles are covered, irrespective of the propulsion system, whilst the Decision covered vehicles with a cylinder capacity exceeding 50 cubic centimetres.
- Trailers with an unladen mass of more than 750 kg, caravans, boats and their engines[15], aircraft, containers, firearms[16], industrial equipment, blank official documents, issued identity documents, vehicle documentation[17] and banknotes (including counterfeit ones) are retained.

These new types of objects are included:

- Aircraft engines.
- Information technology articles.
  - Storage devices, servers, network devices, smart devices and general purpose electronic items[18].
- Identifiable components of motor vehicles.
  - Engines, transmissions and gearboxes, airbags, multimedia devices, steering wheels and engine control units. It should be noted that catalytic converters, which are commonly stolen and contain high-value metals (platinum, palladium and rhodium) and may have a serial number that allows their identification, are not included.
- Identifiable components of industrial equipment.
- Other identifiable objects of high value, although this category is not yet operational.

[15] The Decision specifically covers outboard engines, whereas the Regulation covers all kinds of engine.

[16] Also included as firearms are cannons, howitzers, mortars, grenade launchers, missiles, airguns, airsoft and disabled weapons.

[17] Registration certificates and number plates, including forged ones.

[18] The specific term in the technical documentation is *consumer electronics*.

- Watches, bicycles (conventional and electric), ingots, sound, video and photographic goods.

The Commission may adopt delegated acts to amend the last four types to include new objects, which is a reasonable provision in view of the new devices that are increasingly used and can be stolen. It has been proposed, for example, that crossbows and bows should be included, and that airsoft weapons and airguns, are not firearms either.

3.2.7. Unknown persons to be identified - Article 40

Within the emphasis given to the use of biometric data in the regulation, this provision allows the identification of unknown persons whose fingerprint data have been discovered at the sites where terrorism or other serious crimes are under investigation and where it can be established with a very high degree of probability that they belong to a perpetrator of such a crime.

The registration process must first involve a search for fingerprint data in a national, EU or international database. It should be noted that SIS may be consulted in relation to the indications of Art. 26, 32, 36, 37 bis, and 40. If, and only if there is no match, can such an alert can be created.

In this type of alert, apart from the fingerprint data enabling identification, the type of crime has to be provided; because the alert requires that the fingerprint data must be collected at the scene of a serious crime or terrorist offence, to provide intervening officers with useful information that may enable them to take additional security measures.

In case of a match when identifying a person by fingerprint data, an expert checks that the data of the identified person match those of the fingerprint, notifying the issuing MS of the identity and whereabouts of the identified person by exchanging complementary information to facilitate the investigation of the case.

This type of alert would not have existed during the drafting process had it not been for the insistence of several delegations (including the Spanish delegation), because others considered that the exchange of dactyloscopic data through the then existing PRUM decisions covered this need. The problem is that the exchange of data through these decisions only provided for investigations and not for real time identifications on the street, so that a then unknown capability was lost. The new PRUM Regulation[19], recently published, maintains the exchanges of fingerprint data, but again only for

[19] Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) No 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation). These two decisions already allowed the exchange of fingerprints, DNA and vehicle registration data.

investigations. Operational necessity and the possibility of multiplying the probability of having matches with unknown prints prevailed.

It is valid for three years, with reviews every three years.

3.3. SPECIFIC RULES FOR BIOMETRIC DATA

According to Art. 43.1, photographs, facial images, dactyloscopic data and DNA profiles may be used to confirm the identity of a person who has been located following a search with biographical data in the SIS, but according to Art. 43.2, dactyloscopic data may also be used to identify a person. Due to advances in technology, the regulation provided for this identification measure by equipping the Central SIS with an automatic fingerprint identification system.

Article 43.4 provides for a possibility the use of photographs and facial images to identify a person in the context of official border crossings should not be concealed. That is, the use of facial recognition. However, in the wording of the drafts there was a subtle difference from the final wording, which was the presence of the adverb "only", which would limit the use of facial images and photographs within the national territory.

It was the intervention of several delegations (again, the Spanish delegation) that succeeded in having this adverb removed so that the possibility of using facial images to identify a wanted person in the SIS was not curtailed. The argument for this measure not to be limited exclusively to border crossings was not only limited to those for the detection of persons with security measures such as checkpoints or arrest warrants, but to one where there could hardly be any opposition, such as the tracing of missing persons and victims of crime.

The final wording of Art. 43.4 established that a report from the Commission was first necessary to analyse whether the technology is available, reliable and ready for use, consulting the European Parliament on this report. It is only at official border crossing points that the Commission may adopt delegated acts determining the circumstances in which photographs and facial images may be used to identify persons.

3.4. LINKS BETWEEN ALERTS

The 2007 Decision already envisaged the use of inter-alert connections, provided that they meet an operational need of the issuing MS. One example of a connection between alerts could be an alert involving two vehicles and one for the identified occupants that are known to be used to commit crimes against property. The real usefulness of these connections is that when one of the linked entities is queried, the system used by the agent to view the SIS data should quickly allow him to see the other related alerts without having to do an additional search. This makes much more information instantly and effortlessly available. The term used at SIS user level is "link".

The regulation goes a step further, so that in all alerts (with the exception of those in Art. 38 and 40) explicitly include the possibility of linking to other alert, although they could also be used in the other two cases; for example, if several firearms are stolen, there is nothing to prevent links being created between their alert, and it would also be operationally feasible (in theory) to create links between alerts for unknown persons.

However, at the technical level, it was decided to further advance the concept of connection by creating the concept of "extension". The main difference is that an extension is always from a person to an object (and not for all types of object) without any alert for that object.

The provisions that provide for extensions are those in Arts. 26, 32 and 34, meaning that when you search for an object that is an extension of a person, that person's alert will be displayed directly on the screen. Extensions are not envisaged for the alerts in Art. 36 and 37 bis, because if an object is to be listed in the SIS with a alert, it would be incongruous to use an extension.

The clearest example of the use of extensions is that of a missing person with their vehicle. With the Decision, if it was necessary to locate a missing person whose vehicle was known to have been taken, there was the option to create two alerts in the SIS: one for the person and one for the vehicle (it would be even worse to create one for a vehicle to be seized or used as evidence in criminal proceedings), creating a *link* between both. However, as we have already seen, the creation of a control or surveillance for the vehicle implies that the vehicle may have some connection to the commission of serious crimes or terrorism, so this measure may be considered disproportionate, even though it may have some utility. However, the same effect is achieved with the extension without the need to create a control or surveillance alert on that vehicle. The vehicle registration number can be used as query data and will allow the acting officer to know that there is a person with a missing person signal related to that vehicle without there being an alert on that vehicle, this being a fully proportionate action for the purpose pursued.

The other nuance to be taken into account is whether or not it is necessary to create a marker on an object in order to locate a person: if the answer to the question "should a marker be created on an object to locate a person on whom there is a marker" is "yes", this would be the case of the *link*. In case of a negative answer, and provided that it is technically feasible according to the SIS rules, an extension is involved.

4. BORDER REGULATION AND DIFFERENCES TO REGULATION 1987/2006

Regulation 2018/1861, known as the Border Regulation, is the evolution of Regulation 1987/2006 for denying entry into the Schengen Area to third state nationals for whom this measure has been taken, and shares that it only has the alert of refusal of entry, albeit with minor improvements to facilitate police intervention. As a special feature, such alerts can only be created by national immigration authorities.

Border controls are of vital importance and must be carried out systematically and correctly. One example of how this has sometimes not been the case in the past; in relation to one of those arrested for the 13 November 2015 attacks in Paris, according to Bellanova and Glouftsios (2020, p. 1), "*information about this person was already stored in the Schengen Information System (SIS II) before he arrived at the border*" (information about this person existed in SIS II before he reached the border).

The differences can be summed up in terms of the data of the person and of the alert, as well as the specific conditions of the alert.

4.1. PERSONAL DATA

The data set covered by the 2006 Regulation has been increased, providing the end-user with more information to enable appropriate law enforcement action. It is summarised as follows:

- In relation to personal data, there is no difference with the Regulation on police and judicial cooperation, although DNA data are not covered.
- The difference is that it is possible to indicate whether the reported person is a family member of an EU citizen or another person with the right of free movement, or whether the decision to refuse entry and stay is based on a previous conviction, serious threat to security, circumvention of national or EU law on entry and stay, entry ban or restrictive measure.

4.2. ALERT DATA

The details of the alert remain unchanged (reason, authority creating the alert, reference to the decision giving rise to the alert, measures to be taken, connection(s) with other alerts and type of offence). However, there is a significant nuance with the 2006 Regulation, which is the obligation to fill in the grounds on which the decision to refuse entry is based, with five possibilities:

- Previous conviction; similar to the 2006 Regulation, which can occur when the citizen has been convicted in a MS of an offence punishable by a sentence of at least one year.
- Serious threat to security; where there are serious grounds for believing that the third-country national has committed a serious crime, in particular a terrorist offence, or clear indications of their intention to commit such a crime on the territory of a MS.
- Circumvention of national or Union law on entry and stay.
- Entry ban, in accordance with procedures complying with Directive 2008/115/EC.
- Restrictive measure; for third country nationals, aimed at preventing their entry into or transit through the territory of the Member States, where such a measure has been adopted in accordance with legal acts adopted by the Council, including measures implementing a travel ban determined by the United Nations Security Council.

The response of officers will depend on whether the person in question is found, with no difference to the 2006 Regulation, in the following scenarios:

- At external borders trying to enter a MS or when trying to obtain a short-stay visa at a consulate. In this case, the person will be refused entry and the SIRENE Bureau is contacted.
- Within the territory. In this case, information shall be obtained from the person, the competent immigration authority and the SIRENE Bureau is contacted.

The alert is valid for a generic period of three years, to be reviewed every three years after an assessment of the case; if the national decision to create the alert is valid for more than three years, it may be reviewed every five years.

As for the rules on processing biometric data, they are similar to those of the regulation on police and judicial cooperation.

5. RETURN REGULATION

Completely new and without precedent, this regulation addresses the need for the SIS to provide for alerts related to decisions to send back third state nationals and for these to be enforceable by officers of the competent authorities accessing the SIS, which in practice are those carrying out border controls, those carrying out controls and customs in the Member States and those involved in the prevention, detection, investigation and prosecution of serious crime and terrorism or other serious offences. Similar to border regulations, such alerts can only be created by national immigration authorities.

Its wording refers to that regulation to avoid redundant articles in a text which, together with the aforementioned border regulation, serves to maintain confidence in the Union's asylum and migration policy.

5.1. PERSONAL DATA

Briefly, with regard to personal data, there is no difference with the border regulation, with the only exception that the return regulation does not provide for the possibility of adding objective physical features. In addition, the following points are added: it can be indicated whether the return decision has been suspended or the entry into force of the return decision has been postponed as a result of an appeal; it can be indicated whether the return decision is motivated by the fact that the third country national is a threat to public security or national security; the last day of voluntary departure should be indicated if stated in the return decision issued by the competent authority; and it should be indicated whether the return decision is accompanied by a refusal of entry.

5.2. ALERT DATA

These alert are entirely new; however, they share the essential data of the other types of alert (reason, authority creating the signal, reference to the decision giving rise to the signal, measures to be taken, connection(s) with other alert and type of offence). The response of officers will depend on whether the reported person is found in the following scenarios:

- At external borders when leaving the territory of a MS. In this case, information is collected on departure, as well as the place, date and time, and whether the departure was forced and not voluntary, and the SIRENE Bureau is contacted.
- At external borders trying to enter a MS or when trying to obtain a short-stay visa at a consulate. In this case, information on the location of the person (at the border or at a consulate), as well as the place, date and time, is collected and the SIRENE Bureau is contacted.

- Within the territory. In this case, information shall be obtained from the person, the competent immigration authority and the SIRENE Bureau is contacted.

The alert is valid for a generic period of three years, to be reviewed every three years after an assessment of the case. If the national decision is valid for more than three years, it may be reviewed every five years.

As in the border regulation, the rules on processing biometric data are similar to those in the police and judicial cooperation regulation.

6. CONCLUSIONS AND PROPOSALS

The usefulness of the SIS as a major information system for police use is patently clear. It allows the police to take measures on a person or object to be available to officers almost instantly, in some cases. Compared to INTERPOL, the SIS is suitable for exchanging many more types of information and on more entities; for example, INTERPOL does not have an "analogous" measure for checks and surveillance for means of transport or other objects. The availability of the SIS to all officers is another advantage, given that access to INTERPOL's databases is often restricted to the National Central Bureaus.

However, there should be no room for complacency, as the SIS can (and must) evolve. Among the measures discussed during the Spanish Presidency of the Council of the EU, a modification to fight more efficiently against theft was proposed. Since the SIS envisages the possibility of creating alerts on stolen objects that are commonly and easily trafficked to second-hand shops (mobile phones, laptops, tablets, bicycles, etc.), an amendment to the Regulation on police and judicial cooperation allowing very limited access to second-hand shops was considered of interest. Such access would, in any case, not bring up personal data and could only be used to search for certain types of assessed objects. In this way, a business could be notified in real time to contact its reference police force to clear up any doubts about the lawful origin of an item offered for sale by a private individual and even to be able to locate the seller and launch an investigation. This could reduce the likelihood of the illegal purchase and sale of an second-hand object.

However, this process can be complex because it requires the agreement of the other Member States and, finally, for the European Parliament to consider the measure to be proportionate. The author believes that this measure could be a sign of what European institutions and security forces can provide for their citizens.

7. BIBLIOGRAPHICAL REFERENCES

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). *SIS II - 2013 Statistics.* https://www.eulisa.europa.eu/Publications/Reports/eu-LISA_SIS%20II%20-%20Statistics%202013.pdf

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). *SIS II - 2017 Statistics.* https://www.eulisa.europa.eu/Publications/Reports/2017%20SIS%20II%20Statistics.pdf

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA). *2023 Annual Statistics.* https://www.eulisa.europa.eu/Publications/Reports/SIS%202023%20Annual%20Statistics%20-%20Report.pdf

Bellanova, R., & Glouftsios, G. (2020). Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance. *Geopolitics, 27(1)*, pp. 160–184. https://doi.org/10.1080/14650045.2020.1830765

Benzo Sáinz, F. and García Inda, A. (1996). The third pillar of the European Union. cooperation in justice and home affairs. *Revista Aragonesa de Administración Pública, 8*, pp. 299-333. https://dialnet.unirioja.es/descarga/articulo/8888566.pdf

Bigo, D., Brouwer, E., Carrera, S., Guild, E., Guittet, E-P., Jeandesboz, J., Ragazzi, F. and Scherrer, A. (2015). *The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda, European Journal of Migration and Law.* https://www.ceps.eu/ceps-publications/eu-counter-terrorism-policy-responses-attacks-paris-towards-eu-security-and-liberty/

European Commission (2016): *The Schengen Information System.* https://home-affairs.ec.europa.eu/document/download/f6d95205-ebc2-444b-b580-d1de7b24c687_en?filename=sis_factsheet_21122016_en.pdf

Council of the European Union (2018). *Schengen Information System: Council adopts new rules to strengthen security in the EU.* https://www.consilium.europa.eu/en/press/press-releases/2018/11/19/schengen-information-system-council-adopts-new-rules-to-strengthen-security-in-the-eu/

Transparency Portal. General State Administration (8 May 2024). *Register of Processing Activities of the Ministry of the Interior.* https://transparencia.gob.es/transparencia/dam/jcr:b3eb17bc-b1a7-4092-9c99-f11f62d868ae/20240508%20Registro%20de%20Actividades%20de%20Tratamiento%20del%20Ministerio%20del%20Interior.pdf

Pulido Catalán, F. (2022). The interoperability of European information systems. Operational application and technical integration for the Guardia Civil. *Cuadernos de la Guardia Civil, 67,* pp.103-118. https://biblioteca.guardiacivil.es/bib/23048

8. REGULATION

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II). Official Journal of the European Union 205 of 7 August 2007. https://eur-lex.europa.eu/eli/dec/2007/533/oj

2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States Official Journal of the European Union 190 of 18 July 2002. https://eur-lex.europa.eu/eli/dec_framw/2002/584/oj

Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals. Official Journal of the European Union 348 of 24 December 2008. https://eur-lex.europa.eu/eli/dir/2008/115/oj

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. http://data.europa.eu/eli/dir/2016/680/oj

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II). Official Journal of the European Union 381 of 28 December 2006. https://eur-lex.europa.eu/eli/reg/2006/1987/oj

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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). http://data.europa.eu/eli/reg/2016/679/oj

Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals. Official Journal of the European Union 312 of 7 December 2018. https://eur-lex.europa.eu/eli/reg/2018/1860/oj

Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006. Official Journal of the European Union 312 of 7 December 2018. https://eur-lex.europa.eu/eli/reg/2018/1861/oj

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU. Official Journal of the European Union 312 of 7 December 2018. https://eur-lex.europa.eu/eli/reg/2018/1862/oj