Carlos Manuel Fernández González
Data Protection Delegate of Secretary
of State for Security
PhD student at the Catholic University of Murcia
Official Master of Criminology
and Security Sciences

SECURITY OF INFORMATION OF PROTECTED WITNESSES AND VICTIMS OF CRIME AS A PROTECTION MEASURE

SECURITY OF INFORMATION OF PROTECTED WITNESSES AND VICTIMS OF CRIME AS A PROTECTION MEASURE.

Abstract: People who become victims or witnesses of crimes, especially those requiring elevated levels of protection in criminal proceedings—such as those granted the status of protected witnesses, victims of gender-based violence, or minors—are subjects of rights to whom such circumstances should not result in additional harm. During legal proceedings, corresponding to their condition and the level of risk attributed to them, they must be effectively protected. Among the guarantees of their fundamental rights, in the fully digitalized world in which we live, the safeguarding of their personal data and information affecting them is of particular importance. This measure constitutes a basic element necessary to guarantee the rest of the measures that need to be adopted, considering that the extensive use of Information and Communication Technologies (ICTs), the everyday use of cyberspace, computer tools, and Artificial Intelligence (AI) is widespread globally. This results in increased difficulty in achieving optimal security levels. Insufficient knowledge, lack of awareness, and difficulty in effectively applying legislation increase the chances of identification, tracking, and locating individuals, thereby significantly raising the difficulty in protecting them.

Resumen: Las personas que resultan víctimas o testigos de delitos, especialmente aquellas a las que es necesario elevar sus niveles de protección en los procesos penales como serían a las que se les otorga la condición de testigos protegidos, las víctimas de delitos de violencia de género o las menores de edad, son sujetos de derecho a los que dichas circunstancias no les deberían derivar perjuicios añadidos. En el curso de las actuaciones, en correspondencia con su condición particular y con el nivel de riesgo que se les atribuya, se les debe proteger eficazmente. Entre las garantías de sus derechos fundamentales, en el mundo totalmente digitalizado en el que vivimos, cobra especial importancia el aseguramiento de sus datos personales y la información que les afecte. Esta medida constituye un elemento básico para poder garantizar el resto de las que se deben adoptar, teniendo en cuenta que la extensión de las Tecnologías de la Información y Comunicación (TIC's), el empleo cotidiano del ciberespacio, de herramientas informáticas y el uso de Inteligencia Artificial (AI) es masivo en el conjunto de las sociedades a nivel mundial y esto tiene como resultado el incremento de la dificultad a la hora de logran niveles óptimos de seguridad. El insuficiente conocimiento, la falta de concienciación y la dificultad de aplicación efectiva de la legislación, elevan las posibilidades de identificación, seguimiento y localización de las personas, lo que eleva notablemente la dificultad protegerlas.

Keywords: Protected Witnesses, Victims of Gender Violence, Minors, Personal Data Protection. Information Protection.

Palabras clave: Testigos Protegidos, Víctimas de Violencia de Género, Menores de edad, Protección de Datos Personales. Protección de la Información.

ABBREVIATIONS

B.C.: Before Christ.

AI: Artificial Intelligence.

AP: Provincial Court (*Audiencia Provincial*).

App.: Web application.

Art.: Article.

BOE: Official State Gazette (*Boletín Oficial del Estado*).

CCN: National Cryptology Centre (*Centro Criptológico Nacional*).

CE: Spanish Constitution (*Constitución Española*).

ECHR: European Convention on Human Rights.

CGPJ: General Council of the Judiciary (*Consejo General del Poder Judicial*).

CP: Criminal Code (*Código Penal*).

DPO: Data Protection Officer.

DEPO: Directive on the European Protection Order.

EOMF: Organic Statute of the Public Prosecutor's Office (*Estatuto Orgánico del Ministerio Fiscal*).

ENS: National Security Scheme (*Esquema Nacional de Seguridad*).

FCSE: State Law Enforcement Forces and Agencies (*Fuerzas y Cuerpos de Seguridad del Estado*).

FGE: State Prosecutor's Office (*Fiscalía General del Estado*).

LECrim: Criminal Procedure Act (*Ley de Enjuiciamiento Criminal*).

LEVD: Law on the Statute of the Victims of Crime (*Ley del Estatuto de la Víctima del Delito*).

LOFCSE: Organic Law on State Law Enforcement Forces and Agencies (*Ley Orgánica de Fuerzas y Cuerpos de Seguridad*).

LOPDGDD: Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (*Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*).

LOPDP: Organic Law on the Protection of Personal Data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal sanctions (*Ley Orgánica de Protección de Datos Personales*).

LOPIVI: Organic Law for the comprehensive protection of children and adolescents against violence (*Ley Orgánica de Protección Integral a la Infancia y la Adolescencia frente a la Violencia*).

LOPIVG. Organic Law on Comprehensive Protection Measures against Gender Violence (*Ley Orgánica de Medidas de Protección Integral contra la Violencia de Género*).

LOPJ: Organic Law of the Judiciary (*Ley Orgánica del Poder Judicial*).

LOPSC: Organic Law for the Protection of Citizen Security (*Ley Orgánica de Protección de la Seguridad Ciudadana*).

LOPT: Organic Law on Witness Protection (*Ley Orgánica de Protección de Testigos*).

LOTJ: Organic Law of the Jury Court (*Ley Orgánica del Tribunal del Jurado*).

LRMRP: Law on Mutual Recognition of Criminal Judgements in the European Union (*Ley de Reconocimiento Mutuo de Resoluciones Penales en la Unión Europea*).

LSO: Official Secrets Act (*Ley de Secretos Oficiales*).

MF: Public Prosecutor's Office (*Ministerio Fiscal*).

RDL: Royal Legislative Decree (*Real Decreto Legislativo*).

RDLJTICS: Royal Decree-Law approving urgent measures for the implementation of the Recovery, Transformation and Resilience Plan in the areas of public justice services, civil service, local government and patronage.

GDPR: General Data Protection Regulation.

STC: Judgement of the Constitutional Court (*Sentencia del Tribunal Constitucional*).

STS: Judgement of the Supreme Court (*Sentencia del Tribunal Supremo*).

ECHR: European Court of Human Rights.

ICTs: Information and Communication Technologies.

CJEU: Court of Justice of the European Union.

TS: Supreme Court (*Tribunal Supremo*).

EU: European Union

1. INTRODUCTION

The use of media and information technologies has built a hyper-connected society through a cybernetic environment. This makes it much easier to obtain information, communicate and locate people by means of an almost unlimited number of identifiers. This habitat, where the decline of privacy is the keynote in the whole spectrum of social relations, among other consequences, increases the difficulty of protecting certain legal assets such as privacy, image, honour or personal data, which are inherent to the security of citizens.

In the case of victims of crime and of witnesses in criminal proceedings, we have made a detailed analysis of the regulations, case law and international treaties and conventions signed and endorsed by Spain. This reveals that, in our country, the set of specific legal instruments that provide protection for personal information, especially in proceedings involving unlawful conduct related to terrorism, organised crime, whether transnational or foreign, crimes of gender-based violence, violence against women or minors, is meagre in comparison with that regulated in countries sharing our social, political and cultural background.

The legal tools for providing security for these people are not yet sufficiently developed. In fact, although some protection measures have been put in place, mainly through the work and efforts of the courts, prosecutors and the FCSE, it can be said that the system is not sufficiently mature. It is possible that the current regulation may meet its goals in some cases, but in practice, the reality is that such measures are not as efficient as desired. Concerning the vulnerability of these people, in 2012 some judges on the National Court criticised the LOPT by pointing out that *"The law has only four articles: it does not provide for anything – neither work nor money nor relocation," says Judge Gómez Bermúdez."* (Irujo, 2012)

In light of the increasing potential for interference by persons involved in all kinds of criminal acts, with the aim of attacking, intimidating or discrediting victims or witnesses, authorities responsible for guaranteeing fundamental rights and public security should not tolerate such a situation. Our democratic system recognises the rights and obligations of parties involved in criminal proceedings (as it should), and these rights and obligations must be made effective, and not simply consist of expressions of intent due to a lack of regulation or resources.

It should be emphasised that constitutional guarantees and essential principles in these proceedings should not be unjustifiably affected by victim or witness protection measures, even though these may be necessary. To this end, it is crucial that any such measures be backed by strict compliance with the law and a solid rationale that, weighing the rights at stake, prioritises the interests of all those involved in the justice system and allows them to achieve their ultimate goals.

This work aims to highlight the importance of guaranteeing the fundamental right to the protection of personal data and information security in order to achieve the comprehensive security of individuals (Ayllón, 2021). One cannot plan to defend a legal asset unless, once harmful agents have been identified and risks analysed, an organised and functional procedure is implemented. This is necessary to prevent the dangers from the outset of the potential threat and, if such threat cannot be avoided, to detect it and

provide an adequate response. If the perpetrator can easily identify, locate and communicate with the person(s) we intend to protect, the measures to be taken will logically have to be in accordance with these considerations, or, in other words, they will have to be adapted to the fact that if they know the target and where, when and with whom they will be, it will be much easier to attack the target.

Moreover, it is essential to be aware of the varying and heterogeneous rules that converge in these actions so that training and awareness become key elements in the protection of those participating and working within the Administration of Justice.

It is not just a matter of there being an entity that is singularly responsible for providing protection to those who need it, but of making clear the need for a comprehensive system for preventing and combating danger. This premise can only be achieved if, from the start and encompassing the entire applicable legal framework, the necessary processes are introduced for preserving individuals' information and data, among other aspects.

All of this is without prejudice to the fact that this defence must be transversal and complete, so that the fundamental rights set out in Article 18 of the Constitution (in particular section 4[1]) are also guaranteed to the full extent for victims, perpetrators and all those who participate in criminal proceedings.

2. ANALYSIS OF THE APPLICABLE LEGISLATION

It is imperative that measures implemented for the protection of victims and witnesses respect the fundamental principles of our criminal procedure system in order to avoid any significant infringement that could lead to material defencelessness for accused persons. This raises a delicate balance between the need for their adoption and the rights affected thereby, and, in this context, the question arises as to which protected legal interest should prevail in a potential dispute between the safety of victims, witnesses and experts, and the right to effective judicial protection for persons suspected to have committed a criminal offence (Torras, 2019).

The question itself should perhaps be worded differently. From the beginning of modern legal systems, the protection of those involved should be seen as essential and central, not simply an adjunct to the goal of delivering an appropriate decision or judgement[2]. This degree of necessary security should be proportionate to the level of risk that individuals may face as parties to the proceedings, provided that effective judicial protection can also be guaranteed.

When attempting to detail systems for the protection of persons involved in criminal cases, the first question is whether the general protection provided by police and public safety laws to society as a whole is sufficient or not. These provide a first level of defence to all those who fall within the territorial scope of application of our legal system

[1] Article 18(4) of the CE provides that: *4. "The law shall limit the use of information technology in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights."*

[2] Once the objective of sentencing the accused has been achieved, concern for the victims or parties cooperating with the justice system should not be diminished by this mere circumstance.

and, therefore, would also be applicable when such persons are in the role of protected victim, witness or expert.

It should be taken into consideration that the LECrim obliges people to report crimes of a public nature and that those who have the status of witnesses have the duty to cooperate with the justice system, both of which would require a consideration on the part of states, i.e. that their participation should take place in an environment that is conducive to ensuring that this cooperation does not revictimise them and does not endanger their well-being more than is strictly necessary (Ruíz, 2013).

The Spanish Constitution guarantees the right to the protection of the life and physical integrity of all people, and this necessarily includes persons under investigation. However, we aim to analyse which national normative specialisations can be applied in these cases and whether they are sufficient in the field of securing their information and data (Teatino et al., 2022). We should not forget that some national laws include content derived from the application or transposition of EU regulations, such as the DOEP and its incorporation into national law through the LRMRP.

2.1. PROTECTION OF WITNESSES AND VICTIMS IN NATIONAL LAW

2.1.1. General regulations

The first step to be included in this analysis would be the content of Articles 15, 17, 53, 126 and 149.29 of the Spanish Constitution of 1978, the LECrim, the LOPJ, the EOMF, the LOFCS, the CP, the LOPSC and a long list of police and public security regulations, which it is not considered convenient to list in their entirety for reasons of time and length.

The right to life, liberty, effective judicial protection, public safety and how the judicial power and police are constituted enshrined in our Constitution would form the basis of the system of instrumental protection of all persons involved in criminal proceedings.

This section also includes the various resolutions and recommendations of the UN, the Council of Europe and the European Union on the subject[3].

[3] Vid. UN: General Assembly Resolution 39/46 of 10 December 1984, General Assembly Resolution 40/34 of 29 November 1985, General Assembly Resolution 45/107 of 26 March 1991, General Assembly Resolution 46/152 of 18 December 1991, Security Council Resolution 827/1993 of 25 May 1993, the Convention against Transnational Organised Crime, signed in Palermo on 15 November 2000 and the Convention against Corruption, signed in Merida on 31 October 2003 and the UNODC "Handbook of Good Practices for the Protection of Witnesses in Criminal Proceedings Involving Organised Crime" of 2008. Council of Europe: Recommendation (97) 13 of 10 September on witness intimidation and defence rights, Recommendation (2005) 9 of 20 April on the protection of witnesses and collaborators of justice and Recommendation 2063 (2015) of 30 January on the protection of witnesses as an indispensable tool in the fight against organised crime and terrorism in Europe, adopting Resolution 2038 (2015). EU: Council Resolution of 23 November 1995 on the protection of witnesses in the fight against international organised crime, Council Resolution of 20 December 1996 on persons who cooperate with the judicial process in the fight against international organised crime and the European Handbook on Witness Protection: Common Criteria and Principles, consisting of two documents: "Basic principles for police co-operation in the European Union in the field of witness protection" from 2000 and "Common criteria for the inclusion of a witness in a protection programme" from 2002.

On a second level, the missions and duties contained in the EOMF, the LOFSC and the LOPSC establish which institutions are the most directly responsible for guaranteeing fundamental rights and protecting citizen security, and what actions they should carry out.

However, there are many other protection measures that would derive from the content of other provisions, as is the case, as a paradigmatic example, with the CP, which includes various specific criminal offences whose protected legal interest includes, but is not exclusively focused on, the protection of victims, witnesses or experts derived from their participation in criminal proceedings. Thus, we can cite Articles 263.2. 1, which contains an aggravated subtype of the crime of damage, Article 464, which criminalises violence or intimidation to influence witnesses, or Article 471 bis, which criminalises the corruption or reprisals of witnesses before the International Criminal Court.

Likewise, the LECrim establishes various protection measures for victims and witnesses. These include the claim for compensation for participation in the case (Articles 241 and 242), guarantees for online proceedings in specific cases such as gender violence (Article 258 bis), regulation of undercover agents (Article 282 bis), condition to decree provisional detention avoiding concealment or alteration of relevant evidence (Article 503), protection of victims' legal assets, trials behind closed doors with an absolute prohibition on revealing the identities of minors or disabled persons (Articles 681 and 682), restrictions on audiovisual media in courtrooms, and the possibility of making statements in a separate room to avoid confrontation with the defendant (Article 707).

With the entry into force on 21 March 2024 of the RDLJTICS, a qualitative step forward has been taken by regulating:

- the use of information technologies by citizens and professionals in their relations with the Administration of Justice and in the relations of the Administration of Justice with the rest of the public administrations, and their public bodies and related and dependent public law entities.
- the use of ICT by the Administration of Justice, ensuring digital legal certainty, access, authenticity, confidentiality, integrity, availability, traceability, conservation, portability and interoperability of the data, information and services it manages in the exercise of its functions.
- the instrumental nature of ICTs to support and back up jurisdictional activity, with full respect for procedural and constitutional guarantees.

Many of the measures contained in the procedural norms have been recently incorporated and applied after the approval of the LOPIVI, which aims to guarantee the fundamental rights of children and adolescents to their physical, psychological, psychic and moral integrity against any form of violence, ensuring the free development of their personality and establishing comprehensive protection measures, including awareness-raising, prevention, early detection, defence and reparation of harm in all areas in which their lives are developed. This regulation defines violence against these groups as any action, omission or negligent treatment that deprives minors of their rights and well-being, that threatens or interferes with their physical, psychological or social development, regardless of the form and means of its commission, including through information and communication technologies, especially digital violence.

Similarly, we cannot ignore the provisions of the LOPIVG, which had an impact on the comprehensive protection of victims in these processes; these providing high levels of defence of their protected legal assets. We should also note the provisions of the LRC, which make it possible to change surnames or identities by means of a procedure for victims of gender violence and other persons when reasons of urgency or security or other exceptional circumstances require this (not constituting gender violence). The change of surnames or the total change of identity may be authorised by Order of the Ministry of Justice, in the terms established by the implementing regulations.

As a basic rule, the LEVD establishes measures to guarantee the protection, information, support and participation of victims in criminal proceedings, especially those in need of special protection, including minors. In addition, it contemplates protection measures that seek effectiveness against retaliation, intimidation, secondary victimisation, psychological harm or attacks on dignity during interrogations and witness statements. These also include physical protection measures to others, previously mentioned, such as the use of separate rooms in courts to avoid contact between the victim and the offender and any others, at the discretion of the courts, that circumstances may require. In the latter case, it provides that for the protection of victims, one or more of the protection measures referred to in Art. 2 of the LOPT may be adopted.

Within this framework, we cannot forget the application of the regulations on the protection of classified material, which, without prejudice to the content of Articles 301 and 302 of the LECrim, is specifically regulated by the LSO and its implementing regulations.

Lastly, reference should be made to the content of the provisions that fulfil the mandate of Article 18(4) EC by protecting the fundamental right to the protection of personal data in the context of processing for the purpose of prevention, detection, investigation and prosecution of criminal offences. Specifically, we must cite Chapter I bis of Title III of the LOPJ, Arts. 12, 14 and 20 LOMF and the full content of Organic Law 7/2021 of 26 May on the protection of personal data processed for the purposes of the prevention, detection, investigation and prosecution of criminal offences and the execution of criminal penalties (LOPDP).

2.1.2. Regulations specific to protected witnesses and experts.

In addition to the previously incorporated abstract protection, partly derived from compliance with international agreements ratified by the Spanish State, the legislature enacted the LOPT. This law implemented a series of measures with the aim of increasing the protection of those persons who act as such in criminal proceedings, recognising the importance of their collaboration in the judicial system. Without going into an in-depth analysis, it is clear that some aspects have been unquestionably completed and improved by subsequent general regulations, so that it could be summarised that, at present, this organic law merely contains a series of measures with procedural, police and personal repercussions for some very specific cases of special protection.

The law applies to witnesses and experts in criminal proceedings, without defining these concepts exhaustively. Within this framework and subsidiarily applying the concepts and descriptions contained in the LEC, practice has gradually established the content of these concepts and descriptions (and therefore their subjective scope of

application), extending them, depending on the specific case, to the person defined as a witness (according to the definition and obligations contained in the LECrim), to those who have the status of expert witnesses (any person called to testify in a procedure as such), to the victims according to the concept of the LEVD, the co-defendants, the agents of the law enforcement forces and agencies and, partially and practically, to the relatives of the latter.

In order to apply these security measures as permitted by law, the court is required to rationally conclude that there is a serious danger. This decision requires that the authority assess the facts and determine the relevant actions in such a way that the decisions are motivated and conditioned to the factual assumptions and circumstances of the persons to be protected and that they are based on the assessment of an effective and serious danger from at least a particular entity (Cubillo, 2009).

These measures must be adopted, clearly differentiating in this matter between those that can be developed in the investigation phase and those that can be developed in the prosecution phase. As per Article 2 of the LOPT, these are the following:

- Not identifying during proceedings the first name, surname, address, place of work and profession of the persons to be protected, or any other data that could be used to identify them. A number or any other code may be used for identification purposes.
- When taking part in any procedure, using such measures as necessary to make normal visual identification impossible.
- Fixing as a domicile, for the purposes of summons and notifications, the address of the intervening court, which will then forward them in confidence to the person to whom they are addressed.

These measures are easy and quick to implement, but sometimes they will prove to be completely ineffective. Why? Let us imagine for a moment that there are several people involved in a criminal event (e.g. 3). If during the investigation period, two of them are arrested, charged and subsequently accused (of whatever offence), and if the witness evidence is subsequently produced (whether it is considered *anonymous*, *concealed* or the image, voice or appearance of the witness is modified, etc.), and in which such information is made public of which only the third party involved could be aware, a person’s identity could be easily inferred. In such cases, therefore, these initial protective measures will be superfluous and more comprehensive ones should be put in place.

Article 3 focuses on the measures that can be taken by the Court, the Public Prosecutor's Office and the FSC, which can be summarised as follows:

- Prohibit the taking of photographs or images of victims, witnesses and experts.
- Transport to be in official vehicles and allocation of reserved premises in court facilities
- Establishment of police protection (escort services, whether dynamic and/or static, counter-surveillance services, installation of alarm systems, etc.) throughout the process or even after its completion if the danger persists. The Public Prosecutor's Office is of particular relevance as it can urge that these

measures be applied during the whole trial and, if serious danger persists, after the trial is over[4].

- In exceptional cases, new identity documents (Ministry of the Interior) and financial means to change residence or place of work (Ministry of Justice or Autonomous Communities) can be provided by each of the competent authorities.

Once the above measures have been adopted, Article 4 provides that the court with jurisdiction to rule on the matter may review those adopted by the investigating judge, considering the constitutionally protected legal interests and fundamental rights in conflict (Magro, 2010 a). The decisions adopted during the process itself can be grouped as follows:

- Maintenance or lifting of security measures by means of a reasoned order stating that the protected person must be protected against the danger posed by the person or organisation for which the testimony can be considered as evidence for the purpose of a criminal conviction (Magro, 2010 b).
- Disclosure or not of identity data (the parties can request knowledge of the identity of proposed witnesses and experts, respecting any guarantees provided by law) but this can be denied for several reasons: reasoned judicial refusal, consideration of the witness as not relevant, lack of extra-procedural relationship with the accused, acceptance or inactivity of the defence, waiver of the witness by the prosecution, partial disclosure, etc.
- Assessment of the evidence provided.

It should be noted that the measures adopted are subject to appeal and reform.

3. TYPE OF GENERAL MEASURES FOR THE PROTECTION OF VICTIMS OF CRIME AND PROTECTED WITNESSES.

As per the foregoing, the type of protection measures are approached with a combination of legal and practical measures that must or can be adopted in the cases under analysis, and can be divided into blocks differentiated by the assets of these persons.

In the form in which they are included in the legislation, there is a dispersion of measures in various legal provisions and the absence of a comprehensive specific regulation that comprehensively covers the subject in all or most aspects. It is remarkable that our country is the only one in the EU that does not have a comprehensive witness protection programme or a multidisciplinary body to ensure the effective implementation and facilitation of measures, and that the rule that established the basic status of victims is only valid for eight years.

The blocks, broken down by broad themes, could be as follows:

[4] The Instruction of the FGE of 16 November 2007, in correspondence with Article 3.1.10 of the EOMF, which establishes: *"For the fulfilment of the missions set out in Article 1, the Public Prosecutor's Office shall be responsible for: Ensuring the procedural protection of victims and the protection of witnesses and experts, promoting the mechanisms foreseen so that they receive effective help and assistance"* established that the Public Prosecutor's Offices should take the utmost care not to fail to urge in criminal proceedings the adoption of protective measures that may be appropriate by virtue of Article 3.2 of the LOPT.

Determine the reservation of identity:

As stated above, different rules provide for the possibility of keeping the identity of witnesses and experts secret, thus avoiding their public disclosure. This approach is primarily aimed at preventing potential retaliation and ensuring their personal safety. However, this reservation may be lifted in criminal proceedings in order to ensure effective judicial protection.

Change of Identity:

In situations of gender-based violence, extreme need or risk, the complete or partial change of identity of the victim or witness may be considered as an additional protective measure to avoid tracing and minimise the risk of retaliation. However, there are significant differences between civil registration and protected witness regulations in terms of the effectiveness and extent of this measure. In the first case, the change of identity, once granted, has legal effects in legal transactions. On the other hand, in the second case, the change of identity does not imply a legal or registry change of identity, but simply provides the witness with documentation pertaining to an assumed identity (usually a DNI) without an express regulatory backing for its use in legal transactions. In other words, in one situation, the registration is changed, and a new identity is obtained, and in the other, just a document is provided in order to be able to operate in everyday life.

It is important to note that these measures are not retroactive and do not affect all of a person's documents, which means that documents, authorisations and certificates (such as studies and permits), as well as other rights to be exercised (such as mortgages, property or rents), will have to be adapted to this new reality. This process can create a significant security breach, as it involves processes of all kinds. If a new definitive identity is provided, the person will have to change all his or her documents to match the new identity. In other words, if you already have a vehicle in your name, you have to change the registration at the DGT. If you have a degree, the same applies to education, your job, etc. But it is more difficult for those who only have a document for their supposed identity, as this is a temporary situation without legal validity, and they will have to carry out all these procedures in any case.

Restrictions on image and sound registration:

The taking of images or recordings that could reveal the identity of victims (especially minors[5]) and witnesses is prohibited. These restrictions help to maintain confidentiality and in particular to protect the personal data of these individuals so that such activity can be considered as a preventive security measure that will have one or another impact depending on where it is intended to be carried out. The possibility of its implementation on the public highway will not be the same as in the courtroom of a court or tribunal, being necessary on many occasions and depending on the specific case to weigh this right, the right to publicity of criminal proceedings and the right to receive truthful information from the public.

[5] Pursuant to Article 13.2 of the LOPDP, the data of minors may be processed, but always in their best interests and with the appropriate level of security.

Physical Protection:

In order to better protect victims and witnesses, in addition to safeguarding their information, several measures can be implemented to ensure their physical safety. These measures include, among others, the development of specific protection and self-protection plans, the geolocation of aggressors, the assignment of escorts, the provision of safe locations or relocations, and the authorisation of concealment and the establishment of adequate premises to prevent any kind of threat.

It is crucial to differentiate between police and judicial activity in these contexts. The court is responsible for making reasoned decisions based on risk analyses provided to it indicating the level of danger to the witness or his or her relatives. This decision must be reasoned and should consider the extreme circumstances and the high personal, social, moral and economic cost to those affected. Furthermore, the Law Enforcement Forces and Agencies are tasked with the practical implementation of these measures, such as the assignment of escorts and the guarding of secure locations.

However, one handicap we encounter is that our legal system does not explicitly specify the protection measures that can be applied, the administrative bodies responsible for their implementation, nor the budget necessary to carry them out. This lack of detailed regulation hinders the effective implementation of these measures and the adequate protection of victims and witnesses.

Technological Measures:

There are technological resources that are used to protect witness information in records such as audio recordings, transcripts and other documents. The measures aim to prevent the accidental identification of the witness through electronic means and to this end, the security of the means used and the security of the repositories through which the information and data it contains is transmitted and stored must be guaranteed. To this end, it is very important that the security dimensions set out in the ENS[6] are complied with. This instrument stipulates that the protection of public administrations' information must guarantee at least the following dimensions of security: confidentiality, availability, integrity, authentication and traceability of systems and their users.

Financial and social measures:

These measures, whether direct or indirect through social and financial assistance or benefits, complement the previous ones and contribute to effective cooperation with justice and the protection of victims and witnesses. It is important to note that the system applicable to "ordinary" victims, witnesses or experts is completely different from that applicable to persons granted protected witness or expert status.

Law 1/1996 of 10 January on free legal aid and the provisions contained in the LOTJ have very different scopes and areas of application. In the case of the LOTJ, its

[6] The ENS is made up of the basic principles and minimum requirements necessary for adequate protection of the information processed, and the services provided by the entities within its scope of application, in order to ensure access, confidentiality, integrity, traceability, authenticity, availability and preservation of the data, information and services used by electronic means that they manage in the exercise of their competences.

application is indeterminate, imprecise and insufficient. Given the constitutional distribution of competences, and the assumption by the ACs of the means for the application of justice, it is the ACs that exercise the functions of facilitating economic and social measures in each case, with the exception of cases heard by the National Court, where the latter directly applies some financial measures in its proceedings.

Right to the protection of personal data:

Legislation recognises the right to the protection of personal data of persons involved in criminal proceedings[7]. It is important to note that, in the development of each of these missions of the authorities involved, a large and heterogeneous number of measures and goals arise (victim protection, risk assessment, security of protected witnesses, etc.).

From the combination of the aforementioned missions, it is inevitable that during the development of these functions, it shall be necessary to process information and the personal data it contains, and, therefore, the actions of these institutions must be oriented towards guaranteeing fundamental rights both as a purpose in itself and as an integral element of any of their other goals. In other words, it should be pointed out that guaranteeing the protection of personal data is transversal to the development of all or most of these tasks (Fernández, 2023).

The processing of data and information has always been important, but at this moment in history, this has enormous potential and is a crucial aspect of protecting the rights of individuals and ensuring the security of all individuals. On the contrary, however, this does not prevent these actions from being carried out in strict compliance with the necessary rules, immediacy, capacity, ethics and, of course, guarantees and protection of rights.

4. PROTECTION OF PERSONAL DATA AND INFORMATION.

4.1. PERSONAL DATA PROTECTION.

According to legal ground 7 of Constitutional Court Ruling 290/2000 of 30 November 2000[8], the right to informational self-determination or "*Habeas Data"* would be the power of disposal and control over personal data that empowers the individual to decide which data to provide to a third party, whether the State or a private individual, or which can be collected by this third party, and which also allows the individual to know who possesses this personal data and for what purpose, being able to oppose this possession or use. The

[7] Articles 99 and 110 of the RDLJTICS, respectively, state*: "Article 99 Data protection in the use of technological and computer media. The systems used in the Administration of Justice and which process personal data that are to be incorporated into a judicial process or prosecutorial file for jurisdictional purposes shall comply with the regulations provided for in Articles 236 bis to 236 decies of Organic Law 6/1985, of 1 July; in Article 2, paragraphs 4 and 5, of Organic Law 3/2018, of 5 December, and in Article 2.2 of Organic Law 7/2021, of 26 May. Article 100. Data protection in electronic court documents. Judicial and prosecutorial offices shall have the appropriate technological means for the automated implementation of the anonymisation, pseudonymisation and dissociation of personal data. In order to make the provisions of the previous paragraph possible, procedural and judicial decisions shall be adapted to a standardised format stipulated within the State Technical Committee for e-Judicial Administration."*

[8] Judgement 290/2000 of 30 November (BOE No. 4 of 4 January 2001) ECLI:ES:TC:2000:290

Court defines it as an independent, autonomous right, distinct from the right to privacy, honour and self-image. This is a very important question, since the extent and scope of each right, although we can speak of closely related rights, has its own presuppositions and characteristics that are important to know, since very different consequences and situations arise when it comes to their application, protection or exercise (Teatino, et al., 2022).

In line with this fundamental right, it must be remembered that, as with almost all fundamental rights, this is not an absolute right, but must be considered by function in society and in balance with other fundamental rights, in accordance with the principle of proportionality. This is particularly important in criminal proceedings, since from the most embryonic pre-procedural actions of the Public Prosecutor's Office or the FCSE to the resolution of the proceedings, the contributions and actions of all the persons and entities involved therein will be analysed in one way or another.

In order to protect the information and data of persons who collaborate with the justice system, one must first analyse which legislation is applicable, the RGPD and the LOPGDD or other special category legislation. The answer is simple: special rules, as the very essence of the processes and the purpose of the processing, require certain differences that are difficult to incorporate into general rules.

In Declaration No. 21 on the protection of personal data in the areas of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the Intergovernmental Conference that adopted the Treaty of Lisbon signed on 13 December 2007, from the internal debates of those discussing it at a technical level and from the analysis of the factual circumstances that occurred at the local and global levels in the framework of security (the attacks on the Twin Towers on 9/11, the Madrid attacks of 11-M, etc.), the European legislator discovered that it was necessary to develop other provisions that respond and adapt to specific scenarios, such as the framework of the missions of the competent authorities to prevent, detect, investigate and prosecute crimes, and to ensure the enforcement of penalties.

It should be recalled that the aforementioned declaration recognised that specific rules on the protection of personal data and the free movement of personal data might be required in the areas of judicial cooperation in criminal matters and police cooperation, due to the specific nature of the data (Fernández, 2023).

As a result of the above, the EU decided to establish a general processing regime and a specific one for police functions. Thus, Article 2(2)(d) of the GDPR itself provides for the exclusion from its scope of application of 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, including the protection against and prevention of threats to public security.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data 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, the transposition of which into Spanish law has taken place through the LOPDP, which

amended the LOPJ, the EOMF and the LECrim. This ensemble forms the basis of the special regime governing data protection procedures in the framework of the action of the competent authorities in this framework.

4.1.1. General security measures to be applied by data controllers.

Until recently, the justice system was mainly concerned with guaranteeing the success of criminal prosecution and avoiding the impunity of the guilty. The protection of certain people affected by the proceedings (such as victims and witnesses) was considered merely incidental (Turienzo, 2021). Fortunately, the approach has changed, placing the rights of all individuals at the centre of this protection, especially in terms of information, data and identifiers (Fernandez, 2023).

The first measure of a general nature applicable to the group that applies the LOPDP is the inclusion in the policy of the organisations of the legal obligation contained in the personal statutes of the general principle of confidentiality that requires the people comprising the institutions to maintain the reserve and secrecy of everything they learn in the performance of their duties. This is an issue that is not often remembered, but it is one of the foundations on which any system for the protection of assets that do not belong or do not only belong to organisations, such as information and personal data of third parties or their staff, should be based.

Another main measure to achieving this goal is to process the data of individuals with guarantees regardless of their nationality or place of residence, with the controller distinguishing, as far as possible and without disregarding the right to the presumption of innocence, different categories of data subjects, depending on their role, among others:

- Persons in respect of whom there are serious grounds for believing that they have committed or are likely to commit or assist in the commission of a criminal offence.
- Persons convicted or punished for a criminal offence.
- Victims or those affected by, or likely to be affected by, a criminal offence.
- Third parties involved in a criminal offence such as: persons who may be subpoenaed to testify in investigations related to subsequent criminal offences or prosecutions, persons who may provide information about such offences, or contact persons or associates of a person referred to in the first two subparagraphs.

In these situations, although it will often be difficult to classify the person responsible in the same processing (co-accused vs. witness vs. co-defendant), the person responsible will be classified according to the concepts and definitions included in other rules, as in the case of convicted persons (with or without a final sentence, a matter that is not specifically included in the rule), victims and protected witnesses.

Once these roles have been structured and established, the data controller must implement security measures throughout the data lifecycle, i.e. in all operations carried out from the time the data is obtained until it is finally destroyed, without prejudice to applying them even outside the organisations themselves, for example, with traceability systems and remote control of the data when it is transferred to third parties. A paradigmatic example of such systems would be the use of CNN-CERT's CARLA tool for data protection and traceability (CCN, 2024).

These security measures have to be effectively implemented taking into account the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity to the rights and freedoms of natural persons, which increases exponentially in the case of certain victims and persons with protected witness status. To this end, controllers or processors shall implement appropriate technical and organisational measures at their disposal to ensure and be in a position to demonstrate that processing is carried out in accordance with the law (principle of proactive accountability: comply and be able to demonstrate compliance).

In the case of competent authorities, in addition to the protection measures considered by the controller derived from the risk analysis, they should conform as closely as possible to the content of those included in Annex II of the ENS.

As legal systems implemented, one could analyse the appointment of the persons designated as DPOs in their role as system auditors, the registration of operations, the restriction of rights, the management of security breaches and the obligation or not to provide information on the data being processed in the pre-procedural and procedural phase.

4.2. OPERATIONS REGISTER.

The Operations Register constitutes one of the instrumental bases of the system of self-regulation of data controllers in this framework. This is a mandatory control system, which is in turn included in Article 33 of the LOPDP, according to which data controllers and processors must keep records of the identification, authentication and traceability in automated systems of at least the operations of collection, alteration, consultation, communication, including possible transfers, combination and deletion of personal data.

Within these automated systems, records of consultation and communication shall also make it possible to identify the justification for the operation, the date and time thereof and, as far as possible, the name of the person who consulted or communicated personal data, as well as the identity of the recipients of such personal data.

As can be seen, the incorporation of this tool is a top-level indicator for accrediting the measures of proactive responsibility and to adapting the control of access, transfer of data or assignments to the level of risk of judicial or police processing, which directly affects the security of the persons whose data are processed.

The purpose of this register is to verify the lawfulness of processing and self-monitoring, and to ensure the integrity and security of personal data in the field of criminal proceedings. It will only be made available to the competent supervisory authority (AEPD, CGPJ and the authority related to the Public Prosecutor's Office), at their request, and always in accordance with the law in force.

4.3 RESTRICTION OF RIGHTS, LIMITATION AS A CONSEQUENCE OF CRIMINAL INVESTIGATIONS AND PROSECUTIONS.

4.3.1. Restriction of rights

Another instrument made available to the competent authorities by the LOPDP is Article 24, which contains the legal provision enabling the restriction of the exercise of the rights of the persons concerned, which, de facto, sometimes constitutes another protection measure.

The Article provides that the controller may defer, restrict or omit information relating to the data subject's rights, as well as refuse in whole or in part requests to exercise the rights, provided that this is necessary and proportionate in order to: prevent the obstruction of enquiries, investigations or judicial proceedings; prevent prejudice to the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties; or to protect public security, national security or the rights and freedoms of others. As a result, sometimes information will not be provided at an inopportune procedural moment and sometimes the reasons for the restriction may be omitted or replaced by neutral wording where disclosure would jeopardise the purposes of the restriction. This is because the mere communication of the restriction (confirming that data is being processed) would affect the security of individuals.

4.3.2. Rights as a result of criminal investigations and prosecutions.

Article 26 of the LOPDP indicates the form of the exercise of the rights of individuals as a consequence of criminal investigations and prosecutions. This states, on the one hand, that it will be carried out in accordance with the rules of criminal procedure when the personal data appears in a judicial decision, or in a register, proceedings or files processed in the course of criminal investigations and proceedings and, on the other hand, it states that the processing of data in criminal proceedings will be carried out as per the provisions of the LOPJ, the rules of criminal procedure and, where appropriate, the LOMF. This clearly indicates that only in the absence of the regulation of these exercises in these rules will the LOPDP be applied when providing information or access to data.

The Second Criminal Chamber of the Supreme Court analysed these questions in its Judgement 312/2021[9] (rapporteur Pablo Llanera). In connection with Directive 2012/13/EU of the European Parliament and of the Council, of 22 May 2012, in its first legal ground (1.12), it considered that:

- The parties, and in particular the defendants, have the right to know the full content of the procedural proceedings, with no exception other than that derived from their declaration of secrecy (Art. 302 LECrim).
- This right extends to judicial acts limiting fundamental rights carried out in other court proceedings, when the validity of the evidence that affects them depends on their legitimacy, and they have not already been incorporated into the proceedings (Arts. 579 bis and 588 bis i of the LECrim).

[9] STS 1388/2021 of 13 April – ECLI:ES:TS:2021:1388

- The right of the parties to know and examine the court proceedings, embodied in Articles 118, 627, 780.1 and 784.1 of the LECrim, does not entitle them to know any pre-procedural investigation not material to the proceedings.
- Exceptionally, when there are well-founded indications of circumstances that compromise the validity of the evidence or that may reasonably condition its credibility or its indicative capacity, thereby affecting the rights of defence of the parties' claims, the parties may request that the competent court incorporate only the specific points of the preliminary investigation that reflect such conditions.
- In such cases, the court carries out a double analysis of the relevance and necessity of the requested enquiry (Arts. 311, 659, 785 and 786.2 LECrim).

4.4 SECURITY BREACH MANAGEMENT.

In the event of a security incident affecting confidentiality, such as the leakage of data to third parties, the data controller must have an efficiently defined and implemented protocol for containment, communication and action in the event of security breaches affecting its data.

It should not be forgotten that a breach can have a series of considerable adverse effects on people, which can cause physical, material or immaterial damage and harm; therefore, it is necessary to try to avoid them and, if they do occur, to manage them appropriately, especially in these cases.

When the breach has materialised, such as through access to data of victims or protected witnesses, without prejudice to other responsibilities or actions to be taken, those responsible are obliged to notify the competent supervisory authority[10] when it is likely to constitute a risk to the rights and freedoms of individuals (which in this case would be beyond doubt). This communication should also be made to the data subjects[11], unless it is not necessary because the controller has taken appropriate technical and organisational measures that avoid the above risks, minimise the harm to rights and freedoms and/or make it reversible. In addition to this, subsequent to the personal data breach, protective measures may be taken that fully or partially mitigate the possible impact on data subjects and ensure that the high risk to their rights and freedoms is no longer likely to materialise or would involve a disproportionate effort. In this case, a publication shall be made in the relevant official gazette, on the controller's website or another official channel that allows effective communication with the data subjects.

However, even if it can be inferred that there are high levels of risk for the individuals concerned, Article 39.5 of the LOPDP[12], allows for the postponement,

[10] At the national level, the supervisory authority would be the Spanish Data Protection Agency, unless it can be attributed to the poor management of the Autonomous Administration of Andalusia, Catalonia or the Basque Country, in which case it would correspond to the Data Protection Authority of those autonomous communities.

[11] In order for them to exercise the actions they deem appropriate in defence of their interests and implement the self-protection measures they deem necessary.

[12] Article 39.5: *"The communication to the person concerned referred to in paragraph 1 may be deferred, limited or omitted subject to the conditions and on the grounds provided for in Article 24.*

limitation or omission of the communication subject to the conditions and on the basis of the purposes contained in 24.1[13].

These actions and breaches of communication procedures should contain clear instructions on how to act in the event of a leak of the data of the parties in criminal proceedings[14] to the media. This does not seem to be carried out with the necessary efficiency, since information about the persons involved (defendants, victims, witnesses, etc.) often appears in the media from sources that are not or should not be open.

[13] Article 24.1: "1. The controller may defer, restrict or omit the information referred to in Article 21.2, as well as refuse, in whole or in part, requests to exercise the rights referred to in Articles 22 and 23, provided that, taking into account the fundamental rights and legitimate interests of the data subject, it is necessary and proportionate for the following purposes: a) To prevent the obstruction of enquiries, investigations or judicial proceedings. b) To avoid prejudice to the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties. c) To protect public safety. d) To protect national security. e) To protect the rights and freedoms of other persons.

[14] It is true that the right to public information must be respected and guaranteed, but we should also consider whether the processes of obtaining such information, for example, when it is not obtained from press offices or press units but is "leaked" by "sources" from an entity, constitutes a security breach in the organisations that had the obligation to keep it secure.

5. CONCLUSIONS

The legal system for the protection of information and data of persons involved in criminal proceedings is composed of several rules that converge on this issue. In today's information and communications society, ensuring this security is essential as it is very easy to identify and locate people in such a way that they can be profiled, coerced or threatened, to the detriment of the administration of justice.

The LOPJ, the EOMF and the LOPDP, especially since the entry into force of the RDLJTICS, constitute milestones in criminal proceedings, as they oblige all entities responsible for processing operations to adopt measures to secure data as a major element of criminal investigations and proceedings. These standards could be considered basic in this respect, and their premises converge with a number of other standards whose content develops a solid and robust system for achieving their goals from a theoretical point of view.

The implementation of security processes is time-bound and requires adequate budgetary allocations so that these actions can be carried out effectively and do not remain mere declarations of intent. It is crucial to develop automated security processes throughout the data lifecycle, both inside and outside the bodies involved, and to demand greater accountability for non-compliance. In other words, entities have to install technical (cybersecurity) and operational processes that secure information from the first actions until the end of the processes and, subsequently, for as long as it is necessary to maintain the data.

A leakage of information from an entity constitutes a security breach which must be reported to the relevant independent supervisory authorities and to the persons concerned.

These persons need to be trained and informed about the dangers and level of risk of exposing themselves or not acting safely on information and social networks or applications.

In addition to securing the information of victims, witnesses and experts, for the same purpose, information relating to authorities and public officials whose data (beyond that which is legally required to be public due to the performance of their duties) must also be safeguarded.

The standards in this framework are not yet well known, which highlights the need for more investment, training and awareness raising. It is essential to align staff on the importance of the information they handle and to make them believe that they really are a fundamental part of the security process. The chain is always broken by the weakest link, so courses and workshops in a cycle of continuous improvement are an indispensable element in achieving these goals.

In the specific case of persons who are granted the status of protected witness or expert, without going into the rest of the measures adopted, it is stated that the LOPT has clear gaps in this field of information protection that must be completed with the application of the previously mentioned rules. This protection system lacks the necessary legal and regulatory backing to enable the creation of a comprehensive, interdepartmental

witness protection programme that sets out clear commitments and obligations of the parties (witnesses vs. administration) and facilitates solutions to the serious information security failures it possesses. As this paper explains, the witnesses themselves are responsible for carrying out actions in legal transactions necessary for adapting their legal status as a result of the adoption of a new identity or the provision of documents of assumed identity, and this means that their security is permanently compromised in the course of the proceedings necessary for this purpose. Similarly, they are responsible for the application of security precautions in the use of information technologies and Apps.

The public parts of the projects to enact a new LECrim of the years 2011, 2013 and 2020 (the latter still published on the public participation page of the Ministry of Justice since 26 January 2021) have been analysed, and none of them includes a comprehensive and systematised programme, system or set of measures to protect these persons nor a body at the national inter-administrative level with specific competences to do so.

The Supreme Court, in its judgement of the Second Criminal Chamber no. 468/2020, of 23 September[15] (rapporteur Vicente Magro Servet), in the second legal ground, 1, indicates that experience reveals the reluctance of citizens to assist the judicial police and the Administration of Justice in certain criminal cases for fear of reprisals, which often leads to a lack of valuable testimony and evidence in these proceedings. Faced with this situation, the legislator must dictate rules that are effective in safeguarding those who, as witnesses or experts, must comply with the constitutional duty to cooperate with the justice system. Sharing this criterion, it would be essential that, if the latest draft or future drafts of the reform of the LECrim continue, these provisions be incorporated in order to comply more effectively with security requirements and not continue to be one of the few countries in the European Union which, in the area of protected victims and witnesses, does not have a national programme that covers all of these issues in one way or another.

[15] STS 468/2020, 23 September 2020, ECLI:ES:TS:2020:2987

BIBLIOGRAPHICAL REFERENCES

Ayllón Santiago, H. S. (2021). *Tratamiento de datos de carácter personal en el ámbito policial.* Madrid. Reus.

CCN, C. C. (10 March 2024). *CCM-CERT.CNI.ES*. Retrieved from https://www.ccn-cert.cni.es/es/soluciones-seguridad/carla.html

Cubillo López, I. J. (2009). *La protección de testigos en el proceso penal.* Pamplona: Civitas.

Fernández González, C. (2023). La protección de datos personales en el ámbito policial. Especial referencia a la LO 7/2021, de 26 de mayo. *La administración de justicia y el derecho a la protección de datos personales* (p. 66). Madrid: Centro de Estudios Jurídicos.

Gascón Inchausti, F. (2001) *"Prueba sobre la prueba," protección de testigos menores, objeto y motivación del veredicto y control del juicio de indicios en el proceso penal*. Retrieved on 16 February 2024, from https://eprints.ucm.es/26585

Irujo, J.M., (2012) *Testigos desprotegidos. El precio de acusar. El País.*

Magro Servet, V. (2010) *Régimen legal de los testigos protegidos en el proceso penal*. Retrieved on 16 February 2024, from https://dialnet.unirioja.es/servlet/articulo?codigo=3320107

Magro Servet, V. (2010). *Régimen legal de los testigos protegidos en el proceso penal***.** La Ley Penal -- No. 75 p. 24-35

Navarrete, E. M., García, J. C., & Muñoz, F. A. (2014). *Protección de Víctimas y Testigos como una garantía Constitucional*. Retrieved on 16 February 2024, from http://ri.ues.edu.sv/id/eprint/7504

Ruiz Barba, O. (2013). *Diferentes modelos de protección de testigos*. Retrieved on 16 February 2024, from https://dialnet.unirioja.es/servlet/articulo?codigo=4548356

Teatino Gómez, D. (2022). *Estudio sobre el sistema de protección de datos personales con finalidad de prevención, detección, e investigación policial de infracciones penales.* Madrid: Ministry of the Interior, State Secretariat for Security.

Torras Coll, J. M. (2019). *Los testigos protegidos y el derecho de defensa*. Retrieved on 16 February 2024, from https://dialnet.unirioja.es/servlet/articulo?codigo=7151044

Turienzo Fernández, A. (2021). *Sobre el testigo protegido en España: La Ley Orgánica 19/1994, de 23 de diciembre bajo examen. Revista General de Derecho Procesal*, No. 51, Article number 423249.

Vega Dueñas, L. C. (2015). *La protección de testigos, víctimas y colaboradores con la justicia en la persecución a la criminalidad organizada.* Retrieved on 16 February 2024, from https://dialnet.unirioja.es/servlet/tesis?codigo=54332.