The17th Year Publication, No.1

June 2025

THE IMPACT OF DIGITALIZATION ON THE LEGAL PROTECTION OF VICTIMS OF CYBERCRIME: A CRITICAL ANALYSIS AND PERSPECTIVES FOR ALBANIA

Gerta Gjeta*; Ermira Biba**

*Albanian University, Tiranë

Abstract

In an increasingly digitalized society, where social, economic, and institutional interactions are shifting to the virtual sphere, cybercrime has become a major challenge for criminal justice and the protection of individuals' fundamental rights.

This paper analyzes the impact of digitalization on the legal protection of victims of cybercrime, by examining the transformation of the nature of crime, the new forms of victimization, and the legal challenges arising from these developments.

Relying on a theoretical and comparative analysis methodology, the paper identifies gaps in the current protection of victims at both the European and national levels, and critically addresses the limitations of the traditional punitive model in the context of digital crime.

Within this framework, alternatives are proposed for building a new model of protection, based on integrated assistance, harm restoration, and the guarantee of victims' rights, inspired by the most advanced models of the European Union.

The paper concludes with concrete recommendations for adapting the Albanian system to the new challenges of cybercrime, highlighting the need for institutional, legal, and social reforms to ensure the effective protection of fundamental rights in the digital age.

Keywords: *Cybercrime, victim protection, digitalization, restorative models and victim assistance, Albania*

1. Introduction

In a society that is becoming increasingly digitalized each day; in this world where social, economic, and institutional relationships are shifting toward the virtual realm, cybercrime has become a challenging issue for criminal justice and the protection of basic individual rights. As technology has rapidly transformed the world, unleashing a wealth of benefits on one hand, it has also created a new space where crime can operate, undermining traditional understandings of crime, authorship, and the locus of the criminal act. *(McGuire, 2021).*

In this transformed context, victims of cybercrime face a range of new and potentially harmful effects that go beyond financial losses, including serious harm to privacy, personal integrity, and psychological well-being. *(Yar, 2013).* Compared to conventional criminal acts, these offenses can be committed anonymously, globally, and at a speed that surpasses the response capacity of current legal protections *(Broadhurst, 2006).* This raises an important need to redefine the idea of victim protection in the era of digital risk. As

Bélanger and Crossler (2021) emphasize, the protection of privacy and rights in cyberspace are among the most multi-dimensional challenges of contemporary law, which require an essentially more unique and networked cooperation within and between criminal legislation, privacy rights, and human rights. And these challenges are not only academic. The digitalization of public services and the increase of online interactions in Albania have exposed citizens to a wide range of cyber risks, and the legal-institutional infrastructure for victim protection still needs to be developed. For example, although Albania has signed the Budapest Convention and has adopted a comprehensive legal framework as a supporting instrument for the national cybersecurity architecture, the lack of effective tools and support in terms of reporting, psychological and legal assistance for victims still creates a substantial gap in practice.

Taking this scenario into account, this article aims to elaborate on a critical analysis of the treatment of cybercrime victims, by addressing:

- The developments of the digital criminal phenomenon,
- The response of widespread legal systems,
- And the need to build a new tool for security and the protection of human rights.

In function of this study, the following research questions are posed:

What are the key differences or similarities in victimization between cybercrime and traditional crime, particularly with regard to the structural aspects of the offenses?

What are the most significant gaps within the existing laws and practices both at the international and Albanian level in ensuring effective protection for victims of cybercrime?

How can a more effective legal and institutional framework be developed to ensure comprehensive protection for victims in the digital age?

By applying such a comparative analysis, this paper seeks to enrich and establish a more advanced conceptual and practical platform for the protection of cybercrime victims, balancing international experience with the specific challenges and realities of the Albanian context.

Methodology:

The approach adopted in this paper includes theoretical, analytical, and comparative methods, aiming to critically and thoroughly understand the challenges posed by the phenomenon of cybercrime to the protection of victims, both globally and within Albania. The primary technique employed is a theoretical-normative analysis, conducted through the examination of the most recent academic literature on cybercrime, criminal law, victims' rights, and digital privacy. Within this framework, the study considers theoretical constructs, normative models, and current trends related to the nature of cybercrimes and victimization.

In addition, the comparative paradigm has been used to examine the similarities and to develop the differences between international instruments for the protection of victims of digital economy crimes and what we have so far in Albania. This comparison is made with the aim of identifying the current problems in Albanian legislation and suggesting convergences with the highest international standards. In that context, the article relies primarily on modern academic sources, international instruments including the Budapest Convention and Directive 2012/29/EU, as well as analytical reports from international organizations such as ENISA, Europol, and the European Union Agency for Fundamental Rights (FRA).

2. The Theory of Cyber Victimization and Cybercrime

Technological changes and the digitalization of modern society are creating a favorable environment for the development of new forms of crime, undermining the very foundations of criminal justice. In this environment, cybercrimes have evolved as a new dimension a unique and rapidly changing form of contemporary crime with wide-ranging consequences for the citizens' social, economic, and personal lives.

In this section, we will examine the concept of cybercrime and its impact on victims, as well as the challenges it presents for the modern legal system, and we will conduct a comparative analysis of the situation in Albania and the experiences of other countries.

2.1 The Concept of Cybercrime and Its Fundamental Characteristics

In contemporary literature, cybercrimes are defined as illegal acts committed through or against information technology systems, targeting computer systems, digital data, or individuals exposed in the virtual space. *(Wall, 2022).*
Brenner (2010) identifies four characteristics that distinguish cybercrimes from traditional criminality: the anonymity of perpetrators, the globalization of the operational space, the ease of reproducing the offense, and the difficulty in gathering evidence. These characteristics significantly alter the way crime is conceptualized, investigated, and punished, challenging the traditional importance of factors such as physical location, direct contact, and material evidence.
Broadhurst (2006) emphasizes that, due to the cross-border nature of cybercrimes, traditional procedures of international cooperation often prove to be slow and ineffective, complicating the prosecution and punishment of offenders.

2.2 The Victim in the Digital World and New Forms of Victimization

Furthermore, in an effort to understand the social component of cybercrime, Yar (2013) argues that such criminal behaviors cause a new type of victimization that is not necessarily linked to physical or material harm. In the digital world, hate speech can lead to mental and social health effects, where the loss of privacy, reputation, and personal dignity is preserved over time, affecting the emotional balance of victims. Phenomena such as revenge porn, phishing, exploitation of personal data, and online blackmail reveal a form of victimization that is neither spatial nor temporal, but can extend globally and without time limits. Individually, in assessing the consequences caused by these crimes, the damage is not only economic, but also includes very serious emotional and social harm, ultimately constituting one of the defining features of a phenomenon that becomes a new reality for its victims.

2.3 Challenges in the Legal Protection of Cybercrime Victims

The legal protection of cybercrime victims faces numerous systemic and conceptual challenges. According to Bélanger and Crossler (2011), in the era of digital society, the concept of privacy holds a fragile position, and its violations can have lasting effects on an individual's social, emotional, and economic life. The goal of developing effective protection at the international level can be seen, for example, in the adoption of instruments such as the General Data Protection Regulation (GDPR) 2016 and Directive 2012/29/EU on victims' rights. However, the implementation of these standards remains unequal and partial across EU Member States (European Union Agency for Fundamental Rights, 2021).
In Albania, efforts have been made to align legislation with that of Europe, including the adoption of Law no. 2/2017 "On Cybersecurity" and related regulations within the Criminal Code. However, the protection of digital crime victims remains weak. There are no concrete mechanisms in place to provide legal or psychological support for trauma. In the real world, there are no specific centers to assist victims of digital crimes, and the point of contact with victims is fragmented and not known by the public.
Without appropriate institutions such as the Internet Ombudspersons mentioned by McGuire (2021) "the digitalization of society far from being a tool to help, protect, and expand individual rights seems far more likely to introduce yet another layer of dependency through which humans will be exploited and monitored by both people and machines" (McGuire, 2021).

3. Gaps and Challenges in the Treatment of Cybercrime Victims

The exponential rise of these crimes in the digital world has simply exposed the systemic shortcomings of the legal and institutional framework for victim protection. With the characteristics of a transnational and immutable virtual space, it is difficult to trace the identity of cybercriminals and to secure valid evidence, which makes it impossible to rely on traditional legal measures for their punishment and prevention.
At the level of the European Union (EU), legal instruments such as the Budapest Convention on Cybercrime

(Council of Europe, 2001) and Directive 2012/29/EU on victims' rights establish principles of protection and support, although the available evidence on their actual implementation is partial and inconsistent (European Union Agency for Fundamental Rights). Legal and psychological support is often limited for the majority of victims, especially for those who have not identified the perpetrator, and bureaucratic procedures are time consuming and complex for them.

In Albania, the problems are even more complicated. The law lacks provisions for dedicated structures to protect victims of digital crimes. The current legal framework is still largely oriented toward traditional forms of crime, and offers very limited protection for acts committed online. The absence of a centralized reporting mechanism, a specialized support network, or a compensation system for victims all contribute to a significant institutional gap.

In terms of procedural reality, victims often struggle to understand their rights and what actions they should take. Current systems do not provide immediate assistance at the moment of victimization, leaving individuals to face a complex and often traumatic process of seeking help on their own.

Materially, the state's inability to financially compensate victims of cybercrime due to its exclusion from the classic mechanisms of enforcing criminal punishment further exacerbates the problem. Where the crime remains unresolved, victims are left bearing various costs (financial, pain, and suffering) that money cannot recover, and for which no genuine form of redress is available.

Ultimately, the current system remains rooted in a punitive and retributive logic that limits the restorative dimension of victim protection in the increasingly complex reality of technology. There is a risk that, without a more harmonized and adapted policy to address digital criminal offenses, the negative implications may worsen for both individuals and society as a whole.

The study of these gaps reveals the urgent need for a paradigmatic shift in victim protection: from a domain merely concerned with punishing the offender, to a structure that guarantees practical support, restitution, and full compensation for the victim regardless of the outcome of criminal proceedings.

3.1 The Identification of Offenders and the Challenge of Criminal Prosecution

One of the greatest challenges in curbing cybercrime is identifying offenders and prosecuting them. Digital crimes are highly complex, as anonymization tools, networks, and cryptographic servers located outside a nation's jurisdiction make identification extremely difficult (McGuire, 2021).

Victims' ability to trace the source of the attack is often limited, and legal authorities may encounter both technical and legal obstacles in their efforts to gather evidence. These challenges are further exacerbated in Albania, where there is no specialized infrastructure for detecting digitally based crimes, nor an adequate system for international cooperation.

Therefore, violations committed in cyberspace, by their very nature, often cannot be prosecuted, and victims are left without assistance within the framework of the rule of law; there is no possibility to obtain compensation for the harm caused.

3.2. Gaps and Deficiencies in the Legal Framework for the Protection of Victims

Another concern is the accumulation of existing gaps. This includes victims who still lack specialized networks to care for them. EU Member States have begun to develop such structures, most notably Weisser Ring in Germany or FraudHelpdesk in the Netherlands, but Albania still relies on general support mechanisms that are not specifically designed for victims of online crimes.

Legal assistance, psychotherapeutic support, and technical help to recover one's identity and information are almost entirely absent as organized services. This creates a significant gap that leaves victims to deal with the consequences of the attack alone, often without support from formal or institutionalized responses (European Union Agency for Fundamental Rights, 2021). This absence makes victims vulnerable, especially in cases where criminal proceedings are significantly delayed and whose outcomes often do not result in punishment for the offenders.

3.3 Compensation Agreements for Victims

A form of compensation is lacking for victims. Although in most EU Member States there are

state funds available to provide compensation for crime victims and cover damages, in Albania the state fund is practically nonexistent in the field of cybercrime. Those who suffer financial hardship, reputational damage, or emotional distress due to a digital attack receive no financial support whatsoever from the state. Given the often anonymous and difficult-to-trace nature of cybercrimes, the attempt to seek justice against such offenders through the traditional criminal justice system is nearly impossible. For this reason, as Wall (2022) also emphasizes, states must develop specific compensation schemes so that victims can at least partially repair their damages. The absence of such a fund in Albania means that not only is the harm further aggravated, but citizens' trust in the justice system and in the state's ability to protect fundamental rights online is also seriously undermined.

4. Alternative and New Models for the Protection of Crime Victims: A Comparative and Critical Study

In response to the structural and institutional shortcomings in the protection of cybercrime victims, current literature and the most innovative international experiences offer several alternative models to be reconsidered when designing a more effective and inclusive system. This architecture should place the victim at the center of institutional action, protection, restoration, and compensation regardless of whether a successful criminal prosecution is achieved. In practical terms, some EU countries have developed models that may serve as references for adapting the Albanian framework. For example, the FraudeHelpdesk service in the Netherlands operates as a single reporting point for digital fraud, including the provision of legal and psychological support (FraudeHelpdesk, 2021). In addition, in Germany, Weisser Ring, through its nationwide network, offers dedicated care for victims including financial support in cases where the offender cannot be identified (Weisser Ring, 2020).

Sweden has organized the inclusion of support for victims of digital crime within its national social services, enabling all citizens to have direct and easy access. In comparative terms, this type of model shares several key components that may offer a foundation for developing a new model of victim protection in Albania:

- *Creation of a centralized portal for reporting and assistance:* A digital platform for real-time reporting of crimes, legal and psychological assistance, and guidance on the protection of personal data.
- *Establishment of specialized victim care centers:* Centers that provide specialized services and a comprehensive rehabilitation system (legal, psychological, and technical) to support the victim throughout the recovery process.
- *Drafting of a Cybercrime Victims' Bill of Rights:* A legally binding document outlining the rights of victims in relation to the state, as well as public and private sectors.
- *Creation of a Public Victim Compensation Fund:* A financial mechanism that ensures victims receive compensation for damages, especially in cases where the offender is unknown or no criminal prosecution has taken place.

Especially in the case of Albania, the creation of such a model cannot rely solely on legal reform, but must instead be realized through building institutional capacities, the training of justice system professionals, and the development of public awareness and communication channels to inform citizens about the risks of digital crime and the victims' rights.

At the same time, any reform must reflect the country's economic, institutional, and cultural realities, creating opportunities for alliances between the public sector and the private technology sector in order to be effective. Only through a comprehensive and parallel effort can an effective protection system be developed, one that is tailored to the real needs of traumatized victims of cybercrime in Albania.

Finally, increasingly sophisticated international models and modern literature leave no doubt that mechanisms for building specialized support networks, ensuring access to justice, and planning compensation are essential to ensuring that the protection of victims in the digital age is truly effective. As a country striving toward European standards in the field of combating online crimes, Albania must take strong and well-considered steps to establish a system that genuinely and functionally supports victims

of online criminal acts.

4.1 Critique of the Current Punitive Model

The punitive model currently in place the "fail and punish" approach is flawed. The retributive logic directed toward the offender within the traditional framework of criminal justice has proven insufficient when applied to cybercrimes and their victims. In these virtual crimes, even when prosecution is impossible or nearly impossible, the exclusive focus on punishing the offender fails to address the victim's needs for the fulfillment of violated rights, moral support, and compensation for their losses.
As Wall (2022) points out, in the digital age, justice should not be solely about punishment, but rather about ensuring reparation and the empowerment of the victim. In this context, restorative and supportive models that prioritize the needs of the victim emerge as more applicable options for addressing the nature of cybercrime today.

1.2. Advanced Models of the European Union: Practical Examples

To develop an effective system for the protection of cybercrime victims, the first step must be to explore the experiences and more advanced models in European Union countries' systems that have established structures responsive to the new realities of digital crimes.
In the Netherlands, there is the successful case of FraudeHelpdesk, considered a best practice initiative. It operates as a central call point for cases of fraud and cybercrime. This channel not only enables quick and easy access for reporting criminal behavior, but also provides legal assistance and psychological support for victims, effectively linking justice mechanisms with humanitarian aid for those affected (FraudeHelpdesk, 2021).
In Germany, the Weisser Ring system represents a different type of victim support model, which combines legal and psychological assistance with financial compensation in cases where the offender is unknown or the case cannot be prosecuted (Weisser Ring, 2020). This model acknowledges the need for "immediate and continuous support" beyond formal criminal justice procedures.

In contrast, Sweden has adopted an integrated approach by incorporating protection for victims targeted by digital crimes into the national social service system. This integration means that victims have easy access to swift and comprehensive care as part of regular social assistance, without the need to enter legal proceedings or navigate complex justice systems.

The analysis of these models shows that support networks, financial security, and ease of reporting are integral components in establishing a successful model for the protection of cybercrime victims.

4.3. Recommendations for the Design of a New Model in Albania

Considering the identified shortcomings and the best international practices, this paper suggests the development of a new model for the protection of cybercrime victims in Albania, based on four main pillars.
First, the establishment of a National Platform for Victim Reporting and Assistance. Such an integrated digital platform where users can report threats and abuse, access emergency legal advice, and receive psychological support would eliminate bureaucratic barriers and ensure that all individuals are treated equally.
Second, the creation of Specialized Centers for Cybercrime Victim Support. These centers would assist victims through an interdisciplinary approach: legal aid, psychological support, and technical expertise to recover compromised data. There should be fair national distribution of these centers.
Third, the codification of a Charter of Rights for Cybercrime Victims would serve to enshrine victims' rights, making them enforceable in practice and widely recognized by the public.
Finally, the establishment of a Public Fund for the Compensation of Digital Crime Victims, which would provide financial assistance to victims, ensuring they are not left unsupported in cases where criminal prosecution fails or the perpetrators remain unidentified.

The adoption of such measures would contribute not only to ensuring the respect of victims' rights but also to building public trust in the justice system and increasing the overall level of digital security in the country.

4.4 Implementation Perspective in Albania: Challenges and Priorities

While the proposed model lays a strong foundation for the development of an effective protection system for cybercrime victims in Albania, there are nonetheless significant challenges to its implementation.
Firstly, there are capacity limitations at the institutional level; there is a lack of both human and technological resources. The development of secure digital platforms and support centers is costly and involves the training of justice professionals and IT experts.
Secondly, there is a critical need for public awareness and education to sensitize the wider population to the risks of digital crime and the rights of victims. Such awareness must be addressed both at the individual level of citizens and at the institutional level of justice bodies and law enforcement agencies.
Thirdly, implementation depends on the creation of a strong partnership between state agencies, the private technology sector, and civil society groups.
International experience shows that genuine and sustainable protection of digital crime victims can only be achieved through a coordinated and holistic approach. In this context, there is a need to introduce advanced models and the readiness to adapt them to the economic and institutional realities of the Albanian market, as well as continued political commitment from institutions' key factors for achieving the necessary reforms in this field.

5. Conclusions

This paper is built on the conviction that effective protection of cybercrime victims requires a profound re-evaluation of legal and institutional tools that go beyond the traditional criminal justice model and adapt policies to contemporary challenges in the virtual space. From this objective, the most essential research question was formulated at the outset of the paper: *What kinds of obstacles exist in the protection of cybercrime victims, and what existing models can be leveraged to create a better-functioning system in Albania?* This question is answered based on the following findings, which are grounded in a comprehensive review of the literature and a comparison with the most advanced models in the European Union.
Firstly, one of the key findings was that victims of cybercrime may face and suffer consequences beyond monetary damages, directly affecting their privacy, personal integrity, and psychological health. The multifaceted aspects of online victimization should be addressed not only through the offenders' criminal prosecution but also by extending protection to the full restoration of the victim's right to dignity.
Secondly, the comparative analysis has demonstrated that some EU countries, such as the Netherlands, Germany, and Sweden, have already recorded positive impacts due to the creation of integrated support networks, dedicated reporting and care platforms, and a mechanism provided by the new Directive whereby victims can receive compensation without prior identification within a specified timeframe. From these models, it is clear that achieving results in victim care requires the establishment of a broad framework that operates alongside traditional criminal justice.
Thirdly, another important finding is that Albania experiences a deep institutional and procedural gap, including the absence of specific regulation, lack of easily accessible reporting channels, non-inclusion of specific legal and psychological support, and the absence of a fund to compensate digital damages. These deficiencies not only expose victims to the risk of re-victimization but also erode trust in state institutions and the justice system.
In order to address these challenges, this paper has developed a model for the protection of cybercrime victims in Albania based on four essential pillars:

- the creation of a dedicated "real-time reporting and assistance network";
- the establishment of specialized centers for legal and psychological support for victims;
- the drafting of a Charter of Rights for Cybercrime Victims;

- and the creation of a Public Compensation Fund.

This model aims to be a responsive, proactive, and restorative system that revolves around the real needs of the victim, establishing a protective environment aligned with the challenges of the digital era. The scientific novelty of this paper lies not only in analyzing existing gaps but also in proposing an operational protection model based on best international practices, adapted to the realities of Albania.

In this way, the paper contributes to advancing a critical and creative methodology to safeguard the rights of cybercrime victims toward political and practical solutions aligned with the most advanced human rights protection standards.

The outlook for the future anticipates further development across various dimensions, including institutional capacity for addressing digital crime, training of justice professionals, and building cooperation between the public sector, private sector, and civil society organizations.

It is also essential that education and awareness-raising of citizens about the risks of cybercrime and their rights as victims be incorporated into national cybersecurity strategies.

Finally, successful victim-oriented measures related to cybercrime are not only a legal and moral necessity but also an essential prerequisite for a safe, just, and sustainable society in the digital age.

Bibliography

1. Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35 (4), 1017-1041. https://misq.umn.edu/privacy-in-the-digital-age-a-review-of-information-privacy-research-in-information-systems.html
2. Bolivar, D. Aertsen, I. Mesmaecker, V. Lauwers, N. (2011). Restorative justice and the active victim: exploring the concept of empowerment context: DOI: 10.2298/TEM1101005A Researchgate https://www.researchgate.net/publication/215564643_Restorative_justice_and_the_active_victim_exploring_empowerment
3. Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger, 2010
4. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal*, 29(3),
5. https://www.researchgate.net/publication/27465550_Developments_in_the_global_law_enforcement_of_cyber-crime
6. European Union Agency for Fundamental Rights. (2021). *Protecting victims' rights in the digital age*. Publications Office of the European Union.
7. European Union. (2012). Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime. *Official Journal of the European Union*, L 315/57.
8. FraudeHelpdesk. (2021). Over ons. https://www.fraudehelpdesk.nl
9. Komisioni Evropian. (2020). *e-Victims Project: Enhancing protection of cybercrime victims in the EU*. Brussels.
10. McGuire, M. (2021). The Dark Web and Cybercrime: Current Threats and Future Trends (2021) https://www.surrey.ac.uk/people/michael-mcguire
11. McGuire, M. (2016). C*ybercrime 4.0: Which way now*. p.251-275 Palgrave Macmillan.
12. https://openresearch.surrey.ac.uk/esploro/outputs/bookChapter/Cybercrime-40---Which-way-now/99514221702346
13. Wall, D. S. (2024). Cybercrime: The Transformation of Crime in the Information Age, 2nd edition, Cambridge, Cambridge: Polity. ISBN-10: 0745653529
14. https://www.researchgate.net/publication/378013252_Cybercrime_The_Transformation_of_Crime_in_the_Information_Age_2nd_edition
15. Weisser Ring. (2020). Hilfe für Opfer von Kriminalität und Gewalt. https://weisser-ring.de
16. AKCESK – Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike. (2023). *Raporti vjetor mbi sigurinë kibernetike në Shqipëri*. Tiranë.
17. Yar, M. (2013). *Cybercrime and Society* (2nd ed.). SAGE Publications.