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

Collaboration

LAW ENFORCEMENT COOPERATION AND CRIMINAL PROSECUTION: PARALLEL CONSTRUCTION?

English translation with AI assistance (DeepL)

Adriano J. Alfonso Rodríguez
Doctor of Law
Professor of Law-Criminology UNED-Lugo. Judge(s)
ajalfonsorodriguez@hotmail.com
ORCID: 0009-0005-2821-4603

Received 14/05/2025
Accepted 14/05/2025
Published 27/06/2025

Recommended citation: Alfonso, A. J. (2025). Cooperation between law enforcement agencies and criminal prosecution: Parallel Construction? *Revista Logos Guardia Civil*, 3(2), p.p. 13-34.

Legal Deposit: M-3619-2023
NIPO online: 126-23-019-8
ISSN online: 2952-394X

ORCID: 0009-0005-2821-4603

LAW ENFORCEMENT COOPERATION AND CRIMINAL PROSECUTION: PARALLEL CONSTRUCTION?

Abstract: The existence of two types of security, national and public, has served to empower different bodies to prevent it. The secret services have acquired a prominent role in national security, while public security implies the presence of police bodies. In both cases, surveillance and protection work requires the authorised infringement of fundamental rights. However, the same standard does not exist when the secret services are involved, which is lowered because they are not investigating a criminal act and the problematic communication of the information obtained, when it appears, to the police forces. Is a strategy of concealing the source necessary? In short, is a parallel construction necessary?

Resumen: La existencia de dos tipos de seguridad, la nacional y la pública, ha servido para apoderar a organismos diferentes sobre su prevención. Los servicios secretos han adquirido un protagonismo destacado en lo que respecta a la nacional, mientras que la pública implica la presencia de órganos policiales. Para el trabajo de vigilancia y protección es necesario en ambos casos vulnerar, autorizadamente, los derechos fundamentales. Sin embargo, no existe el mismo estándar cuando participan los servicios secretos que se ve rebajado por no estar investigando un hecho delictivo y la problemática comunicación de la información obtenida, cuando aquel aparece, a las fuerzas policiales ¿Es necesaria una estrategia de ocultación de la fuente? ¿Es precisa, en definitiva, una construcción paralela?

Keywords: Public security, National security, Police, Intelligence service, Procedural safeguards.

Palabras clave: Seguridad pública, Seguridad nacional, Policía, Servicio de inteligencia, Garantías procesales.

ABBREVIATIONS

Art.: Article.

EC: Spanish Constitution.

PC: Penal Code.

CESID: Centro Superior de Información de la Defensa.

CIA: Central Intelligence Agency.

CITCO: Intelligence Centre for Terrorism and Organised Crime.

CNI: National Intelligence Centre.

DEA: Drug Enforcement Agency.

DIA: Defence Intelligence Agency.

MS: Explanatory Memorandum.

FBI: Federal Bureau of Investigation.

FJ: Legal Basis.

LOPJ: Organic Law of the Judiciary.

LOPSC: Organic Law for the Protection and Security of the Citizen.

LSN: National Security Law.

NSA: National Security Agency

SAN: Audiencia Nacional ruling.

SECED: Central Documentation Service.

SED: Secretary of State Director.

SIAM: Senior Staff Information Service.

STC: Ruling of the Constitutional Court.

STS: Supreme Court Judgment.

SC: Supreme Court

1. PREFACE.

Since the attacks on the Twin Towers in New York on 11 September 2001 - with their painful aftershocks on 11 March 2006 in Madrid - we have been facing a convulsive world, where democratic systems are faced with various open fronts, ranging from armed conflicts to transnational organised crime, against the backdrop of persistent terrorist risks, or espionage carried out by hostile countries. Also, less conventionally, we must be alert to cyber-attacks or disinformation campaigns, respond to irregular migration flows, climate catastrophes and global pandemics, or economic insecurity. These facts reflect a world far removed from perpetual peace and expressive of a "Risk Society" which implies confronting a situation of unrest, not provoked by threats but by the individuals who make them manifest (Beck, 2006, p. 107).

Facing the challenges that arise, all of which are very varied, with different roots and complex solutions, places us in the sphere of the so-called protection of "National Security", a concept that has been explained from different perspectives. However, in our country, the regulation of this concept is very recent, barely ten years old, and seeks to provide a regulatory framework for a space which, traditionally, has been in the shadows because it was considered that state action in certain areas should be kept strictly secret, in clear contrast to the idea of "Public Security", whose legislative presence is much earlier, obligatory in democracy, and based on the idea that governing implies a power of containment of police power (Zaffaroni, 2006, p. 165).

In any case, our constitutional text (hereinafter EC) has not addressed the idea of "National Security", nor does it contemplate a definition as such, although it does allude to the concept of "Public Security" in various precepts of our lex superior by establishing the guarantee of "citizen security" by the police forces (art. 104.1 EC) or exclusive state ownership of "public security" (art. 149.1.29 EC).1 CE) or the exclusive state ownership of "public security" (art. 149.1.29ª CE), without forgetting art. 126 CE where it speaks of a "Judicial Police" in a situation of dependence on Judges and Prosecutors in the investigation of crime and the discovery of the offender (*Cfr.* SSTC 175/1999, of 30 September, FJ 7º 86/2014, of 29 May, FJ 4º or 55/1990, of 28 March, FJ 5º). This situation, lacking recognition, has not prevented the idea of "National Security" from emerging as a singular tool for protection, as a policy of its own, although without a ministry to manage it (Herbon Costas, 2021, p. 164). However, this does not prevent us from observing that both "securities" operate in the same spheres, touch on similar aspects and set identical objectives, and although fundamental rights can be violated on both levels, they operate under different criteria, more flexible in their ethical dimension when it comes to matters of national security, and which leave in the air the existence of a bridge to be crossed in cases of collaboration between the different operational bodies responsible for overseeing their fulfilment.

From a regulatory perspective, Article 3 of Law 36/2015 of 28 September on National Security (hereinafter LSN) states that "For the purposes of this law, National Security shall be understood as the action of the State *aimed at protecting the freedom, rights and well-being of citizens, guaranteeing the defence of Spain and its constitutional principles and values*, as well as contributing together with our partners and allies to international security in the fulfilment of the commitments undertaken". In line with this definition, the idea of "Public Security" in the Explanatory Memorandum (EM) of Organic Law 4/2015, of 30 March, on the Protection of Public Security (LOPSC) states

that "The Law, in accordance with constitutional jurisprudence, is based on a material concept of public security understood as an activity *aimed at protecting people and property and maintaining the peace of mind of citizens*, which encompasses a plural and diversified set of actions, different in nature and content, aimed at the same purpose of protecting the legal good thus defined. Within this set of actions are the specific actions of the instrumental organisations destined for this purpose, especially those corresponding to the Security Forces and Corps, to which Article 104 of the Constitution *entrusts the protection of the free exercise of rights and freedoms and the guarantee of public safety...*".

It is easily perceptible, as has been highlighted, the common idea of protection of freedoms and rights that places both concepts in a clear thread of connection, which we can even observe in case law. In this sense, STC 184/2016, of 3 November, the first ruling that has addressed the concept of "National Security", states "*On the other hand, since the State competence is clear, both in matters of defence and public security, it would not make sense that, in an area such as national security, so closely linked to both, to the point of identifying its aims and objectives and the legal assets protected in the manner indicated, the State's competence would become purely residual. In short, national security is not a new competence, **but is integrated** into the state competences of defence and public security*" (FJ 3º). This judgement, which does no more than link the two concepts, does not prevent us from establishing clear differences.

Firstly, the defence of national security against threats, by obtaining information, is a matter for the secret services, specifically, and in our country, the National Intelligence Centre (CNI). In the case of public security, or citizen security, its protection is entrusted to the police services, be they central, regional or local government. Secondly, the secret services, in the surveillance of those activities that could affect national security (espionage, counter-espionage, anti-terrorist work, etc.), operate under a clear criterion of security.), operate under a clear criterion of extreme operational discretion, so that their work remains under the umbrella of classified information, which is not known to the public, and the results of their work are rarely brought before a court, situations that do not affect the work of the security forces, who carry out their activities under the supervision of judicial bodies, with results that are public and publicised, the ultimate aim being to lead, as a rule, to the determination, or not, of criminal liability to be judicially elucidated. Fourthly, the organised violation of fundamental rights requires, both in police work and in the work of the CNI, judicial authorisation, however, while the criminal procedural framework derived from the Criminal Procedure Act (LECRIM) acts as a flange for public security agencies, the secret services operate in a necessarily broader framework where the normative regulation is rather limited, through the only article contained in Law 2/2002, of 6 May, with judicial supervision limited to the authorisation of measures affecting the secrecy of communications and house searches that partially affect art. 18 EC, its purpose being the collection of information whose destination is not, in principle, a trial. However, several questions arise: What is our model of judicial supervision of intelligence activities like? Is it possible for secret services to share information with police agencies? Would it be possible to use it in the framework of criminal investigation and prosecution? Let us look at different aspects suitable for formalising the debate.

2. THE MODEL OF JUDICIAL AUTHORISATION FOR CNI ACTIVITIES.

Traditional intelligence gathering by espionage services has always been based on clandestine techniques and with a necessarily flexible ethical dimension in its development with a rather blurred framework of guarantees for those affected. The greater the threat, the more complex the methods of obtaining information, where evaluation and analysis become precision tools for determining the response, action or decision. In fact, the importance of the secret services in a democracy lies in helping the executive to follow specific lines in defence of national interests, becoming important actors in political decision-making (Pinto Cebrián, 2019, pp. 51 et seq.). They have nothing to do with the investigation of the criminal act, nor of the offender or their procedural prosecution (Sánchez Ferro, 2020, pp. 188-189), without forgetting that it is precisely national security that justifies their functions and enables the violation, albeit ordered, of fundamental rights (Aba Catoira, 2020, p. 228).

In our country, as I anticipated, the CNI, a body of the General State Administration with a unique nature (SAN 2632/2009, 27 May, Sala de lo Contencioso (Rapporteur: Mr Gil Ibáñez, FJ 1º), dependent on the Executive and which *"... is not, nor is* it assimilated to, a body identified with an independent administration, in the sense of that typology of public law entities endowed with the autonomy and functional independence that characterises it: it is an instrumental body of the Government..."*.is not, nor can it be assimilated to a body identified with an independent administration, in the sense that this type of public law entity is endowed with the autonomy and functional independence that characterises it: it is an instrumental body of the Government...*" (STS 1238/2021, of 18 October, Chamber III, (Rapporteur: Mr. Requero Ibáñez) FJ 7º) , which reflects, in its physiognomy, a long evolution in the history of our services. Thus, it became the successor to the High Defence Information Centre (CESID) which, in turn, was created by Royal Decree 1558/1977 of 4 July 1977, a body which brought together the previous information services, the Central Information Service of the Presidency of the Government (CESED) and the Information Service of the High General Staff (SIAM), It has always acted as an intelligence assessment body and, during the different governments, has depended on the Ministry of Defence, except for a period of dependence on the Ministry of the Presidency during the government of Mariano Rajoy Brey. Its initial integration with members of the Armed Forces has ended up evolving with the incorporation of civilian personnel, so that this body can no longer be seen as a mere compiler of military intelligence in the face of a potential military conflict. Its work goes beyond this, as threats are increasingly heterogeneous, with asymmetrical conflicts that develop on invisible battlefields and whose existence and intervention is essential to confront them.

According to article 9 of Law 11/2002 of 6 May 2002, the CNI is headed by a Secretary of State **(**SED**)**, who is the "National Intelligence and Counterintelligence Authority" with the title of "Director", appointed by Royal Decree at the proposal of the Ministry of Defence, and with a five-year mandate that can be successively extended or replaced at any time by the government. Its functions are of "promotion" and "coordination", which can be summarised as "direction" of the body's tasks, appointment of the different management positions, budgetary competence and cooperation "*with the information services of the State Security Forces and Corps*, and the bodies of the civil and military Administration, relevant to intelligence objectives...". He is assisted by a Secretary General, with the rank of Undersecretary, who, among other functions, in

addition to substituting him, is in charge of "Directing the functioning of the common services of the Centre through the corresponding instructions and service orders" (art. 10, Law 11/2002). These are, therefore, the main managers in charge of functions of responsibility in the CNI, with the possible and hypothetical existence of the Foreign Intelligence Division, Counterintelligence Division, Internal Intelligence Division, Economy and Technology Division together with the Sub-Directorate General for Administration and Services and the Sub-Directorate General for Personnel and a Legal Advisory Office, a Technical Office, a Head of Operational Support and a Security Service (arts. 1 and 2 RD 2632/1985). 1 and 2 RD 2632/1985, of 27 December 1985, although later, in RD 266/1996, of 16 February 1996, art. 2 established the existence of intelligence units and operational and technical support units together with a security unit in charge of protection tasks). In any case, it is possible that this internal organisation is very different today.

Among all the issues, there is one that underlies with importance in the face of a history that placed the work of our secret service in the shadows. This is the case of intelligence activities in which searches and wiretapping of targets were carried out, a scenario that was orphaned of any regulation and enormously problematic until Law 2/2002, of 6 May, which in a single precept, with an impact through its transitory law on the Organic Law of the Judiciary 6/1985, of 1 July, (LOPJ), in arts. 125, 127, 135, together with the new art. 125, 127, 135, together with the new art. 342 bis in the same text, decides that a Supreme Court Judge (Second Criminal or Third Administrative Chamber) will be responsible for authorising the CNI to carry out acts affecting the inviolability of the home (art. 18.2 CE) and the interception of communications (art. 18.3 CE). This is an unusual system (Lanz Muniain, 2023, p.27), unparalleled in our neighbouring countries, with the exception, with relative nuances, of the United States, as we shall see, the attribution of jurisdiction to a single judge, and for a temporary period of five years, is not exempt from criticism for departing from the constitutional sense of the ordinary judge predetermined by law (De la Oliva Santos, 2006, p. 154). It is clear that a court of espionage has not been properly created.

The justification for the amendment is provided by the MS of Law 2/2002 which states "For activities that may affect the *inviolability of the home and the secrecy of communications*, the Spanish Constitution requires in its Article 18 judicial authorisation, and Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms requires that this interference be provided for by law and constitute a measure which, in a democratic society, *is necessary for national security, public safety*, the economic well-being of the country, the maintenance of order and the *prevention of crime*, the protection of health or morals, or the *protection of the rights and freedoms of others*". As can be seen, it alludes to the two securities and the aspects that nourish them as an element justifying the violation of Art. 18 EC and against the backdrop of the protection of rights and freedoms, a core element of both.

The authorisation model is extremely peculiar, regulated in the sole article of Law 2/2002, of 6 May, and in synthesis is initiated by the SED, who submits to the SC Magistrate (Chamber II or III), elected by the General Council of the Judiciary (CGPJ) for a period of five years - coinciding with the mandate of the SED - a request for violation of fundamental rights, which must be duly motivated and necessarily contain the

following points: "*(a) Specification of the measures requested. b) The facts on which the request is based, the aims motivating the request and the reasons advising the adoption of the measures requested. c) Identification of the person or persons affected by the measures, if known, and designation of the place where the measures are to be taken. d) Duration of the measures requested, which may not exceed twenty-four hours in the case of the inviolability of the home and three months for the intervention or interception of postal, telegraphic, telephonic or any other type of communications, both periods extendable for successive equal periods in the event of necessity.* Once the petition filed by the SED has been received, the SC Judge has 72 hours (or 24 hours depending on the urgency of the measure) to safeguard its proceedings, which will be secret. The initial judicial decision, possibly an order, and the subsequent ones that extend it, cannot be appealed, nor can they be reviewed, and this is because the only actors in this procedure are the SC Magistrate and the SED, who, on the other hand, "shall order the immediate destruction of the material relating to all information that, obtained by means of the authorisation provided for in this article, is not related to the object or purpose of the authorisation".

It is clear that there are no principles that inspire the request, criteria for granting or refusing it, use or destination of the material obtained, judicial control of the execution of the measures or of the result obtained, with the exception of the extension, the situation of those affected by the immission measure or appeals against the decision issued. In this sense, the justification is, a priori, that the material obtained is neither likely to generate evidence nor will it be used in criminal proceedings (González Cussac, 2015, p.88). However, we cannot rule out, as a first element of nuance, the procedural transcendence of intelligence work, as the use, in the contentious jurisdiction, of CNI reports to deny the nationality of foreign applicants for reasons of "national security" stands out (SSTS 233/2022, 23 February, Chamber III, Speaker: Mr. Menéndez Pérez, FJ 4º; 395/2022, 29 March, of Chamber III, Rapporteur: Mr. Román García FJ 6º; 367/2021, of 17 March, of Chamber III, Rapporteur: Mr. Herrero Pina FJ 2º,; 4376/2015, of 26 October, of Chamber III, Rapporteur: Mr. Del Riego Valledor, FJ 4º; STS 2105/2014, of 26 May, of Chamber III, Rapporteur: Mr Del Riego Valledor, FJ 5º). However, I will return to its use in criminal proceedings later to clarify the issue. In any case, the aim has been to combine relatively antithetical aspects such as supervising something which, by its very nature, could not be supervised, by opening a judicial channel which, on the other hand, does not operationally constrain the agents by keeping them outside the requirements derived from the existence of open criminal proceedings (Alfonso Rodríguez, 2024, p. 132).

The starting point of the request revolves around art. 4 b) of Law 11/2002, of 6 May, which establishes, among others, as the main function of our espionage service that of "*Preventing, detecting and enabling the neutralisation of those activities of foreign services, groups or individuals that put at risk, threaten or threaten the constitutional order, the rights and freedoms of Spanish citizens, the sovereignty, integrity and security of the State, the stability of its institutions, national economic interests and the welfare of the population*". In this sense, this reflects the justifying element of the request for judicial authorisation in the single article, converting the authorising SC judge into the interpreter of non-legal concepts such as "sovereignty" or "integrity", "national economic interests" or the "well-being of the population", which are the ultimate aims of the development of espionage tasks and which, together with respect for rights, freedoms or institutional stability, imply making him the guardian of "national security" that empowers the service to be able to carry out its functions.

The question raised by the judicial empowerment of the CNI to intercept a telephone or enter a home is that it implies a kind of safeguard but distances itself from a function of guaranteeing fundamental rights (Pascual Sarria, 2007, p. 197) which, on the other hand, the Judiciary is attributed by virtue of art. 117.4 EC, and converts the procedure into *a sort of secret file for requesting measures limiting specific fundamental rights, in the framework of intelligence operations for the protection of national security, to a judge of the SC, subject to a temporary mandate and expressly appointed for this purpose* (Alfonso Rodríguez, 2023, p.89).

3. THE AMERICAN MODEL: THE FISA COURT AND A FALLING WALL.

It is not clear whether the United States has been the model for the configuration and physiognomy of our system of control of intelligence activities. However, it is clear that we cannot accept total inspiration, as the procedural system is distant between the two countries, with the adversarial system of North America in which the parties (accuser and accused) are the true "owners" of the American criminal process, and where the principle of the "Due Process of Law", the right to due process with all the guarantees, is shown to be the "motor" of the procedural organisation (Gómez Colomer, 2006, pp. 50-57), in contrast to a model of the Investigating Judge who is blessed by a Trial Judge who is the "owner" of the system (Gómez Colomer, 2006, pp. 50-57), in contrast to the model of the Investigating Judge who is the "owner" of the system. 50-57), in contrast to a model of the examining magistrate that is blessed by a LECRIM of 1882, which is impossible, under any circumstances, in the United States. However, it should be noted that the procedural model of the FISA Court does not respond to this adversarial system.

The US intelligence model is based on a plurality of agencies (CIA, NSA, DIA, FBI in its intelligence branch, Armed Forces and Government Departments with their own services) that are now coordinated by a National Intelligence Director, in accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPA) as the Executive's commissioner for the adequate coordination of all organisations, coexisting with intense control by the legislature through parliamentary oversight committees. Given this circumstance, it is necessary to start from a phase of systematic abuses by the FBI or the CIA, highlighted by the Senate *Church* Committee (Arrieta, 2025, p. 122). 122), led to the enactment in 1978 of the *Foreign Intelligence Surveillance Act* (FISA), part of which was the creation of a Federal Court to control the electronic surveillance of foreign agents in the United States, now made up of eleven Federal Judges with public identities but whose work is carried out in secret, and who are appointed by the *Chief Justice of* the Federal Supreme Court of the United States. It is these judges who are in charge of verifying the requests of the Executive, who must prove as "probable cause" - a sensible suspicion that motivates the request - that the target of the listening or surveillance of the electronic devices is a foreign power or agent of a foreign power that is the target of the intelligence-gathering operation, therefore its use was not, a priori, intended to intercept the communications of US citizens. In the absence of a prima facie case of criminal wrongdoing to obtain the FISA Court's warrant, the standard for authorisation is less stringent than the usual standard required by law enforcement to violate fourth amendment rights - privacy (Ruger, 2007, p. 243).

The application is submitted before a judge of the FISA Court in which the government appears with its representation as the only intervening procedural party, where, in addition to proving probable cause, the identity of those involved and the

officials involved, the duration of the electronic surveillance measures, certificates from the intelligence authorities and details of previous applications, among other elements, must be indicated. The fact that it is the executive branch that acts as the sole participant distances the procedure from the adversarial system typical of the US system (Sobel, 2023, p. 15), estimating that one of the reasons, among others put forward at the time by *Attorney General* Griffin Bell during the drafting of the law, which could motivate the lack of other participants, is due to the reluctance of the government itself to declassify information for fear of leaks (Chin, 2021, p.665).

In view of the data provided, the FISA Judge will grant, or deny in detail, the *warrant* for electronic surveillance requested by the Government, identifying the subjects, means, type of information to be obtained and the duration of the warrant, and its denial can be reviewed before the *FISA Court Review*, composed of three judges of the same body, with the possibility of appealing to the *U.S. Supreme Court* if the review is unsuccessful.

However, while until 2001 the FISA mandate served the purpose of intelligence gathering, the 9/11 terrorist attacks in the United States, with the *Patriot Act* of 2001, under section 203, mutated the architecture of the law and thereby broke the *wall* between foreign intelligence gathering and criminal investigations (Donohue, 2021, p. 204), allowing the use of information-sharing by law enforcement agencies (FBI or DEA), obtained for the purpose of foreign intelligence gathering in light of FISA, and in criminal investigations, mixing the use of information-sharing by law enforcement agencies (FBI or DEA), obtained for the purpose of foreign intelligence gathering in light of FISA, and in criminal investigations. 204), allowing the use of information-sharing by law enforcement agencies (FBI or DEA), obtained for the purpose of foreign intelligence gathering under FISA, and in criminal investigations, thus mixing an identical method with different purposes, which prompts several reflections.

Firstly, by virtue of the standards of the request, in that the accreditation of probable cause is different, since in a criminal investigation it was necessary to prove, through that concept, the possible commission of a criminal act, which is not something that occurs in the request for a warrant under the FISA regulation. Secondly, with the common goal of preventing a terrorist attack, the cooperation and transmission of intelligence between spy agencies and law enforcement agencies, whose tasks are different, increased, and thus the boundaries between Intelligence Community and police agency blurred and blended (Stein, Mondale, Fisher, 2016, p. 2266). Third, the possibility of building a criminal case, with information obtained under FISA criteria, became a distinct possibility (think of a federal terrorism or narco-terrorism case in which law enforcement has received information from intelligence agencies as a result of the results obtained under a FISA warrant) so that a clear debate arose regarding the due process rights of those affected and their right to defence against the sharing of intelligence materials between agencies (Reid, 2015, p. 429).

4. PARALLEL CONSTRUCTION" AND INTER-AGENCY INTELLIGENCE COMMUNICATION.

As a result of what was previously observed with respect to the fall of the wall, it is evident that "National Security", a concept that is too ambiguous, was embedded in "Public Security", bearing in mind that the procedural requirements for the violation of

fundamental rights, particularly the privacy of communications, were lowered in the face of the claim of intelligence gathering, intelligence that later, as a result of a change in realities, which led to a mutation of principles, was used for different purposes in a way that bordered on procedural customs and fundamental rights in exercises of interchangeability, either for political decision-making or to form a basis for a criminal case. It is in this scenario that the concept of *"parallel construction"* makes sense, which began with the receipt of intelligence information with relaxed standards for obtaining it, the origin of which cannot be revealed and which, as I pointed out earlier, could well jeopardise procedural guarantees by providing an operational shortcut that could circumvent legal objections and which forces the invention of a parallel channel that diverts attention from the original source (e.g. an artificially created informant). e.g., an artificially created informant concealing intelligence information obtained from a different mandate such as a FISA Court warrant).

If we previously analysed the model for obtaining information by the CNI, the main body of our Intelligence Community, the situation faced by a police agency, be it a state agency such as the National Police, the Civil Guard or the Customs Surveillance Service, or the cases of Autonomous Police, expressive of an integral model (STC 184/2016, of 3 November, FJ 4º) such as Catalonia, Navarre and the Basque Country, each of which has information units and which make up a sort of "Police Intelligence Community" where the Intelligence Centre for Terrorism and Organised Crime (CITCO) intervenes as a body for analysis and coordination between bodies. However, it should be pointed out that, when it comes to gathering intelligence, police forces are subject to procedural constraints, in the context of satisfying public security, which are radically different from those of the intelligence services, and where the judicial authority acts as guarantor of fundamental rights. In this sense, the framework of action provided for in the LECRIM conditions the passage of investigators, subjecting their activity to a set of principles and requirements that establish a standard of procedural guarantees inherent to the rule of law.

A criminal investigation may affect various fundamental rights such as personal freedom (art. 17 EC), privacy (art. 18.1 EC), inviolability of the home (art. 18.2 EC), secrecy of communications (art. 18.3 EC) and also freedom of movement (art. 19 EC), with the judicial authority determining under the assumptions of the law the possible adoption of any measure that affects the above, therefore, although there must be a legal authorisation that allows its adoption, this, however, is not sufficient. It is necessary for the infringing measure to be sufficiently motivated in such a way that it expresses the factual and legal argumentation that determines its adoption in accordance with the principles of speciality, suitability, exceptionality, necessity and proportionality. In other words, a criminal offence must be under investigation (speciality) which in any case must be sufficiently serious to justify the adoption of such a measure, which serves the purpose of the investigation (suitability; SSTC 85/1994, 14th March, FJ 3°; 181/1995, 11th December, FJ 5°; 49/1996, 26th March, FJ 3°; 54/1996, 26th March, FJ 7° and 8°; 123/1997, 1st July, FJ 4°) as the results cannot be achieved by means of other measures that are less burdensome with respect to the fundamental rights of the person under investigation, being essential from the perspective of the specific case (exceptionality and necessity) and finally, only serious, socially transcendent facts with strong indications justify the sacrifice of key fundamental rights at the risk of seeing a situation of criminal impunity (proportionality, STC 49/1999, 5th April, FJ 7°).

It is clear that the request limiting fundamental rights that the police unit instigates

to investigate is subject to the aforementioned justifying requirements, in such a way that, faced with a criminal act that is being investigated in progress, there is a "wall" that needs to be overcome by judicial authorisation in order to be able to continue with the investigation. Under no circumstances can a police request be made for prospective purposes (STS 822/2022, 18 October, Chamber II (Rapporteur: Mr. Palomo del Arco) , FJ 1º.3. a)), i.e., without a prior crime that is indiciously justified, it is not even conceivable to carry out a request aimed at obtaining a judicial decision that violates a fundamental right. Therefore, it is clear that the police forces are there to investigate under precise parameters and clear limitations, and although the clandestinity of the investigation is precise, its final destination is to emerge in a public trial with full respect for the right of defence and with the clear objective of satisfying the demands of "public security" (STC 175/1999 of 30 September, FJ 7º or STC 86/2014, of 29 May FJ 4º), something that contrasts with the task of the secret services where, in the interests of protecting "national security", information is gathered from natural or legal persons, national or foreign, information which is classified and which is certainly not intended to be publicly aired before a prosecuting body to deduce criminal liability and without ideas such as "contradiction", "defence", "suspect" or "defendant" having any substance of their own, given that their work has nothing to do with criminal investigation.

However, despite the above, the fields of action of police forces and secret services are common. Organised crime, terrorism, illegal immigration...are a simultaneous threat to "public security" and "national security" in such a way that:

Organised crime is a security threat characterised by its essentially economic purpose, its undermining effect on political and social institutions, its transnational nature and its opacity. Criminal groups and criminal organisations disguise their illegal operations as legitimate business and increasingly rely on digital technologies, such as crypto-currencies and the dark web. In addition to its economic dimension, organised crime has a relevant destabilising potential. Its structures adapt to the geostrategic environment and have an impact on governance, social peace and the normal functioning of institutions. In terms of serious crime, activities such as the exploitation of children or trafficking for sexual exploitation target vulnerable groups and seriously violate human rights. Smuggling, cybercrime, trafficking in drugs, arms and wildlife, and corruption are tangible threats to national security. The convergence between terrorist groups and organised crime networks is increasing. The increasingly decentralised organisational patterns of these criminal actors favour their cooperation and facilitate terrorist financing (National Security Strategy (2021), pp. 64-65).

It goes without saying that, in view of the above, it is necessary for our secret service and the police forces to collaborate in an activity that could materially coincide in terms of facts and subjects, hence its clearly concentric nature when it comes to, among other issues, terrorism, organised crime or both. At this point, a clear doubt arises: what happens when the CNI, as a result of its eavesdropping, becomes aware of a criminal act that could be investigated due to its imminence?

It is clear that there is no legally regulated system of communicating vessels to formalise the transmission of information when the CNI becomes aware of the commission of criminal acts (Sánchez Barrilao, 2011, p. 61), as there are hardly any references in Law 11/2002, of 6 May, regarding cooperation with the Security Forces, except for specific aspects such as art. 9.2 d), which attributes to the SED the maintenance

and development of "collaboration with the information services of the State Security Forces and Corps, and the bodies of the civil and military administration, relevant to intelligence objectives". It is here where what we previously pointed out as *"parallel construction"* comes into play as an expression of the configuration of a criminal case by a police force concealing the origin of the source that drives it (Reid, 2015, p. 427) and which could necessarily be connected to information obtained by an intelligence agency, having to construct parallel circumstantial evidence elements intended to be the cloak that hides the genesis of the original information, which forces us to see how we should treat intelligence material as the initiator or driver of a criminal police investigation.

In principle, it is necessary to start from what is stated in STS 746/2022, of 21 July, Chamber II, (Rapporteur: Ms. Polo García) which points out:

"As we have said in the judgment cited by the Chamber - 312/2021, of 13 April - there is no right for the accused to disclose the content and scope of international police collaborations. *The investigated persons subject to criminal proceedings do not have a right to disclose the points of police postings, or the identity of the informants, or the information gathered through criminalistic techniques that would lose their effectiveness if they were massively disclosed. There is no right to know the specific tools and materials that were available to the police for the investigation and which could be rendered ineffective for future interventions.* Nor is there a right to know about the investigations into other crimes that could be attributed to the same suspects but which are still in the process of police confirmation, even less so if we consider that, where appropriate, they should be the subject of a separate criminal prosecution procedure (art. 17.1 LECRIM). It is also unacceptable that investigations which do not even affect those being prosecuted and which could ruin other police actions of obligatory prosecution of criminality should be known". (FJ 3.3).

The origin of the previous ruling was due to the refusal of the judicial body in charge of the prosecution to accept the testimony of American DEA agents who provided information to the National Police who carried out a drug investigation that culminated in a conviction. It should be noted that the previous ruling was not new; our High Court had already made it clear quite previously that "...when foreign intelligence services provide data to the Spanish security forces and bodies, *the requirement that the source of knowledge also needs its own sources of knowledge does not form part of the content of the right to a trial with all the guarantees...*" (STS 445/2014, of 29 May, Chamber II, Rapporteur: Ms. Ferrer García FJ 2º ; STS 884/2012, of 12 November, of Chamber II, Speaker: Mr Marchena Gómez FJ 8). Therefore, we obtain a first partial solution: foreign intelligence services can provide our police forces with their sources without any problem in order to start investigating. Their origin, in short, is not relevant and therefore the DEA (or the FBI, or any other foreign police force) could receive information from its own intelligence agency (CIA, NSA... or its intelligence service) and transmit it to police agencies to initiate a criminal case in our country, without entering into the debate on the relaxation of the legal standards for obtaining it, since there is no right to debate the sources of the information, given that it is not required to know them in order to set up due process.

The question of the transmission to the security forces by the CNI of information it

has been able to obtain as a result of its wiretapping or house searches requires further clarification and is in fact a matter addressed in case law denying that its functions have anything to do with criminal investigation (SSTS 1140/2010, of 29 December, of Chamber II (Rapporteur: Mr Berdugo Gómez de la Torre); 1094/2010, of 10 December, of Chamber II (Rapporteur: Mr Marchena Gómez)). And on this point, once again, the different procedural methodology required for a telephone interception, for example, depending on whether it is requested by the CNI or by a police agency, is that they only have in common the need for judicial authorisation, nothing more.

There is no shortage of arguments in favour of the fact that information obtained by the CNI in violation of a fundamental right, and under its own procedural - not procedural - conditions, with judicial authorisation, can serve as a source for initiating a criminal case with the possible communication to the police forces.

Firstly, there is *a principle of unity of action between police and intelligence agencies*, which is imposed by the National Security Strategies that are dictated as a framework for action (art. 4.3 LSN). Thus:

In traditional areas of security, adapting to the changing nature of threats - armed conflict, terrorism, organised crime, proliferation, irregular migration flows, intelligence activities - is a constant feature of the *actions of the various actors of national security.* As these phenomena become increasingly transnational, *the need for concerted action* at all levels *intensifies*. The close links that often exist between several of these threats make it necessary to address them from broad strategic and operational frameworks, under *the premise of the principle of unity of action.* This Report shows that this approach is already fully valid in Spain's response to classic security challenges (Estrategia de Seguridad Nacional, 2013, p. 145).

It is difficult, at the risk of endangering the community, to admit work configured in watertight compartments, and thus the LSN imposes this "unity of action" (art. 4.2), recalling in art. 9.2 that "The *State Intelligence and Information Services*, in accordance with the scope of their competences, will permanently support the National Security System, providing elements of judgement, information, analysis, studies and proposals necessary to prevent and detect risks and threats *and contribute to their neutralisation*". Therefore, the requirement of a convergent sense necessarily takes the form of cooperation between agencies ("Services") in order to meet the requirements aimed at averting risks ("contributing to their neutralisation"). In short, the communication of information is a key element in helping to neutralise the risks that arise.

Secondly, a justification for the communication could be given by *the obligation to report the criminal acts or their imminent commission* by anyone who witnesses them in accordance with art. 262 LECRIM (De la Oliva Santos 2006, p. 164), starting with the SC Magistrate who authorised the interception of communications or the entry into the CNI's home (López Alafranca, 2014, p. 135). 164) starting with the SC Magistrate who authorised the interception of communications or the entry into the CNI's home (López Alafranca, 2014, p. 135) and also by virtue of the requirement of criminal liability (407 and 408 CP) when we are talking about police officers who may provide services to the CNI. The judge's knowledge of the development of the authorised measure must necessarily derive from the need to extend the measures limiting fundamental rights that the CNI may be interested in, as there is no possibility of the authorising body not

knowing the facts, unless a "blind" authorisation is admitted as a "blank cheque" and without successive control, which is not possible as the law provides for such an extension "in case of necessity" (art. 2 d) Law 2/2002), a necessity that would have to be justified, with the facts resulting from the initially agreed measure, in order to continue with the restrictive measures.

The thesis cannot be accepted, without prejudice to its validity, that the lack of consideration of CNI agents as authorities (art. 5.4 Law 11/2002) prevents the obligation to report crimes (Lanz Muniain, 2023, p. 34), however, the obligation imposed by art. 262 LECRIM on those who "by reason of their positions, professions or trades" have knowledge of the criminal act determines that it makes no difference whether or not they are an authority or its agent, as they know of the act through their profession and must report it. However, this communication has been endorsed by the SC itself when it states that "Therefore, the legal function of this Service is not the investigation of specific crimes, without prejudice to the fact that if in the course of their work *they discover* or have indications of criminal actions *they inform the competent police and judicial bodies*, but - it is insisted - their activity is not directly aimed at the discovery of crimes, nor is it conditioned by the prior commission of any" (STS 1140/2010, of 29 December, of Chamber II (Rapporteur: Mr. Berdugo Gómez Gómez). Berdugo Gómez de la Torre) FJ 9º) .

Thirdly, *a hypothetical secret classification cannot cover the impunity of criminal acts* (López Alafranca, 2014, p. 136), which, on the other hand, must necessarily be prevented. Likewise, even in the case of classified information ("internal organisation and structure, means and procedures, personnel, facilities, databases and data centres, sources of information and information or data that may lead to knowledge of the aforementioned matters..." ex art. 5.1 Law 11/2002), nothing hinders a procedure of declassification of information at a procedural level, but this is an issue unrelated to the communication itself which, precisely, has as a limit that information transmitted in which material that must be declassified is not disclosed (Pascual Sarria, 2007 p. 214).

Fourthly, it is precisely the collection of information by the CNI if it implies a violation of the privacy of communications or an entry into the home *that is backed by a judicial decision necessarily motivated by its harmful effect* (SSTC 126/1995, 25 July, FJ 2; 139/1999, 22 July, FJ 2; in the same sense, SSTC 290/1994, 27 October, FJ 31; 50/1995, 23 February, FJ 5; 41/1998, 23 February, FJ 34; 171/1999, 23 September, FJ 10; 8/2000, 8 January, FJ 4); 41/1998, of 24 February, FJ 34; 171/1999, of 27 September, FJ 10; 8/2000, of 17 January, FJ 4), therefore such measures have not been agreed outside a procedural scheme or on a whim in accordance with their operational needs, so that there is no illegality in their obtaining and therefore, neither in their communication for the initiation of a criminal investigation, an investigation that is not contaminated.

In this respect, the evidentiary aspect must be distinguished from the actual issue of communication for the initiation of criminal proceedings. They are different issues. The material obtained by the CNI is not intended to be evidence in criminal proceedings, and this is because it is the police investigation itself which is intended to fulfil this function, recalling that "unlawful evidence" (art. 11 LOPJ) only exists "when the means used to obtain it are constitutionally illegitimate" (STC 49/1999, 5 April, FJ 12). In this sense, STS 1094/2010, of 10 December, in its FJ 2 A reminds us that ".... But what is beyond doubt *is that the existence of a subsequent criminal proceeding in which the notitia*

criminis is not alien to the security file processed by the CNI does not imply the transmutation of the functionality of that file, which would cease to be what it is, distancing itself from its regulatory principles, to become a procedural act sine qua non of the real process and, therefore, subject to the general rules governing the principle of publicity".

And it is precisely the authorising judicial decision that prevents us from speaking of a sort of illegal "ledge" along which our intelligence service would riskily travel. However, although we have said that intelligence material is not destined for criminal proceedings as an element of evidence, it should not be forgotten that "And with regard to the incorporation into proceedings of evidence obtained by the intelligence services and which refers to declassified material, it can be assessed from two different perspectives. Either it acts in criminal proceedings as documentary evidence, when it is evidence of these characteristics, or it serves to conduct the criminal investigation through the witness statement of the perpetrators" (STS 1140/2010, of 29 December, Chamber II (Rapporteur: Mr. Berdugo Gómez de la Torre) FJ 9º).

However, there is no lack of objections to the system, starting with the complexities that the presence of secret services in criminal proceedings could entail (Hassemer, 2000, p. 114), so that there could be a confusion, almost a mixture, that would make police and intelligence gathering functions indistinguishable (Orgis, 2011, p. 162). It would not be good for the police forces, it would not be good for the secret services, and this by virtue of the different parameters of action. On the other hand, obtaining a wiretap or house entry by our secret services is subject to a different standard where one has to justify one's own extremes of danger to national security that may have nothing to do with the commission of a criminal act. In short, it is one thing if in the course of an intelligence operation a serious criminal act is discovered, or one whose commission is imminent, something that must necessarily be communicated or reported to the police forces, and quite another if the procedure of requesting and obtaining a wiretap or house entry by the secret services serves, as a procedural shortcut, to search for the crime itself, which would lead to the irrelevance of the system of constitutional procedural guarantees with regard to the limitation and violation of fundamental rights.

Finally, we noted earlier that not all information can be known, which could lead, in the context of criminal proceedings, to the right of defence being put to the test (art. 24.2 EC), as access to the file in the case of the CNI is subject to restrictions and a situation of classification that contrasts with the availability to the parties involved of all the elements of the criminal investigation. In other words, the presence of the secret services and the information obtained by them in the framework of criminal proceedings cannot emerge as naturally as in a police investigation. In short, not everyone can have access to all the information, with the result that there are elements that are not subject to a hypothetical defence strategy, either of a defendant or of third parties outside the proceedings whose communications or addresses could be affected, that will remain hidden, which may serve to question the purity of the proceedings and of the decision on criminal liability.

5. CONCLUSIONS.

There is a concentric relationship between national security and public security insofar as both work on the assumption of the existence of threats to the rule of law. However, the actors empowered to protect them are different, with the secret services having jurisdiction over the former and the police over the latter. In this sense, tools have been put in place to avert the aforementioned risks through the attribution of measures limiting fundamental rights. In the case of public security agencies (state, regional or local police), their powers are framed within the scope of criminal procedure with very rigorous guidelines for the violation of rights through the need for judicial authorisation to authorise invasive but orderly activities by the security forces within the framework of the LECRIM. The intelligence service (CNI) has only relatively recently been empowered to intercept communications and enter homes by means of a law of judicial control in 2002, but we cannot affirm that its requirements coincide with those of the LECRIM when it comes to granting them, so that we find ourselves with a system of double standards depending on the subject acting.

The concept of *parallel construction* results from a way of acting with respect to police forces who receive intelligence information which, on the one hand, allows them to build criminal cases but, on the other, bearing in mind that there is a lower standard for obtaining intelligence information, they are obliged to conceal its origin, seeking alternative procedures to prevent the original source from surfacing and allowing the investigated person to question its acquisition by violating due process. This issue has come to the fore primarily in North America as a result of the breakdown of the "wall" between police and intelligence activities with the attacks of 11 September 2001, which has led to doubts about the use of information obtained from the Foreign Intelligence Surveillance Court (FISA Court) whose surveillance warrants to an intelligence agency provide information that can then be used by police forces who have been able to avoid having to justify probable cause before a judicial body in order to carry out their investigations. That is to say, it seems to be a sort of operational shortcut that generates doubts, doubts that also affect us about the possible use of information resulting from an authorisation from the SC Judge to the CNI outside a wiretap, outside an entry into a home. In this sense, there are a series of requirements that would motivate the communication of a criminal act resulting from the practice of a procedure restricting fundamental rights by our secret service to police agencies, which could well be the general obligation to report under art. 262 LECRIM. But an elementary unity of action in the prevention of threats that jointly affect public and national security requires cooperation between services and the sharing of information. Think of the imminence of a terrorist attack that comes to light by chance through a secret service wiretap. No one doubts the need for communication and alert, regardless of the possible secret classification of the information, a classification that cannot cover silence in the face of a criminal act or allow it to go unpunished. There is also a declassification process for this purpose.

Our SC has said that when a foreign intelligence service sends a confidence that serves to open a criminal case, there is no right to know the source of the source, therefore, it is not necessary, nor appropriate, to conceal the origin or source of knowledge by the police agency. In the case of communication by the CNI to a public security force, our High Court also endorses, albeit in isolation, the communication of a criminal act without going into the question of whether or not the information is classified as secret, which

means that neither concealment nor the development of alternative strategies, which could compromise the criminal proceedings, seems to make sense. Therefore, there is no room for *parallel construction*, without prejudice to the fact that the presence of secret services in criminal proceedings raises questions which, if they are to be resolved, will require a reform of the system designed by Law 2/2002 of 6 May.

6. BIBLIOGRAPHICAL REFERENCES.

Aba Catoira, A. (2020). Accountability and intelligence services. In J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 209-237). Tirant lo Blanch.

Alfonso Rodríguez, A. J. (2023). Democratic governance and accountability: Judicial control of intelligence activities (SDG 16.6). *Revista de Derecho UNED*, (31).

Alfonso Rodríguez, A. J. (2024). Interception of telephone communications, security(s) and procedural guarantees. *Revista Ciencia Policial*, (182).

Arrieta, G. (2025). Balancing the scales: Amici curiae as special masters in the shadow of FISA. *California Western Law Review, 61*(1), Article 6. https://scholarlycommons.law.cwsl.edu/cwlr/vol61/iss1/6

Beck, U. (2006). *La sociedad del riesgo: Hacia una nueva modernidad*. Paidós Ibérica.

Chin, S. (2021). Introducing independence to the Foreign Intelligence Surveillance Court. *The Yale Law Journal, 131*(2). http://www.yalelawjournal.org/author/simon-chin

De la Oliva Santos, A. (2006). *Writings on law, justice and freedom*. Editorial UNAM, Instituto de Investigaciones Jurídicas.

Donohue, L. K. (2021). The evolution and jurisprudence of the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review. *Harvard National Security Journal, 12*.

Gómez Colomer, J. L. (2006). Adversarial system, accusatory process and accusatory principle: A reflection on the criminal prosecution model applied in the United States of America. *Revista Poder Judicial*, (Special XIX).

Hassemer, W. (2000), Criminal proceedings without data protection? In C. M. Romeo Casabona (Ed.), *La insostenible situación del derecho penal (*pp. 103-128). Comares.

Herbón Costas, J. J. (2021). La gestión de las crisis en el marco de la Ley de Seguridad Nacional: La pandemia por covid-19 y la necesidad de una urgente reforma. *Revista Española de Derecho Constitucional, 121*. https://doi.org/10.18042/cepc/redc.121.05

Lanz Muniain, V. (2023). El CNI un servicio de inteligencia y seguridad: Panorama normativo. *Revista Española de Derecho Militar, (*119).

López Alafranca, M. (2014). But who will watch the watchmen? *Revista Cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales,* (92).

Orgis, M. (2011). Intelligence-led and intelligence-guided operations: The best option for combating pre-eminent threats. In J. Fernández Rodríguez, D. Sanso-Rubert

Pascual, J. Pulido Grajera, and R. Monsalve (Eds.), *Intelligence issues in contemporary society (*pp. 143-166). Ministry of Defence.

Pascual Sarria, F. (2007). El control judicial a la interceptación de las comunicaciones: Especial referencia al control judicial previo a las intervenciones del Centro Nacional de Inteligencia. *Revista Española de Derecho Militar, (*89).

Pinto Cebrián, F. (2019). *Manual of intelligence and counterintelligence (terrorism and counterterrorism)*. Amabar.

Reid, L. (2015). NSA and DEA intelligence sharing: Why it is legal and why Reuters and the Good Wife got it wrong. *SMU Law Review, 68*(2), Article 5.

Ruger, T. W. (2007). Chief Justice Rehnquist's appointments to the FISA Court: An empirical perspective. *Northwestern University Law Review, 101*(1).

Sánchez Barrilao, J. F. (2011). Prevention and intelligence: National Intelligence Centre and the intelligence community in the face of terrorism, organised crime and illegal immigration. *Revista Ejército,* (846).

Sánchez Ferro, S. (2020). Mission impossible? An attempt at a legal understanding of the world of espionage in Spain. In J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 159-207). Tirant lo Blanch.

Sobel, A. X. (2023). Procedural protections in a secret court: FISA amici and expanding appellate review of FISA decisions. *University of Pennsylvania Law Review, 172.* [Note: Corrected "Pennsylvania" to "Pennsylvania". Missing page numbers or article number].

Stein, R., Mondale, W., & Fisher, C. (2016). No longer a neutral magistrate: The Foreign Intelligence Surveillance Court in the wake of the war on terror. *Minnesota Law Review, 100.* https://scholarship.law.umn.edu/faculty_articles/564

Zaffaroni, E. R. (2006). *El enemigo en el Derecho Penal*. Dykinson.

ORCID: 0009-0005-2821-4603