



INTERNATIONAL INSTITUTE FOR PRIVATE
COMMERCIAL AND COMPETITION LAW
(IIPCCCL - AUSTRIA)

Research Article

© 2025 Manjola Kajana & Sotir Kllapi

This is an open access article licensed under the Creative Commons
Attribution-NonCommercial 4.0 International License

[\(https://creativecommons.org/licenses/by-nc/4.0/\)](https://creativecommons.org/licenses/by-nc/4.0/)

Challenges and directions of Albanian criminal policy towards cybercrimes

Manjola Kajana

Special Prosecution Office against Corruption and Organised Crime, Tirana Albania

Sotir Kllapi

Special Prosecution Office against Corruption and Organised Crime, Tirana Albania

DOI: <https://doi.org/10.2478/bjir-2025-0027>

Abstract

Cybercrimes nowadays are becoming an increasingly worrying phenomenon, as their number and complexity are constantly increasing. This is closely related to the fact that modern society is developing in a digital age, where technology evolves at a rapid pace and encompasses every aspect of economic, social, and institutional life. As a result, Albania's Criminal Code has also undergone significant changes, in order to adapt to new forms of criminality that occur in the virtual space. Being new criminal offenses, not only the way these provisions are applied in practice is of interest, but also the criminal policy pursued by the criminal procedure authorities, mainly the prosecution and the court. This paper provides an analysis of the Albanian criminal policy in the field of cybercrimes, based on the statistical data reported for the years 2023 and 2024. The analysis shows a clear fragmentation of the implementation of legal provisions; some provisions are practically unimplemented, such as those related to the distribution of racist or xenophobic materials and insults with discriminatory motives, while some others have a limited application, such as cases of racially motivated intimidation and illegal data sharing. Criminal offenses related to interference with data and computer systems show a high frequency of proceedings, but with minimal court results, highlighting challenges in the technical examination, lack of digital expertise and inter-institutional cooperation. On the other hand, fraud and computer forgery show a more stable and efficient implementation, due to the direct economic impact that drives denunciation and investigation. Transitional provisions, such as unauthorized computer access, begin to yield concrete results with penalties identified for the first time. The study highlights the need to strengthen investigative and judicial capacities, as well as for a more integrated and effective criminal policy approach to cybercrimes in Albania.

Keywords: cybercrime, criminal policy, technology, criminal offense, statistical data.

1. Introduction

Cybercrimes represent one of the most widespread crime phenomena today, due to the rapid development of technology and the creation of a great dependence on the internet. Their genesis dates back to the 1970s–1980s, when computers began to be used on a larger scale and the first cases of unauthorized intrusion into computer systems, known as “hacking”, appeared. Over the 90s, the spread of the internet brought more sophisticated forms of cybercrime, such as the spread of viruses, online fraud, and identity theft. After the 2000s, the development of social networks and electronic payments increased the scale of these crimes, turning them into a threat to the international economy and security.

Another practical problem remains the lack of a universal definition of cybercrimes; due to the rapid pace of technological development, different methods and tactics arise for committing these crimes, but the use of computer systems as a means of committing them remains common. According to INTERPOL,¹ it represents one of the most widespread forms of international crime. UNODC² defines it as criminal activity where a computer or network is the source, means, object or place of committing a crime. The European Union Agency for Cybersecurity (ENISA)³ emphasizes that cybercrime includes illegal actions aimed at harming, interfering with, or taking advantage of computer systems and digital networks. While the OECD⁴ defines it as any illegal act carried out using information and communication technologies to cause economic harm, privacy violations, or interference with other computer systems. These definitions clearly show that cybercrime is not limited to data theft, but involves a wide range of illegal activities in the digital space.

In Albanian Criminal Code, but not only, also in international acts — for example, in the Convention on Cybercrime, otherwise known as the Budapest Convention (hereinafter) — cybercrimes are foreseen and regulated. Albania ratified the Convention in 2002 and has undertaken significant legal and institutional reforms to comply with its requirements. The Convention continues to be a reference document for developments in international criminal law in the face of the ongoing challenges posed by cybercrime.

The convention encompasses four main areas: (1) infringements directly related to computer systems (such as unauthorized access, data tampering, and systems tampering), (2) content-related crimes, such as online child pornography, (3) computer data-related crimes (such as computer forgery and computer fraud), and (4) procedural provisions for investigating and gathering evidence in a digital

¹ INTERPOL, ‘Cybercrime’ <https://www.interpol.int/Crimes/Cybercrime> [accessed 18 October 2025].

² United Nations Office on Drugs and Crime (UNODC), ‘Guidance Note on Cybercrime’ https://www.unodc.org/documents/organized-crime/Guidance_Note_on_Cybercrime_5_January_2010.pdf [accessed 18 October 2025].

³ European Union Agency for Cybersecurity (ENISA), ‘Home’ <https://www.enisa.europa.eu/> [accessed 18 October 2025].

⁴ Organisation for Economic Co-operation and Development (OECD), ‘Digital Security’ <https://www.oecd.org/en/topics/digital-security.html> [accessed 18 October 2025].

environment. A very important aspect of the convention is international cooperation, recognizing the cross-border nature of cybercrime and the need for a coordinated response between states. The Budapest Convention has served as a model for many countries outside Europe, including the United States, Japan, Canada, and the Western Balkan countries, which have signed or harmonized their legislation under it. Subsequently, the Criminal Code of the Republic of Albania has undergone several significant changes to include criminal offenses related to unauthorized interference with computer systems, data theft, electronic sabotage and fraud through IT tools. Article 192/b and other relevant articles have been added or improved to bring Albanian legislation into line with international standards, in particular with the Budapest Convention on Cybercrime, which Albania ratified in 2002. The momentum of the development of mass communication in cyberspace, especially after the 2000s, is orienting Albania towards a new problem that threatens national security, cyber warfare and computer crimes (Security Academy, 2018).

2. Provisions of the Criminal Code of the Republic of Albania for crimes in the cyber field

The Criminal Code is not the only regulatory framework for cybercrimes in Albania. In addition to it, the Constitution of the Republic of Albania, which guarantees fundamental human rights and freedoms, including the protection of privacy and personal data in the digital environment, is of particular importance. Also, Law No. 25/2024 "On Cyber Security" is an important legal instrument that defines the principles, responsible structures and measures for the protection of information systems of particular importance. This law aims to strengthen national cyber security and provides mechanisms for the prevention, detection and response to cyber incidents.

In this context, the National Agency for Electronic Certification and Cyber Security (AKCESK), which is the institution responsible for the supervision, coordination and implementation of national policies in the field of cyber security, also plays a special role. AKCESK has competencies in monitoring cyber incidents, providing technical assistance to public and private institutions, as well as raising security standards in accordance with international legislation and European Union best practice.

An essential characteristic of cybercrimes, as explained above in this paper, is the fact that they are carried out through the use of computer systems and computer data. Before moving on to the analysis of criminal offences in this area, it is necessary to present some basic definitions provided by the Budapest Convention "On Cybercrime", specifically in Article 1 thereof. This Convention clearly defines some key terms, in order to create a common basis of meaning among the participating states. According to it, "computer system" means any device or group of interconnected devices, one or more of which continuously perform automatic data processing through a computer program.

In the same vein, "computer data" represents any expression of facts, information

or concepts in a form suitable for processing by a computer system, including the programs necessary for its operation. Also, “service provider” means any public or private entity that provides communication services through a computer system, as well as any other entity that processes or stores computer data in function of this service. Finally, “traffic data” is computer data related to communication through a computer system, which is produced by the system that represents a link in the communication chain and that indicates elements such as origin, destination, route, time, date, size, duration or type of service used.

Criminal offenses in the field of cybercrime in the Criminal Code of the Republic of Albania constitute a broad system of norms that protect public order, national security and personal data from abuses in the digital space. For the purpose of sharing and facilitating their analysis, we have made a classification of them as follows:

First, among the criminal offenses related to cybercrimes, those related to the dissemination of illegal or prohibited materials stand out. This category includes “Computer distribution of pro-genocide or crimes against humanity materials”, provided for by Article 74/a of the Criminal Code, as well as “Pornography”, provided by Article 117 of the Criminal Code. Article 74/a – Computer distribution of pro-genocide or crimes against humanity materials prohibits the use of computer systems for the distribution of materials that incite, justify or promote genocide and crimes against humanity. The purpose of this article is to prevent the use of the internet as a propaganda tool for criminal purposes, protecting public order, human dignity and social peace. Article 117 – Pornography provides for the punishment of the production, distribution and publication of materials with pornographic content, especially when children or minors are involved. In the context of cybercrimes, this article also includes forms of dissemination on the Internet, through websites, social networks, digital platforms or other electronic means that enable the circulation of such content widely and anonymously.

Second, the offences related to incitement to hatred and discrimination online, constitute a special category of cybercrimes. These works aim to protect the individual and the social order from the spread of hate speech, discrimination and intolerance in the digital space. The Criminal Code provides for several articles that specifically address this form of harmful behavior on the Internet. Article 84/a – Racist and xenophobic intimidation through a computer system includes threats and intimidation that are carried out electronically for racial, ethnic, religious or national reasons. Article 119/a – The dissemination of racist or xenophobic materials through the computer system punishes any form of publication, distribution or online communication of materials that incite hatred, division or discrimination on racial, ethnic or religious grounds. Article 119/b – Insult with motives of racism or xenophobia through the computer system include cases of insults, humiliation or verbal attacks on the Internet that are based on discriminatory motives.

Third, the offences related to the security and integrity of computer systems, constitute one of the most essential categories of cybercrimes. These works aim to protect the digital infrastructure, data and the operation of the system from illegal and harmful

interventions. The Criminal Code provides for several articles that address these violations in detail. Article 137/a – Theft of the electronic communications network consists of the unauthorized use of communication networks (such as internet, Wi-Fi, mobile networks), causing economic or technical damage. Article 192/b– Unauthorized computer access punishes any unauthorized access to a computer system, regardless of whether damage is caused or not. This is one of the basic offences of cybercrime and corresponds to Article 2 of the Budapest Convention (“access to the right”). Article 293/a – Illegal interception of computer data punishes the intervention without authorization to intercept or monitor data circulating through computer systems. Article 293/b – Interference with computer data consists of deleting, altering or damaging computer data without authorization. This includes virus, malware, or ransom attacks that damage databases and the normal functioning of systems. Article 293/c – Interference with computer systems differs from interference with data because it affects the system itself, hindering, damaging or paralyzing its operation. In international terminology, this is equivalent to Denial of Service (DoS). Article 293/ç – Misuse of equipment provides for the punishment for the production or distribution of means (software, equipment) that can be used to commit the above offenses. This article has a preventive character, as it also punishes the preparation for an attack and the potential use of means for criminal purposes.

Fourth, there are the offences related to digital fraud and forgery, which have a direct impact on the ownership, property and economic security of individuals and entities. These crimes are carried out through the use of computer systems and comply with the international provisions of the Budapest Convention. Article 143 – Computer fraud punishes the use of computer systems to gain wealth or harm someone financially, by manipulating online data or transactions. This article corresponds to Article 8 of the Budapest Convention and aims to prevent economic crimes in the digital environment. Article 186/a – Computer forgery includes the creation, alteration or use of false computer data for the purpose of fraud. This article is closely related to electronic fraud and digital economic crimes, aiming to protect the reliability of the system and online information.

Overall, the Albanian legislation is harmonized with European and international standards, providing a broad legal basis for the prevention and punishment of crimes in cyberspace.

3. Criminal Policy for Criminal Offenses in the Field of Cybernetics for 2023 and 2024

Cybercrimes account for a small portion of total criminal proceedings, yet show interesting changes during 2023–2024. The crime rate per 100,000 inhabitants was 11.30 in 2023, while in 2024 it has increased to 12.61, indicating a slight increase in cyber activity in relation to the population. The number of registered proceedings has decreased by 2,88% in 2024 compared to 2023, but proceedings sent to court have marked a significant increase from 10 to 19 cases, or 90%, indicating a greater

commitment of the authorities to prosecute these offenses. The number of registered defendants has decreased from 20 to 16 cases, or 20%, while the number of defendants sent to court has increased significantly from 16 to 59, or 3.7 times more, reflecting a greater focus on effective prosecution. The number of convicted defendants has increased from 9 to 11 cases, or 22.22%, indicating an improvement in the conviction rate for computer crimes. Although the number of registered proceedings has decreased slightly, the data show a greater focus on prosecution and conviction of perpetrators, reflecting improvements in criminal policy and institutional engagement on cybercrimes during 2024.

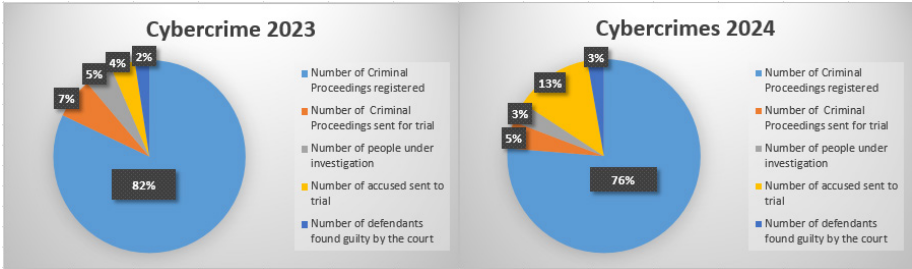
Based on the official reports of the General Prosecutor's Office for 2023, cybercrimes have marked a significant activity, although some categories of offenses remain few or unrepresented. In total, 366 criminal proceedings have been registered, of which 30 have been sent to court, and 11 people have been convicted.

Cybercrimes 2023	Number of Criminal Proceedings registered	Number of Criminal Proceedings sent for trial	Number of people under investigation	Number of accused sent to trial	Number of defendants found guilty by the court
Article 74/a Computer Distribution of Pro-Genocide or Crimes Against Humanity Materials	0	0	0	0	0
Article 84/a Intimidation with motives of racism and xenophobia through the computer system	0	0	0	0	0
Article 117 Pornography	51	2	1	2	2
Article 119/a Distribution of racist or xenophobic materials through the computer system	0	0	0	0	0

Article 119/b Insulting with motives of racism or xenophobia through the computer system	0	0	0	0	0
Article 137/a Theft of the electronic com- munications network	3	0	0	0	0
Article 143/b Computer Fraud	110	5	14	11	3
Article 186/a Computer Forgery	95	4	6	4	6
Article 192/b Unauthorized computer ac- cess	20	1	-	1	-
Article 293/a Illegal inter- ception of computer data	1	0	0	0	0
Article 293/b Interference with computer data	82	0	0	0	0
Article 293/c Interference with computer systems	3	0	0	0	0
Article 293/ ç Misuse of equipment	1	0	0	0	0
TOTALS	366	30	21	18	11

The data on cybercrime proceedings are based on the reports of the General Prosecutor's Office on the state of criminality in 2023 and 2024. From the analysis of these reports, it results that the highest number of proceedings registered for this group of offenses is evident in the prosecutions at the courts of first instance. The Prosecutor's Office at the Court of First Instance in Tirana has registered 65% of the total number of proceedings for these offenses; while in Vlora 9% of the proceedings

have been registered. The lowest number of proceedings is evident in Shkodra, Saranda, Dibra and Gjirokastra, where 1% of the number of proceedings at the national level were registered, respectively. No proceedings have been registered in Kukës for these offenses. These data are based on the official information of the General Prosecutor's Office and reflect the crime situation for the years 2023 and 2024.



Cybercrimes 2024	Number of Criminal Proceedings registered	Number of Criminal Proceedings sent for trial	Number of people under investigation	Number of accused sent to trial	Number of defendants found guilty by the court
Article 74/a Computer Distribution of Pro-Genocide or Crimes Against Humanity Materials	0	0	0	0	0
Article 84/a Intimidation with motives of racism and xenophobia through the computer system	3	0	0	0	0
Article 117 Pornography	51	2	1	2	2
Article 119/a Distribution of racist or xenophobic materials through the computer system	1	0	0	0	0

Article 119/b Insulting with motives of rac- ism or xeno- phobia through the computer system	0	0	0	0	0
Article 137/a Theft of the electronic com- munications network	2	0	0	0	0
Article 143/b Computer Fraud	89	7	9	46	7
Article 186/a Computer Forgery	105	9	5	10	3
Article 192/b Unauthorized computer ac- cess	7	2	0	2	1
Article 293/a Illegal intercep- tion of com- puter data	2	0	1	0	0
Article 293/b Interference with computer data	84	0	0	0	0
Article 293/c Interference with computer systems	12	1	0	1	0
Article 293/ ç Misuse of equipment	1	0	0	0	0
TOTALS	357	21	16	61	13

The socio-demographic data of the defendants for the analyzed group of criminal offenses, including gender, age, education, social status, place of residence and judicial status, are presented as follows:

- Gender: 82.76% of the defendants are male and 17.24% female.
- Education: 34.48% of the defendants have secondary education, 31.04% have higher education, and 34.48% have education up to the 9-year level.

- Residence: 82.76% live in the city and 17.24% in rural areas.
- Judicial status: 90.32% of the defendants have not been convicted before, while 9.68% are repeated offenders for various criminal offenses.

From the data analysis, it results that the profile of the defendants for cybercrimes shows that 82.76% are men, 31.04% have higher education and 90.32% have not been convicted before. Regarding the geographical distribution, the highest number of proceedings was registered in the Prosecutor's Office at the Court of First Instance of Tirana (65%), while the highest coefficient per 100,000 inhabitants results in the Prosecutor's Office at the Court of First Instance of Vlora with 28 proceedings and in Tirana with 26 proceedings. Regarding the criminal policy, in all cases the prosecutor has requested a prison sentence and the court has also imposed a prison sentence. As for the measure of the sentence, in 16.67% of the cases the suspension of the sentence and placement on probation was requested, while the court applied this measure to 9.09% of the defendants; for 8.33% of the cases the minimum sentence was requested, and the court decided it for 9.09%; while for 75% of the defendants the sentence was required in the average margin provided by the provision, and the court decided it for 81.82%. Regarding public security, the number of suspended proceedings for 2024 was 211, or 65.64% of the registered proceedings, compared to 63.46% in 2023.

4. Analysis of the problems and criminal policy on crimes in the field of cybercrime

Statistical data obtained from the annual reports on the state of crime for the years 2023 and 2024 provide a clear picture on how the Albanian criminal policy works in dealing with cybercrimes. Although Albanian legislation includes a wide range of provisions in line with international standards, their practical implementation and effectiveness remain limited. This shows that there is a noticeable gap between the legal norm and the judicial reality.

4.1 Provisions with lack of practical implementation

Criminal offenses related to the distribution of racist or xenophobic materials (Articles 74/a, 119/a, 119/b) as well as those sanctioning insults with discriminatory motives, result without any cases registered during the last two years. This shows that these provisions mainly have a harmonizing function with international conventions, but their implementation in practice is lacking. Although the phenomenon of online hate speech is present in the Albanian reality, the mechanisms of investigation and denunciation do not work effectively.

4.2 Provisions with limited application

Cases related to intimidation with racist or xenophobic motives (Article 84/a) first appeared in 2024 with three proceedings registered, but without any referral to court. Likewise, offences involving illegal data transfer (Article 293/a) and misuse of equipment (Article 293/c) remain almost unimplemented. This shows that the criminal policy in this area is more declarative and preventive, rather than punitive

and effective.

4.3 High-incidence but low-efficiency provisions

Interference with data and computer systems (Articles 293/b and 293/c) is one of the biggest challenges in Albanian criminal practice. During 2023, 82 cases of data interference and 3 in systems were registered, while in 2024 the figures increase to 84 and 12, respectively. However, only one case has been sent to court, and none has ended in conviction. This situation shows the technical difficulties in providing digital evidence, the lack of professional expertise and the weakness of inter-institutional cooperation between investigative bodies.

4.4 Provisions with sustainable implementation

Computer fraud (Article 143/b) and computer forgery (Article 186/a) are two of the most widespread and punished offenses in Albanian practice. In 2023, 110 cases of fraud and 95 cases of forgery were registered, while in 2024, 89 and 105 cases respectively. These are among the few offenses that have brought concrete results in criminal prosecutions: in 2024, computer fraud brought 46 defendants and 7 convictions, while computer forgery brought 10 defendants and 3 convictions. The highest effectiveness in these cases is related to the fact that they directly affect financial interests and cause measurable damages, which encourages denunciation and engagement of justice bodies.

Recently, there has been noticed the commission of "Computer Fraud "criminal offence in an organized manner, in the form of special collaboration, such as an organized criminal group. It has been noted that these fraud schemes are also carried out by companies specifically created for this purpose, which manage platforms created specifically for committing this criminal activity. Such as "Absolut Global Markets," "Aurum pro," and "Finaxis," etc. Through these platforms, using so-called call centers, in Albania, North Macedonia, Ukraine, and Georgia, citizens, mainly from EU countries, are deceived with fictitious investments. Only in the investigations that SPAK has initiated for the year 2024, it is suspected that the economic damages caused by this criminal activity to victims in EU countries may exceed the value of 6 million Euros.⁵

Since 2021 onwards, there has been an increasing number of recorded proceedings, prosecuted individuals, as well as convicted persons. These criminal proceedings, for which prosecution has been carried out by the Special Prosecution Office in Albania, have been successful due to the fact that most of the victims were foreign citizens. Consequently, there has been an increasing interest from foreign law enforcement agencies, including Europol and Eurojust, who have assisted the investigation in Albania not only with ongoing criminal information but also with essential technical issues for investigating these criminal acts. In this regard, it is worth highlighting the creation of several joint investigation teams (JITs) with the judicial authorities

⁵ For more see the SPAK Annual Report 2024, <https://spak.gov.al/wp-content/uploads/2025/04/Raporti-vjetor-SPAK-2024.pdf>.

of EU countries, as well as the coordination of investigative activity, which has significantly influenced the gathering of evidence, its management in real time, and the punishment of this phenomenon.

4.5 Provisions in transition phase

Unauthorized access to computer systems (Article 192/b) represents a downward trend of proceedings – from 20 in 2023 to only 7 in 2024 – but for the first time a conviction was recorded in 2024. This development shows that while this deed remains difficult to prove, justice systems are starting to deliver the first concrete results. From the data analysis, it emerges that the Albanian criminal policy in the field of cybercrimes is still developing and presents a fragmented nature:

- Effective in cases that affect financial and economic interests (fraud and computer forgery);
- Weak and mostly symbolic in the works related to hate speech, illegal seizure and misuse of equipment;
- In transition for offenses related to unauthorized access and interference with computer systems, where although the number of proceedings is high, the court results are still low;

5. Conclusion

From the analysis of the data and the Albanian criminal policy in the field of cybercrimes, it can be concluded that the existing legislation, although harmonized with international standards, continues to lack effectiveness in practical implementation. There is a marked contrast between the broad legal basis and the limited judicial outcomes, which points to structural and institutional difficulties in investigating and prosecuting these offences. The Albanian criminal policy is more functional in cases related to financial and economic damages, such as fraud and computer forgery, while it remains mainly declarative for offenses that affect the freedoms and rights of the individual, such as hate speech or illegal alienation. Technical deficiencies in the provision of digital evidence, lack of professional expertise, and insufficient cooperation between institutions constitute major obstacles to effective law enforcement. However, the presence of some positive results in penalties for unauthorized access to systems indicates a gradual trend for improvement. In order to increase the efficiency of criminal policy in this area, a more coordinated inter-institutional approach, investment in technical capacities and the development of case law through model decisions that would enable sustainable interpretation and more effective application of criminal norms is required.

References

Additional Protocol to the Convention on Cybercrime on the penalization of acts of a racist and xenophobic nature, approved by the Council of Europe, ratified by Albania with Law No.

9262, dated 29 July 2004, ETS 189, in force from 1 July 2004.

Constitution of the Republic of Albania, approved by Law No. 8417, dated 21.10.1998, FZ No. 28, dated 07.12.1998, amended by laws: No. 9675, dated 13.01.2007, FZ No. 2, dated 14.01.2007; No. 9904, dated 21.04.2008, FZ No. 61, dated 07.05.2008; No. 88/2012, dated 18.09.2012, FZ No. 132, dated 10.10.2012; No. 137/2015, dated 17.12.2015; No. 76/2016, dated 22.07.2016, FZ No. 138, dated 27.07.2016; No. 115/2020, dated 30.07.2020, FZ No. 153, dated 05.08.2022; No. 16/2022, dated 10.02.2022.

Convention on Cybercrime, adopted by the Council of Europe, ratified by Albania by Law No. 888, dated 25 April 2002, ETS 185, in force from 1 July 2004.

Criminal Code of the Republic of Albania, Law No. 7895, dated 27 January 1995, amended by Laws No. 8175/1996, No. 8204/1997, No. 8279/1998, No. 8733/2001, No. 9017/2003, No. 9030/2003, No. 9086/2003, No. 9188/2004, No. 9275/2004, No. 9686/2007, No. 9859/2008, No. 10023/2008, No. 23/2012, No. 144/2013, No. 98/2014, No. 176/2014, No. 135/2015, No. 82/2016, No. 36/2017, No. 89/2017, No. 44/2019, No. 35/2020, No. 146/2020, and No. 43/2021; and with reference to the decisions of the Constitutional Court No. 13/1997, No. 46/1997, No. 58/1997, No. 65/1999, No. 11/2008, No. 19/2011, No. 47/2012, No. 9/2016, No. 24/2021, and No. 20/2024. European Union Agency for Cybersecurity (ENISA), "Home". Available at: <https://www.enisa.europa.eu/> [Accessed 18 October 2025].

General Prosecutor's Office of the Republic of Albania, Report of the Prosecutor General on the State of Criminality in Albania for 2024, Tirana, March 2025. Available at: https://www.pp.gov.al/rc/doc/Raporti_PP_2024_permbledhes_28_03_2025_7729.pdf [Accessed 25 October 2025].

General Prosecutor's Office of the Republic of Albania, Report of the Prosecutor General on the Crime Situation in Albania for 2023, Tirana, 28 March 2024. Available at: https://www.pp.gov.al/rc/doc/Raporti_1_PP_2023_date_28_03_2024_7383.pdf [Accessed 25 October 2025]. INTERPOL, "Cybercrime". Available at: <https://www.interpol.int/Crimes/Cybercrime> [Accessed 18 October 2025].

Law No. 25/2024, "On Cyber Security".

Organisation for Economic Co-operation and Development (OECD), "Digital Security". Available at: <https://www.oecd.org/en/topics/digital-security.html> [Accessed 18 October 2025].

United Nations Office on Drugs and Crime (UNODC), Guidance Note on Cybercrime, 5 January 2010. Available at: https://www.unodc.org/documents/organized-crime/Guidance_Note_on_Cybercrime_5_January_2010.pdf [Accessed 18 October 2025].