Article

Cybercrime and its Evolution in the European and Spanish Regulatory Framework

Isabel Mendoza García

Lecturer and Researcher, UCAM Faculty of Law. Head of UCAM Legal Services UCAM – Universidad Católica de Murcia ORCID: https://orcid.org/0009-0005-2874-9106 Email: imendoza@ucam.edu.

Received 03 January 2026, Accepted 21 February 2026

KEYWORDS:

Cybercrime, cybersecurity, digitalization, technology.

ABSTRACT:

Cybercrime is a complex and global phenomenon that requires a multidisciplinary approach to understand and combat it effectively. Spain has approached the issue of cybersecurity in a fragmented, disorganised, and often belatedly manner, which has led to a cybercrime crisis at the legal and institutional levels. The European Union has responded to these threats with a series of legislative initiatives and cooperation strategies, culminating in the creation of the European Cybercrime Centre within Europol. In an increasingly connected world, the increase in cybercrime reflects the risks inherent in technological advancement and the digitalisation of society. Recent years have seen a significant rise in cybercrime incidents, leading to increased legislation to combat this phenomenon.

PALABRAS CLAVES:

Ciberdelincuencia, ciberseguridad, digitalización, tecnología.

RESUMEN:

La cibercriminalidad es un fenómeno complejo y global que requiere un enfoque multidisciplinar para su comprensión y combate efectivo. España ha abordado el tema de la ciberseguridad de una manera fragmentada, desordenada e, incluso, a destiempo, lo que ha provocado una crisis cibernética a nivel jurídico e institucional. La Unión Europea ha respondido a estas amenazas con una serie de iniciativas legislativas y estrategias de cooperación con las que se busca una mayor eficacia en la prevención y lucha contra este tipo de delitos, culminando en la creación del Centro Europeo de Ciberdelincuencia bajo el control de Europol. En un mundo cada vez más conectado, el incremento de delitos en el ciberespacio refleja los riesgos inherentes al avance tecnológico y la digitalización de la sociedad. Durante los últimos años se ha experimentado un aumento significativo en los incidentes de ciberdelincuencia y por ello se ha aumentado la legislación para poder combatir este fenómeno.

MOTS CLES :

Cybercriminalité, cybersécurité, numérisation, technologie.

RESUME :

La cybercriminalité est un phénomène complexe et mondial qui nécessite une approche multidisciplinaire pour être compris et combattu efficacement. L'Espagne a abordé la question de la cybersécurité de manière fragmentée, désorganisée et parfois tardive, ce qui a provoqué une crise cyber aux niveaux juridique et institutionnel. L'Union européenne a répondu à ces menaces par une série d'initiatives législatives et de stratégies de coopération visant à renforcer l'efficacité de la prévention et de la lutte contre ce type de délits, aboutissant à la création du Centre européen de lutte contre la cybercriminalité au sein d'Europol. Dans un monde de plus en plus connecté, l'augmentation des délits dans le cyberespace reflète les risques inhérents au progrès technologique et à la numérisation de la société. Au cours des dernières années, on a constaté une augmentation significative des incidents de cybercriminalité, ce qui a conduit à un renforcement de la législation afin de lutter contre ce phénomène.

Contents:

1 INTRODUCTION

Historical developments in criminal law have repeatedly shown that when it comes to combating crimes whose effects extend beyond the territory of a given country and affect the international community as a whole, such as drug or human trafficking, joint and coordinated action by States is also necessary to achieve greater effectiveness in achieving their objectives.

That being the case, the type of crime that can truly be said to have no borders or territorial limits is cybercrime. This article provides a detailed analysis of the regulatory and chronological development of the most significant European legislative measures that have had the greatest impact on the fight against cybercrime in Europe and in our country, from European Directives to amendments or extensions of criminal offences in the Spanish legal system, increased penalties and new categories that have been defined to broaden the scope of criminal law, fill legal gaps and, ultimately, advance the punitive line to avoid, as far as possible, the risk to the legally protected interest.

2 OBJECTIVE

The aim of this study is to analyse cybercrime and how it has evolved within the European and Spanish regulatory frameworks.

3 METHODOLOGY

3.1 TYPE OF STUDY

This study falls within the scope of exploratory and descriptive qualitative research, the main objective of which is to analyse cybercrime and how it has evolved within the European and Spanish regulatory frameworks. The research is based on a systematic review of academic literature, current legislation and documented cases, supplemented by interviews with experts in criminal law and education (Creswell & Poth, 2018).

3.2 RESEARCH DESIGN

A non-experimental and cross-sectional design was used to examine the relationship between cybercrime and its evolution in the European and Spanish regulatory frameworks. This approach is suitable for analysing current and emerging phenomena, such as the regulatory evolution of cybercrime (Flick, 2021).

3.3 POPULATION AND SAMPLE

The population under study includes:

1. Scientific and academic literature: articles, books, and reports on cybercrime.
2. Legal regulations: European and Spanish legislation on cybercrime.
3. Experts in law and cybersecurity: semi-structured interviews with professionals with experience in cybercrime prevention, cybersecurity, and digital ethics.

Sources were selected using purposive sampling and inclusion criteria, prioritising recent publications (2018–2025) of academic relevance and with institutional or legal recognition.

3.4 DATA COLLECTION TECHNIQUES

3.4.1 Literature review

A systematic search of academic and legal literature was conducted in databases such as Scopus, Web of Science and Google Scholar, as well as on official legislation websites and those of international organisations. Peer-reviewed articles, specialist books and institutional reports on cybercrime and the evolution of the European and Spanish regulatory frameworks were included (Zhang et al., 2024; ENISA, 2024).

3.4.2 Document analysis

Legal documents were analysed, including:

- Spanish legislation on cybersecurity and cybercrime.
- European legislation on cybersecurity and cybercrime.

This analysis enabled the identification of the evolution of the European and Spanish regulatory frameworks regarding cybercrime.

3.4.3 Semi-structured interviews

Interviews were conducted with 5 experts in criminal law, academic ethics and AI technologies, using open-ended question guides to explore perceptions of legal risks and prevention strategies. The interviews were recorded and transcribed for thematic analysis (Braun & Clarke, 2021).

3.5 DATA ANALYSIS TECHNIQUES

Qualitative content analysis was used, coding the data into thematic categories related to types of offences, legal implications, ethical risks and prevention measures. This approach enabled the identification of trends, similarities and differences in the documented cases and the reviewed literature (Flick, 2021).

To ensure validity and reliability, triangulation techniques were applied:

1. Source triangulation: cross-referencing literature, regulations and documented cases.
2. Researcher triangulation: joint analysis of interviews and documents by two independent researchers.
3. Methodological triangulation: a combination of literature review, document analysis and semi-structured interviews (Creswell & Poth, 2018).

3.6 ETHICAL CONSIDERATIONS

The study adhered to ethical research principles, including confidentiality and anonymity of the experts interviewed. (Livingstone & Stoilova, 2023).

4 EUROPE

4.1 COUNCIL OF THE EUROPEAN UNION (2000). COUNCIL DECISION OF 29 MAY 2000 ON COMBATING CHILD PORNOGRAPHY ON THE INTERNET.

In 2000, the European Union and the European Council, in view of the relentless increase in crimes 'against the sexual freedom and integrity of minors' via the internet (Council of the

European Union, 2000), adopted the Council Decision of 29 May 2000 on combating child pornography on the Internet, which expressly states that it is aware 'of the need for the Union to adopt further measures to promote the safe use of the Internet' and the need to 'prevent and combat the sexual abuse of children and, in particular, the production, processing, possession and dissemination of child pornography via the Internet.'

To this end, that Decision sets out various measures to prevent and combat this serious criminal problem more effectively. It is now, having allowed sufficient time to elapse since these measures were adopted, that we should look back and, in the light of the data available to us, draw the appropriate conclusions as to whether the adoption of that Decision has yielded the expected results and, where appropriate, identify other possible measures to be taken.

Thus, regarding the first of these considerations, we could state that, whilst objectives have been achieved through the measures implemented, it is no less true that cybercrime has also seen a significant increase in its overall figures, both in terms of the perpetration of this type of crime and the number of users/consumers of these products; circumstances which have, on the other hand, been facilitated by the progressive and ever-accelerating technological advances that are opening up more and more opportunities, both for the commission of new types of offences and for the concealment of their perpetrators.

All of the above highlights the need for the legislature to put the necessary measures in place to streamline current investigative and preventive procedures and to equip the police and security forces with the tools required to combat this increasingly complex phenomenon, in an environment where there are more and more ways to hinder, if not prevent, the tracing of the origin of criminal activities, thereby constituting a fertile breeding ground for criminal mafias to establish themselves. In this regard, suffice it to say that, today, terms such as 'Dark Web' or 'Deep Web' (Ramos, 2026), and, logically, their meaning and content, are frequently used, with these marginal areas of the internet constituting the usual means of navigation for the perpetration of criminal acts.

We are, in short, faced with a terrain particularly conducive to the perpetration of a wide variety of crimes because, as the saying goes, 'You cannot stem the tide'; it would be even more difficult to contain and set limits on the so-called 'network of networks'. Thus, in recent years, and according to data provided by the National Institute of Statistics, there has been a very significant increase in serious crimes committed via this medium, notably sexual offences and, most critically, against minors, which gives us a very clear idea of the dangers of this medium when used for criminal purposes.

In contrast to all of the above, we can state that Spain is precisely one of the most advanced countries in terms of legislation against these crimes, a fact complemented by the actions of our Supreme Court, which has also ruled on the matter, establishing a uniform interpretation of the various types of crime (Villegas & Encinar, 2023).

Furthermore, and continuing with the aforementioned Council Decision of 29 May 2000 on combating child pornography on the Internet, it is worth noting, as a significant merit of the decision, that it did not confine itself to making mere programmatic, generic statements requiring further elaboration, but rather adopted concrete measures to wage a serious fight against the sexual exploitation of minors via the Internet.

Admittedly, a Joint Action against trafficking and sexual exploitation of children had already been adopted on 24 February 1997, following the conference held in Vienna on women trafficking in June 1996 (European Union, 1997), as well as the extension of Europol's mandate, the aim of which was, as mentioned, to combat child pornography on the internet (European Union, 1997). However, data show that all this proved insufficient and that crime figures continued to rise, compounded by the foreseeable and already documented increase

in such offences committed via the internet, owing to the added difficulty in prosecuting them.

This 1997 Convention, now repealed by Decision 2004/68 of 22 December, sought to establish common standards to improve judicial cooperation and prevent these practices that violate fundamental human rights and dignity. Each Member State was required to review its legislation to criminalise such conduct, adopting effective penalties, protecting victims and cooperating procedurally and judicially with other Member States. Furthermore, an interdisciplinary approach would be promoted and efforts coordinated at national and European level to ensure an adequate response.

The measures agreed in the aforementioned 1997 Treaty were as follows. Firstly, to urge ordinary internet users to report to the authorities any suspected dissemination of child pornography. Secondly, the effective enforcement of sentences against those convicted of such offences is one of the most significant measures, made possible by the creation of units specialising in this issue and the enforcement of sentences. And finally, it is of paramount importance that the competent authorities act swiftly once they receive information from users, in order to prevent and, where appropriate, investigate and subsequently punish offenders (European Parliament, 1999).

From this Decision, we can highlight that all preventive work carried out by the authorities is essential in this regard due to the dual gravity of the crime (minor victims and sexual offences), as the profile of the offenders follows a recurring pattern, as the study confirms.

4.2 European Commission (2001). Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime.

This 2001 Communication from the European Commission, entitled 'Creating a safer information society by improving the security of information infrastructures and combating computer-related crime', establishes a key strategic framework for addressing the challenges posed by the rapid evolution of digital technologies. In the aforementioned document, the Commission highlights European society's growing dependence on critical information infrastructures and emphasises the necessary obligation to ensure their security against threats that may arise from cyberspace, such as cyber-terrorism and attacks on communication networks. This approach reinforces the interconnection between technological, economic and social security, all within the scope of the European Union (EU).

The Communication established as a priority the creation of a cohesive regulatory environment enabling Member States to coordinate actions against cybercrime. In this regard, it advocates legislative harmonisation to overcome existing disparities between national legal frameworks across Member States. Among the key proposals is the strengthening of transnational cooperation between police and judicial authorities, emphasising the importance of Europol and Eurojust in their ongoing fight against cybercrime. Furthermore, it recognises and underlines the need to foster all forms of public-private collaboration to address emerging issues, such as data theft or, more commonly, attacks on financial systems.

Likewise, a key turning point in the Communication is the necessary implementation across all sectors (public and private) of preventive and educational measures aimed at strengthening the resilience of information infrastructures. The Commission urges Member States and technology companies to develop robust risk management systems, incorporating international security standards and promoting all research into cybersecurity. These actions seek not only to protect networks and data against current threats, but also to

anticipate future challenges in the digital landscape, which remains an uncertain prospect. At the same time, the importance of raising awareness among European citizens about the risks inherent to Internet use is highlighted, promoting a culture of digital security. In this regard, the efforts of the Spanish government appear to be truly insufficient to ensure that, through a top-down and cascading approach, awareness is raised through concrete educational and/or training measures and actions that reach all sectors of society in our country. Admittedly, a number of action programmes have been implemented, but, as has been demonstrated, in the field of cybersecurity, nothing ever seems to be enough.

To conclude this review, it is worth noting that the EU's commitment to building a 'safer information society', based on trust and international cooperation, is being reinforced. This effort aligns with the European Union's commitments (UNODC, 2021) within global frameworks promoted by the Council of Europe and the United Nations, particularly in initiatives related to the fight against cybercrime and the promotion of human rights in the digital environment (United Nations General Assembly, 2023). The 2001 Communication is, in short, the policy document that lays the foundations for innovative policies on IT security, and which also reinforces the European Union's commitment to ensuring a trustworthy and secure digital space for all European citizens.

4.3 COUNCIL OF EUROPE (2001). COUNCIL OF EUROPE CONVENTION ON CYBERCRIME.

This Convention on Cybercrime (Council of Europe, 2001) is the first international treaty specifically designed to tackle cybercrime; it was adopted by a large majority in the Council of Europe, with the primary aim of combating cybercrime. Indeed, the agreement can be considered one of the most significant measures adopted to combat online crime. The primary aim was to harmonise the elements of criminal offences in accordance with the criminal legislation in force at the time (2001); member states worked together to harmonise criminal laws, focusing on defining the various cybercrimes, whilst also establishing procedural measures for the investigation and prosecution of such criminal offences. Finally, efforts were made to establish a swift and effective system of international cooperation, providing mechanisms for international cooperation to combat cybercrime; although there was a firm commitment, as time went on and improvements were made, the processes became increasingly complex. Realistically, this convention was the only real option available at the time (Diaz, 2010), although more recently the Second Additional Protocol to the Council of Europe Convention on Cybercrime, concerning enhanced cooperation and the possible disclosure of evidence, was signed (Council of Europe, 2022). This signing represents an extension (2001) but also signifies a strengthening of the commitment to fight cybercrime, reinforcing cooperation between signing states and the exchange of electronic evidence between authorities in the fight against cybercrime.

The improvement of mechanisms for international cooperation in specific criminal proceedings provides new momentum to the already signed Convention (2001). It should be emphasised that the implementation of new protocols to ensure compliance with the regulations is important, as without a genuine commitment, this would lead to increased impunity and, consequently, a rise in the number of such crimes.

And the result of all the above is that States appear to have full confidence in this second protocol signed for the effective fight against cybercrime, in which various improvements are worth highlighting, such as the strengthening of cooperation between States, or the safeguarding of data processing, as well as the application of a protocol and how it is to be implemented. On the other hand, one of the most significant advances introduced by this Convention is that it addresses specific problems which, until then, had been raised but remained unresolved. This includes issues concerning jurisdiction and territoriality in relation to electronic evidence. In other words, the data required for the investigation,

prosecution and punishment of such offences is, in most cases, located in different countries and jurisdictions, which necessitated greater flexibility in cooperation to ensure effective results in the prosecution of these offences (Council of Europe, 2025).

4.4 COUNCIL OF THE EUROPEAN UNION (2001). COUNCIL RECOMMENDATION OF 25 JUNE 2001 ON CONTACT POINTS PROVIDING A 24-HOUR SERVICE TO COMBAT HIGH-TECH CRIME.

This is a necessary and sound recommendation from the Council which, although brief (Council of the European Union, 2001), addresses fundamental issues for the prosecution and suppression of this type of crime. It establishes key guidelines for the necessary improvement noted above, enhancing coordination and effectiveness in the fight against cybercrime both within and outside the European Union. The most relevant aspects of this recommendation include:

1. The creation of operational national contact points, whereby Member States are urged to designate national contact points available 24 hours a day, 7 days a week. The purpose of these points is to facilitate the most immediate and efficient cooperation in investigations related to high-tech crime. To this end, staff in these operations must possess a high level of training and expertise in the field.
2. Secondly, the aim is also to facilitate and streamline the exchange of information, whereby the contact points must ensure the rapid and effective transmission of information between Member States and international organisations, ranging from Europol to the Council of Europe. All of this must be carried out whilst respecting fundamental freedoms and protecting rights.
3. Next, the necessary international cooperation was taken into account, highlighting the need to strengthen cross-border cooperation, whilst also promoting collaboration with third countries and international bodies, ensuring a coordinated approach to combating cybercrime.
4. With regard to technical and judicial support, it is worth noting that technical assistance must be immediate and swift in order to be truly meaningful and achieve the desired results, always employing a process that respects all safeguards regarding rights, from national to international laws, whilst also being capable of providing a rapid and agile response to requests.

Finally, and as a point worth highlighting, it must be mentioned that it would be impossible to implement all of the above without harmonisation between the resources and capabilities required for their development; this requires technological infrastructure to support the measures outlined, including common protocols validated by all stakeholders, Member States, and so on, in order to guarantee a uniform and truly effective response.

All of this has strengthened the fight against cybercrime; it has objectively led to an improvement in the response among Member States (European Commission, 2024); and, above all, as a particularly noteworthy result, it has succeeded in raising awareness among Member States of the need to develop joint actions to achieve more effective outcomes.

4.5 COUNCIL OF THE EUROPEAN UNION (2005). COUNCIL FRAMEWORK DECISION 2005/222/JHA OF 24 FEBRUARY 2005 ON ATTACKS AGAINST INFORMATION SYSTEMS.

This Council Framework Decision 2005/222/JHA of 24 February 2005 (Council of the European Union, 2005) on attacks against information systems, primarily establishes a common framework for prevention by defining and criminalising offences affecting the integrity, availability and confidentiality of computer systems and data in the Member States

of the European Union. Its main objective was to standardise Member States' legislation on cybercrime, thereby ensuring that penalties were effective, dissuasive and proportionate. Behaviours classified as offences include unlawful access to information systems, interference with the functioning of systems (such as denial-of-service attacks) and interference with data through alteration, deletion or intentional corruption (Sieber, 2022). In Spain, this legislation led to the introduction of new criminal offences into our legal system, which was implemented through Organic Law 5/2015 reforming the Criminal Code.

This Framework Decision is a further instrument designed to strengthen cross-border judicial and police cooperation, recognising the global and transnational nature of cyber attacks. To ensure a coordinated response, Member States are urged to establish 24/7 operational contact points, facilitate the exchange of information in real time and collaborate with international organisations such as Europol. Furthermore, it highlights the need to constantly update national legislation to address new forms of cybercrime and to promote cooperation with private sector actors, such as internet service providers, for the detection and mitigation of these attacks (Bantekas & Stein, 2024).

4.6 European Commission (2007). Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime.

This Communication from the European Commission, dated 22 May 2007, marked a milestone in the European Union's strategic approach to tackling the growing threats posed by cybercrime. This document identifies three main categories, or types, of cybercrime (European Commission, 2007): traditional crimes adapted to the digital environment, such as fraud and forgery; illegal online content, such as child pornography or incitement to hatred; and attacks on information systems, cyberattacks and computer sabotage. The Communication highlights the need for a comprehensive framework combining preventive, repressive and cooperative measures to tackle these challenges.

Certainly, a key aspect of this Communication is the creation of a European platform for reporting online crimes, through cooperation between private operators and police forces via common agreements, and the promotion of cyber patrols as a modern tool for monitoring illicit activities on the internet. Furthermore, it proposes solutions to problems arising from anonymity in telecommunications and, finally, it is worth noting that it encourages the use of joint investigation teams.

In the medium term, the Communication prioritises the implementation of systems to block websites containing illegal content, such as child pornography, through common blacklists shared among Member States. It also proposes facilitating rapid access to information via remote searches, harmonising definitions of cybercrimes, and promoting the collection of comparable statistics to better understand trends in cybercrime.

4.7 European Commission (2009). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

This Communication highlighted the need for coordinated action at national, European and international levels to tackle cybercrime: prevention, preparedness and awareness. It also defines a plan of immediate measures to enhance the security and resilience of CIIs (critical information infrastructures). It sets out several key measures, such as the creation of platforms for reporting crimes, the development of public-private cooperation agreements, and the strengthening of cyber patrols and operational collaboration, as the lack of

coordination is highlighted in section 3.4.1. Furthermore, it proposed blocking illegal content, such as child pornography, and promoted legislative harmonisation and the collection of comparable statistics on cybercrime.

The aim is to promote EU and international collaboration and cooperation, as well as raising public awareness, which are the cornerstones of the initiative, seeking a safer and more trustworthy digital society; it is now up to the institutions to respond with robust and secure tools to ensure cybersecurity.

4.8 EUROPEAN COMMISSION (2012). COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT: TACKLING CRIME IN OUR DIGITAL AGE: ESTABLISHING A EUROPEAN CYBERCRIME CENTRE.

This document focuses on the urgent need to strengthen the fight against cybercrime in an era marked by digital globalisation. It proposes the creation of the European Cybercrime Centre (EC3), within the Europol structure, to coordinate efforts among Member States and serve as a central hub for information, training and operational support in investigations related to cybercrime. The EC3 focuses on serious crimes, such as online fraud, child sexual exploitation or cyberattacks on critical infrastructure, whilst fostering cooperation with international partners and private actors to dismantle highly organised criminal networks.

A key improvement would be the integration of a dynamic risk assessment system that enables the anticipation of emerging threats in real time, using artificial intelligence and big data. This could strengthen the EC3's response capacity by equipping it with more advanced tools to identify criminal patterns and predict potential attacks, thereby ensuring better protection of the digital economy and the rights of European citizens. Furthermore, it would be beneficial to raise public awareness of cybersecurity through educational campaigns targeting different sectors of society.

4.9 EUROPEAN COMMISSION (2013). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – THE EUROPEAN UNION CYBERSECURITY STRATEGY: AN OPEN, SAFE AND SECURE CYBERSPACE.

The 2013 European Union Cybersecurity Strategy establishes a comprehensive framework to address the challenges of cyberspace, with five strategic priorities: strengthening cyber resilience, reducing cybercrime, developing cyber defence capabilities, fostering industrial cybersecurity resources, and promoting a coherent international policy for cyberspace. It highlights the importance of multi-sectoral cooperation between public administrations, the private sector and citizens to ensure an open, secure and trustworthy cyberspace, whilst respecting fundamental rights and freedoms online. Furthermore, it introduces key initiatives, such as the creation of Computer Emergency Response Teams (CERTs), pan-European simulation exercises and frameworks for information sharing between Member States.

As a step forward, this new reality must be integrated more broadly, incorporating emerging technologies such as artificial intelligence and big data into cyber threat detection and response systems (ENISA, 2020). This would enable incidents to be anticipated and mitigated proactively, optimising analytical capabilities and strengthening real-time cross-border cooperation. At the same time, it is essential to step up training programmes for professionals and public awareness of digital risks, with a particular focus on universities, which have so much to contribute (ENISA, 2022), thereby ensuring a more robust and interdisciplinary response to cyber threats.

4.10 COUNCIL OF THE EUROPEAN UNION (2015). COUNCIL CONCLUSIONS ON CYBER DIPLOMACY, BRUSSELS, 11 FEBRUARY 2015

The conclusions highlight the need for a comprehensive and coherent approach to addressing cyberspace-related issues in the European Union's (EU) foreign policy. They recognise the cross-cutting impact of cyberspace on security, the promotion of human rights and the digital economy. The Council emphasises the importance of ensuring a free, secure and open cyberspace, based on the EU's fundamental values, such as democracy and the rule of law. Furthermore, it promotes international cooperation to define standards of responsible behaviour in cyberspace and establish confidence-building measures that prevent cyber conflicts and promote global stability (Pawlak and Fighel, 2023).

Key initiatives include supporting internet governance through a multi-stakeholder model, strengthening cybersecurity to protect critical infrastructure, and collaborating with third countries to build cybersecurity capabilities. The Council calls for the integration of human rights into cyber policy, ensuring that the principles of freedom of expression and privacy are respected both online and offline. These conclusions reinforce the EU's role as a key player in global debates on cyber diplomacy and set out priorities for building trust and cooperation in cyberspace (Heller, 2023).

4.11 EUROPEAN COMMISSION (2016). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. "STRENGTHENING EUROPE'S CYBER RESILIENCE SYSTEM AND FOSTERING A COMPETITIVE AND INNOVATIVE CYBERSECURITY INDUSTRY (5 JULY 2016)

There is a need to adopt a comprehensive approach to protect European cyberspace against growing threats. This document sets as a priority the improvement of the resilience of critical infrastructure and essential services through the implementation of stricter and more coordinated cybersecurity measures among Member States. It highlights the importance of cross-border cooperation in the prevention, detection and response to cyber threats, as well as the role of tools such as Security Operations Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) in managing incidents effectively and in real time. The Commission also urges Member States to speed up the adoption of the NIS2 Directive, which strengthens cybersecurity requirements across the Union.

At the same time, the Communication highlights the importance of strengthening the cybersecurity industry in Europe as a driver of competitiveness and technological innovation. The Commission advocates for the promotion of research and development in advanced technologies, such as artificial intelligence and blockchain, in the field of cybersecurity, as well as for the establishment of a European digital ecosystem that enables collaboration between businesses, academic institutions and public administrations. In this regard, it recognises the need to overcome the fragmentation of the internal market in cybersecurity and encourages the creation of common standards and certifications that promote trust in technological solutions developed in Europe. This initiative seeks not only to better protect citizens and businesses against cyber threats, but also to position the European Union as a global leader in the cybersecurity industry.

4.12 EUROPEAN COMMISSION (2017). REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL. SIXTH PROGRESS REPORT TOWARDS AN EFFECTIVE AND GENUINE SECURITY UNION. 12 APRIL 2017

The Sixth Progress Report on a Genuine and Effective Security Union, presented by the European Commission, provides a comprehensive analysis of the progress made in implementing the European Union Security Strategy and sets out priorities for consolidating

a safer space for citizens. The report highlights achievements in the protection of critical infrastructure, the strengthening of cybersecurity and the implementation of stricter measures to dismantle organised crime networks and prevent terrorist acts. It also highlights improvements in cross-border police and judicial cooperation, through more efficient information sharing and the use of innovative tools, such as the strengthening of the Prüm framework and Europol's strategic role in joint investigations.

Furthermore, the report highlights the importance of international collaboration, both in the fight against violent extremism and in improving third countries' capabilities to address global threats. It emphasises the EU's role in promoting global security standards and in the transfer of best practices. However, the document cautions about emerging challenges, such as the technological advances of cybercriminals, digital radicalisation and the need to better protect data in an increasingly interconnected digital environment. It therefore highlights the urgent need to maintain a proactive and coordinated approach among Member States, supported by common policies, innovative capabilities and an ongoing commitment to collective security. This approach seeks to ensure not only immediate protection, but also long-term resilience in the face of an ever-evolving threat landscape.

4.13 EUROPEAN COMMISSION (2017). REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL. NINTH PROGRESS REPORT TOWARDS AN EFFECTIVE AND GENUINE SECURITY UNION

The report presents progress towards a genuine and effective Security Union, highlighting measures taken in key areas such as the fight against terrorism, organised crime and cybersecurity. The report underlines the importance of cross-border cooperation and the integration of information systems to strengthen security within the European Union. Furthermore, it highlights the implementation of the European Travel Information and Authorisation System (ETIAS), as well as the strengthening of Europol's European Counter-Terrorism Centre. The report stresses the need for ongoing coordination between Member States to address common threats, improve information sharing and develop security capabilities, ensuring a comprehensive response to emerging security challenges in the region.

4.14 EUROPEAN COMMISSION (2017). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. RESILIENCE, DETERRENCE AND DEFENCE: BUILDING STRONG CYBERSECURITY FOR THE EU.

The Joint Communication to the European Parliament and the Council entitled 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.' highlights the importance of a comprehensive strategy to protect the European digital environment against growing cyber threats. In this document, the European Commission and the European External Action Service stress the need to increase the resilience of critical infrastructure, secure digital supply chains and foster cooperation between Member States. Furthermore, it addresses the crucial role of public awareness and specialist training in ensuring that citizens and institutions understand and implement appropriate cybersecurity measures. Public-private collaboration is also highlighted as essential for the development of innovative solutions that anticipate and respond to emerging risks.

In terms of deterrence, the Communication emphasises the strengthening of both technological and legal capabilities to identify, track and sanction malicious cyber activities. An update to the existing regulatory framework is proposed to enable a more agile and coordinated response at European level. Furthermore, international cooperation is emphasised as a key tool for promoting stability in cyberspace, fostering common standards and collaborations with strategic partners such as NATO and the United Nations. In this

regard, the EU seeks to establish itself as a global actor in promoting a digital environment based on rules and fundamental rights.

Finally, the strategy recognises the need to strengthen the EU's defensive capabilities against advanced cyber attacks. This includes promoting joint projects under the umbrella of Permanent Structured Cooperation (PESCO) and increasing investment in research and development of cutting-edge cybersecurity technologies. Furthermore, priority is given to implementing an approach based on collective intelligence, integrating national capabilities into an interconnected European system. These measures reflect an effort to ensure that cybersecurity is mainstreamed across all Union policies, reaffirming the commitment to protect the values, economy and security of its citizens.

4.15 EUROPEAN COMMISSION (2017). COMMISSION RECOMMENDATION OF 13 SEPTEMBER 2017 ON COORDINATED RESPONSE TO LARGE-SCALE CYBERSECURITY INCIDENTS AND CRISES.

In 2017, the European Commission adopted the Recommendation on the coordinated response to large-scale cybersecurity incidents and crises, marking a milestone in European cybersecurity policy. This document recognised that the exponential increase in cyberattacks, both in frequency and sophistication, demanded a structured and harmonised response at a supranational level. By prioritising cross-border cooperation, the recommendation establishes a framework for managing cyber crises that exceed the individual capacities of Member States, promoting comprehensive resilience at European level. We could highlight this recommendation as one of the most significant to date in terms of collaboration (Negreiro, 2023).

One of the distinctive features of the initiative lies in the integration of the private sector into the cybersecurity ecosystem. Given that most critical infrastructure is managed by private companies, the European Commission emphasised the need for effective and genuine public-private collaboration. In this context, the recommendation proposed strategies to encourage the exchange of sensitive information through secure platforms and mutual trust mechanisms. Furthermore, it highlighted the importance of conducting exercises at regional and European level, not only to strengthen crisis preparedness but also to build joint learning capabilities based on real and simulated incidents.

Finally, this recommendation highlights the need for strengthened trust among Member States, facilitated by technical and procedural interoperability. In this regard, the creation of a common language for cybersecurity was encouraged, enabling national and European authorities to communicate efficiently during critical incidents. This approach aims not only to reduce the impact of cyberattacks, but also to strengthen political cohesion and European digital sovereignty in the face of global threats. In setting out these principles, the European Commission emphasised that a unified defence is essential to ensuring security and prosperity in a digitalised economy.

4.16 EUROPEAN COUNCIL (2017). CONCLUSIONS OF THE EUROPEAN COUNCIL OF 22 AND 23 JUNE 2017.

European leaders emphasise in these conclusions the importance of accelerating the development of the **Digital Single Market (DSM)**, with the aim of removing regulatory barriers, facilitating the free flow of data and fostering innovation in key sectors such as artificial intelligence, e-commerce and the platform economy. They acknowledged that digital transformation is not only essential for economic progress, but also for ensuring social cohesion in a globalised environment where technology is redefining labour, commercial and educational relations (European Council, 2017).

One of the critical issues in this regard is **cybersecurity**, which is viewed as a cross-cutting challenge affecting, once again, both public and private infrastructure. The Council called for the strengthening of national and European cyber defence capabilities, promoting improved cooperation between Member States to prevent, detect and respond to cyberattacks in a coordinated manner. Furthermore, the need to review the existing regulatory framework to adapt it to new digital threats was highlighted, driving initiatives such as the **NIS Directive (Network and Information Security)** and strengthening the role of **ENISA** (European Union Agency for Cybersecurity) as a key player in the protection of European cyberspace.

Furthermore, emphasis was placed on **connectivity and digital infrastructure**, with the aim of ensuring universal access to high-speed networks as an essential prerequisite for global competitiveness. Measures were proposed to promote investment in emerging technologies, including the development of 5G networks, cloud computing and the Internet of Things, elements that will shape the digital ecosystem of the future. In this regard, the Council advocated for the creation of a regulatory environment that fosters innovation, protects citizens' rights in the digital sphere and stimulates job creation in the knowledge economy (European Council, 2017).

5 SPAIN

5.1 THE INFORMATION SOCIETY IN SPAIN IN THE 20TH CENTURY.

The **Information Society in Spain during the 20th** century was characterised by the transition from a socio-economic model based on industrial production to one centred on the generation, management and dissemination of information. This change was driven by the development of **information and communication technologies (ICT)**, which transformed not only the economy but also the country's social, cultural and political structures. With the adoption of the Digital Agenda for Spain, which included specific plans such as the National Plan for Smart Territories, these measures were implemented across almost the entire country.

Although Spain underwent a process of modernisation later than other European countries, the economic opening following the 1970s and 1980s and its incorporation into the **European Union** in 1986 were decisive in accelerating digitalisation and connectivity across various sectors.

During the final decades of the 20th century, the expansion of **personal computing**, the widespread adoption of **internet use** and the consolidation of **mobile telephones** marked fundamental milestones in the development of the Information Society in Spain. During this period, there was exponential growth in the availability of technological infrastructure, facilitated by public policies geared towards digital development and the liberalisation of the telecommunications market in the 1990s. This process not only democratised access to information and networks, but also redefined labour and educational dynamics, enabling the emergence of new professions and business models based on knowledge, transfer and innovation.

The education sector played a crucial role in the consolidation of the Information Society. The gradual introduction of technological resources into the classroom, alongside digital literacy programmes, enabled new generations to become familiar with essential skills for the digital environment. At an institutional level, the promotion of initiatives such as the **Info XXI Plan (2001)** demonstrated the State's commitment to integrating technology into public administration, improving the efficiency of services and promoting **e-government**, laying the foundations for the subsequent evolution towards **digital government** in the 21st century.

However, this process of transformation was not without its challenges. The **digital gap**, both in terms of access and skills, highlighted inequalities between different regions and social groups. Furthermore, rapid technological change raised new challenges relating to **data protection**, cybersecurity and the regulation of the digital environment. In this sense, the 21st century in Spain emerged as a key period of transition, in which society began to adapt to the new paradigm, where information became a strategic resource for primarily economic development, citizen participation and cultural transformation.

5.2 PROTECTION AGAINST CYBERCRIME IN THE FIRST DECADE OF THE 21ST CENTURY.

During the first decade of the 21st century, the expansion of internet use and the digitalisation of numerous sectors led to a significant rise in **cybercrime**, forcing states and international organisations to develop strategies to protect citizens, businesses and institutions. During this period, cybercrime evolved from electronic fraud and attacks on systems to more sophisticated threats, ranging from **phishing** and **malware** to **denial-of-service (DDoS)** attacks. In response, national and international legislative frameworks were strengthened, consolidating mechanisms for the prevention and prosecution of digital crime (Council of Europe, 2001).

In the regulatory sphere, one of the most significant milestones was the adoption of the **Budapest Convention on Cybercrime (2001)**, promoted by the Council of Europe, which established an international legal framework for the criminalisation and prosecution of cybercrime. Spain, along with other countries, incorporated provisions of the convention into its domestic legislation, strengthening the Criminal Code with amendments (to be included) in 2010 to include offences such as **computer intrusion, digital forgery and cyber-espionage**. In addition, specialised units were created within law enforcement agencies, such as the National Police's **Brigada de Investigación Tecnológica** (BIT, Technological Investigation Brigade) and the Civil Guard's **Cybercrime Unit**, with the aim of combating these new threats (ENISA, 2004).

At the institutional level, **cybersecurity** and international cooperation policies were also developed. Bodies such as the **European Union** strengthened their digital security strategies with the creation of **ENISA (the European Union Agency for Cybersecurity)** in 2004, with the aim of coordinating efforts among Member States (ENISA, 2004). Likewise, in Spain, initiatives such as the **Plan Avanza (2005–2010)** (Advance Plan) were launched, which not only promoted digitalisation but also incorporated measures to strengthen protection against cybercrime **(Ministry of Industry, Tourism and Trade, 2005)**. Despite these advances, the evolution of cybercrime over the past decade highlights the need for continuous and timely updates in digital security, laying the foundations, once again, for cyber protection strategies in the 21st century (Clough, 2022).

6 CONCLUSIONS

1. There is a pressing need to step up the implementation of systems for the regular assessment of the impact of the measures adopted, ensuring that strategies remain effective in the face of emerging technological threats. Furthermore, collaboration with third countries and global actors could be strengthened through binding treaties that guarantee uniform standards and firm commitments in the fight against cybercrime. This would enable a greater global response capacity and more shared resources to address the complexities of cyberspace. Another issue worthy of consideration and potential improvement would be the creation of a continuous assessment mechanism to monitor the impact and effectiveness of the EU's cyber diplomacy initiatives. This mechanism would allow strategies to be adjusted in real time in the face of emerging threats and would ensure that objectives are aligned

with international dynamics. Furthermore, the EU could promote the development of binding global standards on cybersecurity, consolidating its position as a leader in promoting a secure cyberspace that respects human rights.

2. Establish a dynamic and continuous evaluation and monitoring framework to measure the impact of the measures adopted. This framework could include key performance indicators (KPIs) on the effectiveness of cyber-resilience strategies, the speed of incident response and technological integration in the public and private sectors. Furthermore, the creation of a centralised European body, specialising in data collection and the issuance of regular reports on the state of cybersecurity in Member States, would ensure a clearer and more coherent overview of progress and areas for improvement.
3. It would be beneficial to encourage greater public-private collaboration through financial incentives and co-investment programmes in research and development of innovative cybersecurity technologies. This approach would not only strengthen the technological capabilities of European companies but would also facilitate the adoption of cutting-edge technological solutions by small and medium-sized enterprises (SMEs), which often lack the resources to implement advanced cybersecurity systems. This would ensure more equitable protection against cyber threats, whilst strengthening the competitiveness of the European digital market.
4. There should be a greater focus on impact assessment. States should incorporate a more detailed analysis of the actual impact of the measures implemented on the security and well-being of European citizens. This could include quantitative and qualitative indicators showing how security policies have affected both public security and individual rights.
5. Implement improvements in communication, transparency and public participation. Include mechanisms to gather and reflect the views of citizens and stakeholders (organisations, institutions, etc.) on security policies, to ensure they are part of the process and that their concerns are objectively addressed to improve these policies.
6. Conduct a more detailed assessment of the availability and effectiveness of the financial, technological and human resources allocated to each security initiative. This would help determine whether resources are being distributed appropriately or whether adjustments are needed.
7. A balance between security and human rights should be ensured, as this is crucial for public acceptance of the measures.

7 REFERENCES

Agencia de la Unión Europea para la Seguridad de las Redes y de la Información (ENISA). (2004). Regulation (EC) No 460/2004 of the European Parliament and of the Council establishing the European Network and Information Security Agency.
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32004R0460

Asamblea General de las Naciones Unidas. (2023, 22 de diciembre). Resolución 78/213: Promoción y protección de los derechos humanos en el contexto de las tecnologías digitales. Retrieved from https://docs.un.org/A/RES/78/213

Bantekas, I., & Stein, M. (2024). International Criminal Law (5th ed.). Cambridge University Press.

Comisión Europea. (2007, 22 de mayo). Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: Hacia una política general de lucha contra la ciberdelincuencia (COM(2007) 267 final).
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52007DC0267

Comisión Europea. (2009, 30 de marzo). Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de las infraestructuras críticas de información: Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, la seguridad y la resiliencia
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52009DC0149

Comisión Europea. (2012, 28 de marzo). Comunicación de la Comisión al Consejo y al Parlamento Europeo: La represión del delito en la era digital: creación de un Centro Europeo de Ciberdelincuencia (COM(2012) 140 final).
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012DC0140

Comisión Europea y Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad. (2013, 7 de febrero). Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Estrategia de Ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52013JC0001

Comisión Europea. (2024, 15 de mayo). Séptimo informe de situación sobre la Estrategia de la Unión de la Seguridad de la UE (2020–2025) (COM(2024) 198 final). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024DC0198(01)

Consejo de la Unión Europea. (1997, 24 de febrero). Acción común 97/154/JAI, de 24 de febrero de 1997, relativa a la lucha contra la trata de seres humanos y la explotación sexual de los niños. Diario Oficial de las Comunidades Europeas, L 63, 2–4.
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31997F0154

Consejo de la Unión Europea. (2000, 29 de mayo). Decisión 2000/375/JAI del Consejo, de 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet. Diario Oficial de las Comunidades Europeas, L 138, 1–4.
https://eur-lex.europa.eu/eli/dec/2000/375/oj

Consejo de la Unión Europea. (2001, 25 de junio). Recomendación del Consejo relativa a los puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia en el ámbito de la alta tecnología. Diario Oficial de las Comunidades Europeas, C 187, 5–6.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001H0703(01)

Consejo de Europa. (2001, 23 de noviembre). Convenio sobre la ciberdelincuencia (Convenio de Budapest). Consejo de Europa.
https://www.coe.int/en/web/cybercrime/the-budapest-convention

Consejo de Europa. (2001, 23 de noviembre). Convenio sobre la ciberdelincuencia (Convenio de Budapest). Consejo de Europa.
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:22001A1123(01)

Consejo de la Unión Europea. (2005, 24 de febrero). Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información. Diario Oficial de la Unión Europea, L 69, 67–71.
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32005F0222

Consejo de la Unión Europea. (2015, 11 de febrero). Conclusiones del Consejo sobre la ciberdiplomacia (ST 6122/15). Consejo de la Unión Europea. https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/es/pdf

Consejo Europeo. (2017, 23 de junio). Conclusiones del Consejo Europeo (22 y 23 de junio de 2017) (EUCO 8/17). Consejo Europeo. https://www.consilium.europa.eu/es/meetings/european-council/2017/06/22-23/

Consejo de Europa. (2022, 12 de mayo). Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (Serie de Tratados del Consejo de Europa, n.º 224). Consejo de Europa.
https://www.coe.int/en/web/cybercrime/second-additional-protocol

Council of Europe. (2025). The Budapest Convention on Cybercrime: benefits and impact in practice. Strasbourg: Cybercrime Programme Office. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR), 8, 169–203. https://doi.org/10.18172/redur.4071

European Union Agency for Cybersecurity (ENISA). (2020). Artificial Intelligence Cybersecurity Challenges. ENISA.
https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

European Union Agency for Cybersecurity (ENISA). (2022). European Cybersecurity Skills Framework (ECSF). ENISA.
https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

Gobierno de España. Ministerio de Ciencia y Tecnología. (1999). Plan Info XXI: La sociedad de la información para todos. Gobierno de España.
https://www.boe.es/buscar/doc.php?id=BOE-A-2000-1546

Gobierno de España. Ministerio de Ciencia y Tecnología. (2001). El plan de acción Info XXI: La sociedad de la información para todos.
Retrieved from https://avance.digital.gob.es/programas-avance-digital/DescargasPrimerasIniciativas/2001-Plan-InfoXXI.pdf

Heller, D. (2023). "The EU Cyber Diplomacy Toolbox: Ten Years of Evolution from Brussels' Conclusions to Sanctions". European Foreign Affairs Review, 28(2), 115-138. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf

Ministerio de Industria, Turismo y Comercio. (2005). Plan Avanza 2006–2010. Gobierno de España.https://avance.digital.gob.es/programas-avance-digital/DescargasPlanesAvanza/Plan%20Avanza/plan_avanza-Documento_completo.pdf

Negreiro, M. (2023). "The EU's Path Towards a Cyber Solidarity Act: Building on the 2017 Blueprint". European Parliamentary Research Service.

Oficina de las Naciones Unidas contra la Droga y el Delito. (2021). Compendio de delincuencia organizada y ciberdelincuencia. Naciones Unidas. Retrieved from https://www.unodc.org/documents/Cybercrime/publications/compendio_de_delincuencia_organizada_es.pdf

Parlamento Europeo y Consejo. (1999, 25 de enero). Decisión nº 276/1999/CE por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes. Diario Oficial de las Comunidades Europeas L 33, 1–11. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31999D0276

Pawlak, P., & Fighel, J. (2023). Cyber Diplomacy: Governance and Conflict in Cyberspace. Oxford University Press.

Ramos, J. M. (2016). Análisis y respuesta de las fuerzas y cuerpos de seguridad ante el fenómeno de la pornografía infantil en la Red. Tesis Doctoral, Universidad de las Palmas de Gran Canaria. https://accedacris.ulpgc.es/bitstream/10553/24768/4/0740277_00000_0000.pdf

Sieber, U. (2022). Strafrechtliche Verantwortlichkeit im. Max Planck Institute for the Study of Crime, Security and Law.

Villegas García, M. Á., & Encinar del Pozo, M. Á. (2023). Los ciberdelitos en la jurisprudencia del Tribunal Supremo. Diario La Ley, Nº 10283. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=8934530