Law Studies and Justice Journal (LAJU)
Vol 2 (1) 2025 : 96-112

CYBERCRIME VICTIM PROTECTION: LEGAL CHALLENGES AND STRATEGIES FOR MITIGATION

PERLINDUNGAN KORBAN KEJAHATAN SIBER: TANTANGAN HUKUM DAN STRATEGI MITIGASI

Iwan Rasiwan
Universitas Kartamulia
*iwanrasiwan@gmail.com

**Corresponding Author*

ABSTRACT
In today's digital era, cybercrime has increased significantly, posing major challenges to individuals and the legal system. Although much research focuses on technical and preventive aspects, legal protection for victims is still given little attention, creating gaps in access to justice. This research aims to identify and analyze the legal challenges faced by victims of cyber crime in obtaining justice and adequate protection. By using the approach Systematic Literature Review (SLR) and PRISMA guidelines, this research collects and analyzes articles peer-reviewed from Scopus, Web of Science and Springer databases. Data was analyzed thematically to identify patterns and key issues. Findings show that key challenges include disharmony in international regulations, jurisdictional issues, and limited victim protection in national laws. In addition, the lack of psychological support and the unpreparedness of law enforcement officers worsened the victim's condition. This research emphasizes the need for policy reform that is more responsive to the needs of cybercrime victims, as well as closer international collaboration to improve protection and access to justice. These findings contribute to the development of victimology theory and more inclusive legal practice.
Keywords: cybercrime, victim protection, access to justice, legal reform, victimology.

ABSTRAK
Dalam era digital saat ini, kejahatan siber telah meningkat secara signifikan, menimbulkan tantangan besar bagi individu dan sistem hukum. Meskipun banyak penelitian berfokus pada aspek teknis dan pencegahan, perlindungan hukum bagi korban masih kurang diperhatikan, menciptakan kesenjangan dalam akses keadilan. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis tantangan hukum yang dihadapi oleh korban kejahatan siber dalam memperoleh keadilan dan perlindungan yang memadai. Dengan menggunakan pendekatan Systematic Literature Review (SLR) *dan panduan PRISMA, penelitian ini mengumpulkan dan menganalisis artikel* peer-reviewed *dari basis data Scopus, Web of Science dan Springer. Data dianalisis secara tematik untuk mengidentifikasi pola dan isu kunci. Temuan menunjukkan bahwa tantangan utama meliputi ketidakharmonisan regulasi internasional, masalah yurisdiksi, dan keterbatasan perlindungan korban dalam hukum nasional. Selain itu, kurangnya dukungan psikologis dan ketidaksiapan aparat penegak hukum memperburuk kondisi korban. Penelitian ini menekankan perlunya reformasi kebijakan yang lebih responsif terhadap kebutuhan korban kejahatan siber, serta kolaborasi internasional yang lebih erat untuk meningkatkan perlindungan dan akses keadilan. Temuan ini berkontribusi pada pengembangan teori victimology dan praktik hukum yang lebih inklusif.*
***Kata Kunci**: kejahatan siber, perlindungan korban, akses keadilan, reformasi hukum, victimology.*

1. INTRODUCTION

In the current digital age, the proliferation of cybercrime poses significant threats not only to institutions and nations but also has dire implications for individuals. Data from organizations such as Interpol and Europol indicate a disturbing rise in cybercrime incidents, ranging from identity theft and online fraud to more severe forms of exploitation, including online child sexual abuse. This upsurge in cyber misconduct does not merely result in material

losses; victims frequently experience profound psychological trauma, damage to their social reputations, and considerable difficulties in finding justice due to inadequate legal protections (Shukurov & Jafarov, 2023; Borwell et al., 2024).

Research indicates that legal frameworks aimed at tackling cybercrime have often prioritized the prosecution of offenders and the enhancement of cybersecurity measures, while leaving the vital area of victim support inadequately addressed. Victims generally grapple with complex legal procedures, compounded by law enforcement's insufficient awareness of victims' rights and a lack of robust legal and psychological support systems (Ajayi, 2016; (Amoo et al., 2024; . This problem is further exacerbated by jurisdictional limitations that hinder cross-border criminal prosecutions, often culminating in a miscarriage of justice for victims. There exists a pressing need for the establishment of universal standards to protect victims of cybercrime, as varied legal interpretations and institutional inefficiencies complicate victims' ability to navigate the legal landscape (Amoo et al., 2024; Ahmad & Ramayah, 2022).

Furthermore, it is essential to consider the psychological dimensions related to cybercrime victimization. Research reveals that victims of cyber-related offenses endure significant emotional and psychological challenges that can mimic symptoms related to post-traumatic stress disorder (PTSD) (Palassis et al., 2021; Partin et al., 2021). The perception of a lack of available help complicates recovery, especially for those already struggling with psychological issues. The absence of an encompassing support framework for cybercrime victims highlights the necessity for an inclusive policy approach that adequately addresses the experiences and needs of these individuals (Notté et al., 2021; Mwiraria et al., 2022).

Comprehensive studies focusing on the legal and psychological challenges faced by cybercrime victims can provide foundational insights necessary for developing more effective and responsive public policies. It is imperative for policymakers to emphasize victim support mechanisms, ensuring justice and assistance that consider the unique realities of cybercrime experiences. Such an inclusive approach could significantly enhance trust in legal systems and contribute positively to the overall welfare of society in the context of the digital age (Amoo et al., 2024; "Digital Forensics in Cybercrime Investigation", 2024).

A review of the literature shows that most previous research in the cybercrime domain tends to focus on technical aspects, such as detection, prevention and information security, as well as on the profile and motives of perpetrators. Although several studies have discussed the social and psychological dimensions of cybercrime, the issue of legal protection for victims is still very limited and spread across fragmented disciplines.

In addition, very few studies adopt a systematic and comprehensive approach in identifying legal challenges across countries and across jurisdictions. In fact, in the context of internet globalization, cyber crimes often involve perpetrators, victims and technological infrastructure spread across various countries, giving rise to high legal complexity. The absence of a systematic literature review of the legal barriers victims face in obtaining justice and support is an important gap that needs to be filled in the academic literature and policy practice.

Based on the background and research gaps that have been described, this research is designed to identify and analyze the legal challenges faced by cybercrime victims in obtaining justice and adequate protection. The main research question, namely "What are the key legal challenges in ensuring justice and support for cybercrime victims?", aims to explore various obstacles that exist in the justice system, both in terms of legal substance, procedures and policy implementation. This research will explore complex issues related to national and international law, including regulatory disharmony, jurisdictional issues, and limited access to justice for victims. In addition, this research will also consider cross-country perspectives and global contexts, highlighting how regulatory differences between countries can worsen the situation of victims. Thus, this research not only aims to provide a deeper understanding of

existing challenges, but also to offer policy recommendations that can improve legal protection for cybercrime victims more effectively.

The main aim of this research is to develop a comprehensive synthesis of the legal challenges faced in ensuring justice and support for victims of cybercrime, based on a systematic review of relevant academic literature. This research aims to fill the gap in the existing literature by providing a conceptual map that can explain the types of legal barriers most frequently identified in the context of protecting victims of cybercrime. In this way, it is hoped that this research will provide a clearer picture of the complexity of the challenges faced by cybercrime victims and how the legal system can adapt to overcome them.

Apart from that, it is also hoped that this research can make a theoretical contribution by expanding the study of victimology and access to justice in the context of modern cyber crime. This approach aims to integrate existing theories with new issues that arise along with the rapid development of technology and cyber crime, so as to open up space for the development of more relevant and contextual theories.

Furthermore, this research also has practical implications that can influence legal policy. By analyzing existing legal challenges, it is hoped that the results of this research can provide recommendations for lawmakers, law enforcement officials and civil society organizations in designing a legal protection system that is more responsive to the needs of cybercrime victims. This approach based on practical needs can help create policies that are more targeted and effective in protecting victims of cybercrime.

Through a Systematic Literature Review approach, this study also contributes to establishing a solid academic foundation that can be used as a reference for further research, cross-country policy development, and advocacy for the protection of the rights of cybercrime victims in the future. With a comprehensive and structured approach, this research not only fills a gap in the current literature, but also makes a significant contribution to advancing the protection of cybercrime victims globally.

2. METHODS

2.1 Research Design

This research uses an approach Systematic Literature Review (SLR) which adopted the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines. This approach was chosen to ensure that the process of collecting, screening, and analyzing the literature was transparent, replicable, and free from selection bias. SLR allows researchers to synthesize knowledge scattered across studies into a structured and holistic understanding. Considering the complexity of legal issues in the context of protecting victims of cyber crime (cybercrime), this approach is considered the most appropriate for evaluating existing evidence, identifying literature gaps, and proposing future research and policy agendas.

Additionally, the SLR approach provides a strong methodological framework for integrating multidisciplinary perspectives from the fields of law, criminology, information technology, and victimology. In this context, this method not only aims to collect empirical evidence, but also to elaborate the normative dimensions of legal protection for victims of cyber crime, which have so far been relatively neglected in conventional legal studies.

2.2 Inclusion and Exclusion Criteria

To ensure the relevance and quality of the findings, this study established strict inclusion and exclusion criteria. Inclusion criteria include journal articles peer-reviewed published between 2012 and 2025, with the main focus on legal aspects and protection of victims of cyber crime. Selected articles must explicitly discuss issues related to legal challenges, access to justice, support mechanisms, or protection policies for victims in the digital realm.

In contrast, the exclusion criteria included studies that only addressed technical aspects of cybercrime such as network security, encryption techniques, or digital forensics without clear legal relevance. Articles that did not include explicit discussion of victims or legal approaches were also eliminated. This aims to maintain the focus of analysis so that it remains within the legal corridor and victim-oriented perspective.

2.3 Data Sources and Search Strategy

Literature collection is carried out through four main scientific databases: **Scopus, Web of Science, Springer**. These three sources were selected based on their multidisciplinary coverage and credibility in providing reputable scientific articles. The search strategy was formulated using a Boolean logic approach to capture variations in terminology used in international literature. The keyword formulation used is as follows: **(“cybercrime” OR “cyber victim”) AND (“legal challenge” OR “law” OR “justice”) AND (“protection” OR “support”).**

This search strategy was designed to reach articles that discuss both conceptual and empirical dimensions related to legal challenges in providing protection and justice for victims of cybercrime. In addition, the search also considered synonyms or equivalent terms commonly used in various legal jurisdictions, for example “cyber victimization”, “online abuse law”, or “digital justice”.

2.4 Selection Process

The article selection process is carried out through four stages in accordance with the PRISMA framework: (1) identification, (2) screening, (3) eligibility assessment, and (4) inclusion. At stage identification, all articles obtained from the initial search results were compiled and imported into reference management software (Mendeley). Next, stage screening was carried out to remove duplication and filter based on title and abstract. Articles that pass this stage then enter the next stage eligibility, where a full content review was conducted to ensure appropriateness of topic and methodology. Articles that meet all the criteria are then entered into the final stage, namely inclusive.

The entire process is presented visually in the PRISMA flow diagram to ensure transparency and accountability of the selection process. This diagram also allows readers to evaluate the thoroughness of the review process and potential systematic biases that may have emerged during data selection.

2.5 Data Analysis Techniques

Data analysis was carried out using an approach thematic analysis, which allows researchers to identify major patterns and key issues that recur in the literature. This process begins with open coding to highlight legal issues that emerge from the text, which are then categorized into main themes based on similarities in content and significance to the research questions.

Next, it's done framework analysis by referring to relevant theories in legal studies and victimology, such as Victimology Theory, Access to Justice Theory, and a normative approach based on human rights (human rights-based approach). This technique helps in understanding the complex relationship between legal norms, policy practices, and victims' experiences in accessing digital justice.

Apart from that, researchers also integrate a legal hermeneutic approach in interpreting legal or regulatory texts used in the articles reviewed, in order to identify normative ambiguities or inconsistencies between a legal doctrine and practice in the field.

3. RESULTS

3.1 Characteristics of the Studies Reviewed

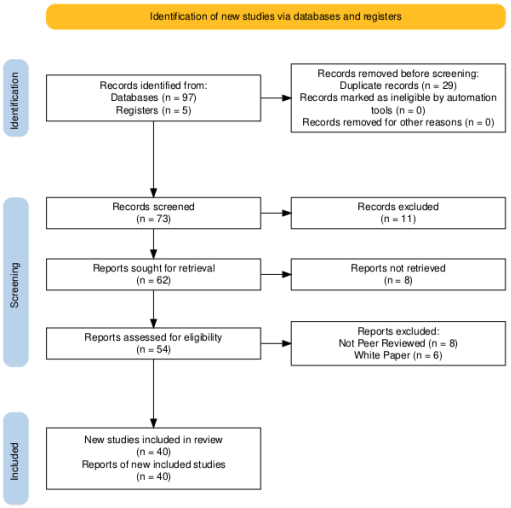

Figure 1. Prisma Diagram
Source: Processed Data, 2025

The systematic process used to identify and screen new studies for inclusion in this review consists of three main stages: Identification, Screening, and Inclusion.

In the Identification stage, a total of 102 records were identified from two primary sources: 97 records from the database and 5 records from the registry. Of these, 29 records were removed because they were duplicates, while no records were marked ineligible by the automation tool or removed for other reasons.

The next stage, namely Screening, involved screening 73 records, of which 11 records were excluded because they did not meet the specified criteria. After that, of the 62 reports sought to be retrieved, 8 reports failed to be retrieved. At the Feasibility Assessment stage, 54 reports were assessed for their feasibility, 14 reports were ultimately excluded. Most of the excluded reports were those that were not peer-reviewed (8 reports) and white paper documents (6 reports).

Finally, at the Inclusion stage, 40 new studies were included in this review, which included relevant reports and met the established criteria. This diagram emphasizes the importance of a careful selection process to ensure that only relevant and high-quality studies are included in this systematic review.

3.2. Geographic Distribution

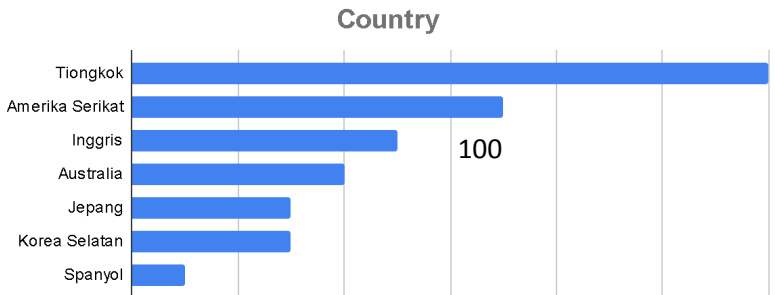

Figure 2. Geographical Distribution
Source: Processed Data, 2025

The geographical distribution of the 40 articles relevant to this research shows that research contributions come from various countries with varying levels of research strength. China recorded the highest number of articles, namely 12 articles, which reflects the country's dominance in related research fields, perhaps due to its rapid progress in the technology, research and development sectors, as well as great attention to global issues. The United States, with 7 articles, took second place, reflecting its strong reputation in academic research and technological innovation. The UK, with 5 articles, also shows a significant contribution in this field, thanks to its well-established academic traditions and a number of leading universities which are research centers in the world. Australia, with 4 articles, reflects its commitment to the development of relevant research, driven by the country's influential academic institutions.

In addition, Japan and South Korea each contributed 3 articles, which shows the interest of these two countries in studying global phenomena, by utilizing their extraordinary technological strengths. Countries such as Spain, Portugal, Indonesia and Malaysia each contributed one article, demonstrating participation from countries with smaller research capacities but still providing unique and useful insights into the development of global knowledge. Canada, with 2 articles, also shows an important role in producing relevant research, driven by strong research policies and leading universities.

Overall, the geographic distribution of these articles reflects the importance of an international perspective in the research conducted. Although this research is dominated by countries with large research capacities such as China, the United States and the United Kingdom, contributions from developing countries such as Indonesia and Malaysia provide a more diverse view and enrich the conclusions that can be drawn from the existing literature.

3.3. Research Methodology

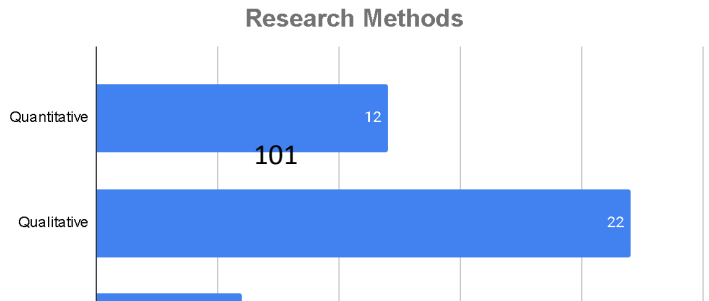

Figure 3. Methods
Source: Processed Data, 2025

The table above shows the distribution of research methods used in the 40 articles analyzed, with the following details: 12 articles use quantitative methods (Quantitative), 22 articles use qualitative methods (Qualitative), And 6 articles using mixed methods (Mix Methods).

Use of methods quantitative which is less than the method qualitative suggests that most research focuses on collecting more subjective and in-depth data, such as interviews and case studies, which are suitable for explaining phenomena more contextually and understanding individual or group perspectives. This is often related to studies related to social behavior, psychology, or policy studies, which require a broader understanding of the factors that influence certain outcomes.

Meanwhile, method quantitative is more widely used in research that prioritizes hypothesis testing through numerical data and statistical analysis, which allows researchers to identify relationships between variables in a more objective and measurable manner. Method Mix Methods used in 6 articles combined quantitative and qualitative approaches, providing depth of analysis and the ability to confirm results more thoroughly.

In the context of this research which aims to understand the dynamics in the topic being researched, the application of the method qualitative The dominant one can provide deeper insight into the perceptions, experiences and views of the research subject, while the approach quantitative And Mixed Methods it would be useful to examine broader patterns and relationships through statistical analysis and integration of findings from both approaches.

3.4. Key Findings

Thematic analysis of the selected articles produced five main themes that describe challenges in legal protection for victims cybercrime:

1. International Legal and Regulatory Challenges

Studies show that The international legal framework surrounding cybercrime remains notably fragmented, characterized by a lack of consensus on its definition and the mechanisms for victim protection. One of the primary challenges emphasized across various studies is the absence of a universally accepted definition of cybercrime, complicating the application of legal principles across jurisdictions. Ajayi points out that the lack of agreement on what constitutes criminal conduct, among other enforcement challenges, hampers effective law enforcement regarding cybercrime globally (Ajayi, 2016). This concern is echoed by Khan et al., who highlight that the Budapest Convention, while recognized as a pivotal international instrument, is not universally adopted, limiting its effectiveness as a comprehensive framework for combating cybercrime globally (Khan et al., 2022).

Moreover, the implementation of existing laws is generally hindered by insufficient legal power for investigations and the variability of norms across different national jurisdictions. Amoo et al. reinforce this point by suggesting that stakeholders must adapt legal frameworks to address the contemporary threats posed by cybercriminals, emphasizing the necessity of a cohesive international response (Amoo et al., 2024). The lack of uniformity in procedural laws, combined with differing national legal definitions, contributes significantly to the enforcement difficulties that persist in cybercrime investigations (Amoo et al., 2024).

Furthermore, the imperative for international cooperation in the realm of cybercrime is underscored by various authors. For instance, Didenko argues for the need for harmonization of legal frameworks concerning cybersecurity, particularly in sectors such as finance, which are vulnerable to cyber threats (Didenko, 2020). This sentiment is corroborated by Broadhurst's observation that despite the acknowledgment of cybercrime as a transnational issue exploiting international differences in legal frameworks, collaborative efforts remain insufficient (Broadhurst et al., 2013). Similarly, the argument for modernizing cooperation mechanisms to combat cybercrime is further articulated by Azzam, who advocates for the need to improve international frameworks and define cyber threats to tackle these challenges collectively (Azzam, 2019).

In summary, while the Budapest Convention provides a foundational approach to international cooperation in addressing cybercrime, the broader legal framework remains inconsistent, plagued by a lack of global consensus on key definitions and enforcement mechanisms. As cyber threats evolve, an urgent adaptation of international norms and cooperative strategies is necessary to effectively counter the pervasive nature of cybercrime.

2. Jurisdiction and Extraterritorial Issues

The cross-border nature of cybercrime presents significant jurisdictional challenges that complicate the enforcement of laws against perpetrators who often operate outside the jurisdictions of their victims. Many nations struggle to effectively prosecute cybercriminals due to varying legal frameworks and geographical boundaries of jurisdiction, resulting in insufficient access to justice for victims.

One major factor contributing to these challenges is the absence of a unified global legal framework regarding cybercrime. Several studies indicate that there is a lack of international consensus on what constitutes cybercrime and how to define it legally, complicating standardized enforcement across different jurisdictions. The legal ambiguity surrounding cyber offenses makes it difficult for victims to have their cases adjudicated effectively, particularly when perpetrators are located in different countries with disparate laws (Shukurov & Jafarov, 2023; (Ajayi, 2016; (Amoo et al., 2024; . As Ajayi notes, differing national laws regarding cybercrime inevitably lead to enforcement challenges (Ajayi, 2016; .

Moreover, the technological nature of cybercrime intensifies these jurisdictional dilemmas. Cybercriminals exploit the global nature of the internet to operate transnationally, making it difficult for law enforcement agencies to coordinate their responses effectively (Ajayi, 2016; (Amoo et al., 2024; Koziarski & Lee, 2020). The ability of these criminals to act from any location and the complexity of tracking their activities further complicate the challenges faced by law enforcement. Nugroho and Chandrawulan emphasize how the COVID-19 pandemic accelerated the evolution of cybercrime, affecting the ability of law enforcement agencies to address these cross-border issues effectively (Nugroho & Chandrawulan, 2022).

Collaboration and cooperation between nations are essential elements in combating cybercrime. Disparities in national laws create obstacles to mutual legal assistance, hindering international cooperation crucial for cybercrime investigations (Ilchyshyn et al., 2023; Broadhurst & Chang, 2012). Additionally, jurisdictions may struggle with varying definitions of evidence, complicating efforts to gather, share, and utilize digital forensic information across borders (Mikkola et al., 2020; Curtis & Oxburgh, 2022).

In conclusion, the challenges in enforcing cybercrime legislation across borders stem from ambiguous laws, diverse legal definitions, and the complex nature of cybercriminal activities spanning multiple jurisdictions. The need for harmonized legal frameworks and robust international collaboration is increasingly recognized as critical for enhancing the effectiveness of responses to cybercrime globally (Amoo et al., 2024; Robalo & Rahim, 2023).

3. Limitations of Victim Protection in National Law

The discourse surrounding victim protection within the criminal justice system has increasingly highlighted a persistent issue: many national laws remain oriented towards the offender rather than the victim. Research indicates that the integration of victim rights into legal frameworks is often inadequate, leading to a situation where protections appear largely symbolic rather than enforceable (Kuzmenko & Kuzmenko, 2024; Katz, 2022). For instance, the literature reveals significant gaps in effective legal mechanisms designed to ensure restitution for victims, particularly in the realm of cybercrime (Robalo & Rahim, 2023; Halder, 2021). This inadequacy is underscored by the absence of dedicated processes that allow victims to seek reparations from offenders, a vital aspect often neglected in many jurisdictions (Belgradoputra et al., 2025).

Further complicating the issue is the ideological framing of victimhood, which has evolved over the decades. Killean discusses how political contexts shape the recognition of victims and their eligibility for reparations, indicating that not all victims are treated equally within judicial processes (Killean, 2018). The integration of victim perspectives in criminal justice is critical in shifting the focus from punishment of offenders to a more restorative justice model that also attends to victim healing and restitution (Absar, 2020). Nevertheless, there are indications that even where victim-centric policies exist, they are not sufficiently robust or comprehensive to provide meaningful support to victims, showcasing a systemic prioritization of offender rights and interests (Haroon & Ali, 2024).

Additionally, the context of transnational crimes, such as child sexual abuse, illustrates the complexities of jurisdictional disparities and the inadequacy of existing victim protection measures across borders (Merdian et al., 2019). The lack of collaborative frameworks and coherent strategies for victim support and restitution in such situations reflects a broader trend in the treatment of victims in the criminal justice system, where the focus often remains skewed towards procedural justice rather than substantive outcomes for victims (Audi & Zakaria, 2022). Ultimately, the literature articulates a critical need for comprehensive reform within national laws to better embrace and support the rights and needs of victims, moving away from an offender-centric model (Robalo & Rahim, 2023; Ahlin & Douds, 2020).

In conclusion, while there have been strides towards recognizing and addressing the rights of victims within the criminal justice framework, substantial gaps remain. These gaps are especially pronounced in relation to specific mechanisms for restitution and support for victims of various crimes, particularly in new and complex domains such as cybercrime and transnational offenses. Therefore, continuous advocacy and legislative reforms are crucial to ensure that victim rights are not only acknowledged but are actively integrated into the justice process to create a more balanced and equitable system.

4. Inequality in Access to Justice and Psychological/Social Support

Cybercrime victimization has profound psychological, social, and emotional impacts on individuals. Victims often experience significant psychological trauma, which can manifest in symptoms akin to those seen in post-traumatic stress disorder (PTSD) as outlined in the literature (Borwell et al., 2021)(Palassis et al., 2021). The emotional fallout associated with cybercrime victimization includes feelings of distress and insecurity regarding digital interactions (Borwell et al., 2021).

Furthermore, Maher and Hayes noted that victims of identity theft may face revictimization, contributing to further psychological harm as they often encounter dismissive attitudes from institutions when attempting to secure recompense for their losses (Maher & Hayes, 2024). This dynamic underlines the emotional burden placed on victims, adversely affecting their mental health and well-being (Maher & Hayes, 2024).

In addition to psychological impacts, cybercrime can lead to significant social consequences. Victims frequently face social stigma and loss, which further exacerbates their emotional trauma (Palassis et al., 2021). For instance, social penalties can arise through misperceptions about victims and their involvement in criminal acts, often promoting sentiments of disbelief or blame directed toward the victims themselves (Black et al., 2019). This stigmatization is particularly pronounced in under-resourced jurisdictions, where support services may be lacking, creating a cycle of misunderstanding and social alienation for the victims (Weijer et al., 2021).

Unfortunately, the availability of recovery support for victims of cybercrime remains disproportionately low, especially in developing regions. Studies have indicated severe limitations in access to crucial recovery resources like counseling, legal aid, and digital reputation restoration services (Weijer et al., 2021)(Hyder, 2022). The lack of these essential services increases the likelihood of revictimization, as victims are left without the necessary tools and support to navigate their trauma and reclaim their digital identities (Weijer et al., 2021). The systemic disparities in access to recovery support starkly illustrate the challenges that victims face, particularly in locales where such infrastructure is limited or non-existent (Hyder, 2022).

Moreover, the intersectionality of victimization within various demographics—particularly among vulnerable groups such as the elderly—demonstrates heightened exposure to repeated victimization and emotional distress (Havers et al., 2024). Reports of older adult victims reveal a troubling trend where they are less likely to report cybercrime incidents, often due to misunderstanding, stigma, or the debilitating effects of their experiences (Havers et al., 2024). As a result, equitable access to recovery support must be made a priority in order to mitigate the impacts of cybercrime across various populations, thereby fostering a safer digital environment.

In conclusion, the interrelatedness of psychological trauma, social loss, and the stigma associated with cybercrime underscores the necessity for a comprehensive approach to victim support. Enhancing accessibility to recovery resources, particularly in developing countries, is critical to reducing the risk of revictimization and fostering psychological resilience among victims.

5. Unpreparedness of Law Enforcement Officials and Judicial Institutions

The increasing prevalence of cybercrime poses significant challenges for law enforcement agencies, particularly concerning the training and capacity of officers to effectively tackle these evolving threats. Many law enforcement personnel lack specialized training in both the technical and psychological aspects of cybercrime, which can hinder their ability to engage with victims and investigate incidents. Shukurov and Jafarov underline that jurisdictions often struggle with a lack of specialized units dedicated to cybercrime enforcement, and this inadequacy hampers international cooperation and a unified response to cybercriminal activities (Shukurov & Jafarov, 2023).

Research from various studies emphasizes the need for enhanced training programs to equip police officers with the necessary skills and knowledge to respond to cybercrime effectively. Ajayi highlights the absence of a global consensus on the definitions and legislative frameworks governing cybercrime, complicating the enforcement process (Ajayi, 2016). Similarly, Koziarski and Lee argue that improving law enforcement's responses to cybercrime is critical to maintaining institutional legitimacy in their role as first responders (Koziarski & Lee,

2020). Furthermore, studies indicate that patrol officers express limited interest or preparedness to engage actively in cybercrime investigations, exacerbating the issue (Holt & Bossler, 2012).

Compounding these challenges is the insufficient understanding of the psychological impact of cybercrime on victims. Research has shown that victims of cybercrime face not only financial repercussions but also severe psychological trauma, which law enforcement officers may be ill-prepared to address if they lack an understanding of these dynamics (Borwell et al., 2021). Recommendations for improving victim assistance emphasize the importance of equipping officers with skills to empathize with and effectively support cybercrime victims, thus facilitating better reporting rates and a more responsive law enforcement framework (Cockcroft et al., 2018).

Additionally, specialized cybercrime policing units serve as a critical mechanism for countering the unique challenges presented by digital offenses. Willits and Nowacki analyze how such units can be effectively organized and utilized within law enforcement, reinforcing the argument that dedicated resources and personnel are vital for addressing the complexities associated with cybercrime (Willits & Nowacki, 2016). Without a comprehensive strategy that encompasses both training and resource allocation, law enforcement agencies risk falling short in their obligation to enforce the law effectively and protect citizens in the digital age (Holt, 2018).

In conclusion, enhancing police capacities to deal with cybercrime requires a multifaceted approach involving specialized training, improved victim support mechanisms, and the establishment of dedicated cyber units within law enforcement. The current deficiencies in these areas pose significant threats to achieving justice for victims and upholding public trust in law enforcement agencies.

4. DISCUSSIONS

4.1 Synthesis of Findings

The findings in this study reveal that there are legal challenges in protecting victims of cybercrime that are complex and interrelated. Through a thematic analysis approach, it can be seen that no one legal dimension stands alone—issues of international regulation, jurisdiction, and victims' rights influence each other systemically.

For example, the limitations of international regulations have a direct impact on the ineffectiveness of cross-border jurisdictions. This then creates a gap in victim protection which not only has a legal dimension, but also bThe impact on psychological and social aspects. This synthesis indicates that protecting victims of cyber crime requires a multidisciplinary and multilevel approach, involving international law, national law, and social intervention.

4.2 Theoretical and Practical Implications

Theoretically, the findings of this study confirm the relevance of several main theories in the context of protecting victims of cyber crime. First, victimology theory which places victims at the center of the modern criminal justice system, although it has not yet been fully adopted in the context of cyber crime. In cybercrime cases, victims are often overlooked in the legal process, so it is important to integrate the victim's perspective into the existing justice system. Second, the theory of restorative justice, which emphasizes the recovery of victims through reconciliation and restitution, is very relevant, especially considering that many cybercrime victims experience digital trauma, as well as reputational losses that are difficult to recover from. This approach can provide a way to restore the psychological and social well-being of victims. Third, international legal theory shows structural weaknesses in dealing with cross-border crimes collectively. Cybercrime, which often involves perpetrators and victims in different countries, highlights the need for more coordinated and effective international legal reform to address this challenge.

Practically, this study proposes several important steps in responding to the challenges faced by cybercrime victims. National legal policy reform is urgently needed, in particular by encouraging the strengthening of restitution mechanisms for victims and the establishment of a cybercrime victim assistance unit that can provide more holistic assistance. In addition, the advocacy role of civil society organizations is very important to pressure the government to expand access to digital justice, provide better protection, and ensure that victims' rights are effectively protected. Closer international collaboration should also be established, through bilateral or multilateral agreements, to improve cyber law enforcement and victim protection at the global level. This approach is expected to create a stronger, more responsive and fair protection system for victims of cybercrime throughout the world.

4.3 Comparison with Previous Studies

The results of this study are in line with previous literature which states that the current legal system is still offender-centric. However, these findings also expand the discourse by adding important dimensions related to the readiness of legal institutions and inequality in access to recovery for victims, aspects that have not been widely discussed in previous studies. Some previous studies emphasize aspects of technology and digital security, while this study places victims as the main entity in the legal protection framework, and integrates social and psychological dimensions as part of comprehensive protection.

4.4 Study Limitations

This study has several limitations that need to be acknowledged. First, database limitations, because the literature search was focused on Scopus, Web of Science, Springer. This may result in a lack of coverage of important articles published in local legal journals or in non-English languages, which may have relevant insights into legal challenges in different countries. Second, the publication time span is limited to years 2012 - 2025 the scope of this research, so that contributions from classic studies or earlier articles that could provide deeper context regarding the development of law and cybercrime are not involved in this analysis. Third, the possibility of publication bias is also an issue, because articles published in peer-reviewed journals tend to follow certain theoretical tendencies, and do not always reflect the real conditions faced by victims in the field. Therefore, although the findings of this study provide a significant contribution, there are limitations in the representation of the data that may need to be considered in the interpretation of the research results.

4.5 Recommendations for Further Research

To deepen understanding and strengthen empirical evidence regarding the protection of cybercrime victims, several further research directions are suggested. First, empirical studies in developing countries are essential to evaluate legal implementation and the effectiveness of victim support in the context of limited resources and prevalent digital inequality. This kind of research can provide new insights into how the law can be adapted to address the unique challenges of countries with less developed digital infrastructure.

Second, evaluating legal policies that have been implemented through a case study approach can provide a deeper understanding of the effectiveness of national cybercrime units and legal aid institutions in handling cybercrime cases. For example, analyzing whether existing policies are truly effective in protecting victims or whether there are gaps that still need to be corrected.

Third, exploring the relationship between forensic technology and victims' rights is also an important direction. Further research could explore how digital evidence is collected and used in legal proceedings, as well as how forensic techniques can be applied without causing revictimization for victims. This will be a very significant contribution in ensuring that forensic technology can be used fairly and does not harm parties who have become victims. With this

more in-depth research direction, it is hoped that more comprehensive policy recommendations can be produced to protect the rights of cybercrime victims.

5. CONCLUSION

5.1 Summary of Key Findings

This study identified significant legal challenges in providing adequate protection to victims of cybercrime. These challenges include disharmony in international regulations, jurisdictional and extraterritoriality issues, as well as limitations of national law in guaranteeing victims' rights. In addition, unequal access to justice, lack of psychosocial support, and unpreparedness of law enforcement officials are als worsening the victim's condition. Through approach Systematic Literature Review following PRISMA guidelines, this study highlights that victim protection has not been a priority in the existing legal framework, both at the national and international levels.

5.2 Contribution to Literature and Practice

Conceptually, this research contributes to the legal literature and victimology studies in several ways. First, this research provides a conceptual map that presents key issues in the protection of cybercrime victims, covering the main challenges faced in the current legal system. This conceptual map can be a reference for further research and more focused policy development.

Second, this research offers an integrative framework that connects regulatory, jurisdictional and victim support aspects. This framework not only highlights the legal challenges faced by victims, but also how various aspects of the law can be integrated to provide more comprehensive and effective protection. Thus, this framework can become a basis for formulating more cohesive policies at the national and international levels.

Third, this research provides practical insights for policy makers, academics and legal practitioners, especially in designing a more humanistic and inclusive approach to victims of cyber crime. This is important, considering that many legal systems are still not fully responsive to the needs of cybercrime victims. It is hoped that this insight can inspire policy reforms that focus more on restoring and protecting victims' rights in an ever-evolving digital context.

5.3 Study Limitations

This study has several limitations that need to be noted. First, data sources are limited to scientific articles indexed in databases such as Scopus, Web of Science, Springer, which may not reflect local policies or practices as a whole. Some literature from local journals or those in non-English languages may not be included in this search, resulting in the potential to overlook important perspectives from the local context.

Second, there are limitations in geographical representation, where most of the literature analyzed comes from developed countries. This can lead to a lack of in-depth understanding of the challenges and solutions facing developing countries, especially in terms of limited resources and digital inequality that affect the protection of cybercrime victims in the region. Therefore, it is important to consider developing country contexts in follow-up research to gain a more holistic picture of the legal challenges facing cybercrime victims.

5.4 Suggestions for Future Research and Policy

To strengthen legal protection for cybercrime victims, several recommended steps include strengthening international law harmonization through multilateral agreements that explicitly include victims' rights in the cyber law enforcement agenda. This is important considering that cybercrime often involves cross-border aspects, so cooperation between countries is key to creating a more responsive system and protecting victims effectively. Furthermore, increasing the capacity of law enforcement institutions through training officers

to understand the dynamics of digital trauma and victim sensitivity is very necessary. This training will enable officers to not only identify the perpetrator but also provide more humanistic treatment, taking into account the psychological impact on the victim. In addition, cross-national empirical research, especially in developing countries, can provide deeper insights into the effectiveness of victim protection policies in local social, economic and political contexts. Finally, a collaborative approach between states, international organizations and civil society will strengthen a more inclusive digital justice ecosystem, which can provide legal and psychological support to victims and expand access to digital justice for all levels of society.

6. REFERENCES

Absar, A. (2020). Restorative justice in islam with special reference to the concept of diyya. Journal of Victimology and Victim Justice, 3(1), 38-56. https://doi.org/10.1177/2516606920927277

Ahlin, E. and Douds, A. (2020). If you build it, will vets come? an identity theory approach to expanding veterans' treatment court participation. Criminal Justice Review, 45(3), 319-336. https://doi.org/10.1177/0734016820914075

Ahmad, R. and Ramayah, T. (2022). A systematic literature review of routine activity theory's applicability in cybercrimes. Journal of Cyber Security and Mobility. https://doi.org/10.13052/jcsm2245-1439.1133

Ajayi, E. (2016). Challenges to enforcement of cyber-crimes laws and policy. Journal of Internet and Information Systems, 6(1), 1-12. https://doi.org/10.5897/jiis2015.0089

Amoo, O., Atadoga, A., Abrahams, T., Farayola, O., Osasona, F., & Ayinla, B. (2024). The legal landscape of cybercrime: a review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205-217. https://doi.org/10.30574/wjarr.2024.21.2.0438

Audi, M. and Zakaria, C. (2022). Legal protection for victims of criminal acts of rape is related to Law Number 31 of 2014 concerning witness and victim protection. Bandung Conference Series Law Studies, 2(1). https://doi.org/10.29313/bcsls.v2i1.379

Azzam, F. (2019). The adequacy of the international cooperation means for combating cybercrime and ways to modernize it. Janus Net E-Journal of International Relation, 1(10), 64-81. https://doi.org/10.26619/1647-7251.10.1.5

Belgradoputra, R., Haryono, W., & Wirogioto, A. (2025). Implementation of criminal sanctions against perpetrators of bank account data theft that is fair for the public. Jilpr Journal Indonesia Law and Policy Review, 6(2), 236-243. https://doi.org/10.56371/jirpl.v6i2.360

Black, A., Lumsden, K., & Hadlington, L. (2019). 'why don't you block them?' police officers' constructions of the ideal victim when responding to reports of interpersonal cybercrime., 355-378. https://doi.org/10.1007/978-3-030-12633-9_15

Borwell, J., Jansen, J., & Stol, W. (2021). The psychological and financial impact of cybercrime victimization: a novel application of the shattered assumptions theory. Social Science Computer Review, 40(4), 933-954. https://doi.org/10.1177/0894439320983828

Borwell, J., Jansen, J., & Stol, W. (2024). Exploring the impact of cyber and traditional crime victimization: impact comparisons and explanatory factors. International Review of Victimology, 31(1), 156-181. https://doi.org/10.1177/02697580241282782

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Steve, C. (2013). Organizations and cybercrime. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2345525

Broadhurst, R. and Chang, L. (2012). Cybercrime in asia: trends and challenges. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2118322

Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z., & Trevorrow, P. (2018). Police cybercrime training: perceptions, pedagogy, and policy. Policing a Journal of Policy and Practice, 15(1), 15-33. https://doi.org/10.1093/police/pay078

Curtis, J. and Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. The Police Journal Theory Practice and Principles, 96(4), 573-592. https://doi.org/10.1177/0032258x221107584

Didenko, A. (2020). Cybersecurity regulation in the financial sector: prospects of legal harmonization in the european union and beyond. Uniform Law Review, 25(1), 125-167. https://doi.org/10.1093/ulr/unaa006

Halder, D. (2021). Charge sheet to charging., 246-257. https://doi.org/10.4018/978-1-7998-6884-2.ch014

Haroon, A. and Ali, K. (2024). Assessment of knowledge and attitude about pocso act among medical interns: a questionnaire based study. Indian Journal of Forensic Medicine & Toxicology, 18(2), 5-8. https://doi.org/10.37506/hvpzys06

Havers, B., Tripathi, K., Burton, A., Martin, W., & Cooper, C. (2024). Exploring the factors preventing older adults from reporting cybercrime and seeking help: a qualitative, semistructured interview study. Health & Social Care in the Community, 2024(1). https://doi.org/10.1155/2024/1314265

Holt, T. (2018). Regulating cybercrime through law enforcement and industry mechanisms. The Annals of the American Academy of Political and Social Science, 679(1), 140-157. https://doi.org/10.1177/0002716218783679

Holt, T. and Bossler, A. (2012). Predictors of patrol officer interest in cybercrime training and investigation in selected united states police departments. Cyberpsychology Behavior and Social Networking, 15(9), 464-472. https://doi.org/10.1089/cyber.2011.0625

Hyder, A. (2022). Cyber-crime victimization through social media: an exploratory study of victims in hyderabad, pakistan. Annals of Human and Social Sciences, 3(II). https://doi.org/10.35484/ahss.2022(3-ii)43

Ilchyshyn, N., Брусакова, О., Krykun, V., & Myroshnychenko, Y. (2023). International legal cooperation in the field of criminal justice: new challenges and ways to overcome them. Journal of Law and Sustainable Development, 11(4), e767. https://doi.org/10.55908/sdgs.v11i4.767

Katz, L. (2022). How victims matter: rethinking the significance of the victim in criminal theory. University of Toronto Law Journal. https://doi.org/10.3138/utlj.2021-0091

Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O., & Vergara, R. (2022). A systematic literature review on cybercrime legislation. F1000research, 11, 971. https://doi.org/10.12688/f1000research.123098.1

Killean, R. (2018). Constructing victimhood at the khmer rouge tribunal. International Review of Victimology, 24(3), 273-296. https://doi.org/10.1177/0269758017747645

Koziarski, J. and Lee, J. (2020). Connecting evidence-based policing and cybercrime. Policing an International Journal, 43(1), 198-211. https://doi.org/10.1108/pijpsm-07-2019-0107

Kuzmenko, V. and Kuzmenko, H. (2024). Problems of protecting rights of violent crimes victims: aspects of the harmonization process of ukrainian law with eu law. European Political and Law Discourse, 11(2), 51-61. https://doi.org/10.46340/eppd.2024.11.2.5

Maher, C. and Hayes, B. (2024). Nonfinancial consequences of identity theft revisited: examining the association of out-of-pocket losses with physical or emotional distress and behavioral health. Criminal Justice and Behavior, 51(3), 459-481. https://doi.org/10.1177/00938548231223166

Merdian, H., Perkins, D., Webster, S., & McCashin, D. (2019). Transnational child sexual abuse: outcomes from a roundtable discussion. International Journal of Environmental Research and Public Health, 16(2), 243. https://doi.org/10.3390/ijerph16020243

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B., Savolainen, I., Sirola, A., … & Paek, H. (2020). Situational and individual risk factors for cybercrime victimization in a cross-national context. International Journal of Offender Therapy and Comparative Criminology, 68(5), 449-467. https://doi.org/10.1177/0306624x20981041

Mwiraria, D., Ngetich, K., & Mwaeke, P. (2022). Factors associated with cybercrime awareness among university students in egerton university, njoro campus, nakuru county, kenya. European Journal of Humanities and Social Sciences, 2(3), 63-68. https://doi.org/10.24018/ejsocial.2022.2.3.256

Notté, R., Leukfeldt, R., & Malsch, M. (2021). Double, triple or quadruple hits? exploring the impact of cybercrime on victims in the netherlands. International Review of Victimology, 27(3), 272-294. https://doi.org/10.1177/02697580211010692

Nugroho, A. and Chandrawulan, A. (2022). Research synthesis of cybercrime laws and covid-19 in indonesia: lessons for developed and developing countries. Security Journal, 36(4), 651-670. https://doi.org/10.1057/s41284-022-00357-y

Palassis, A., Speelman, C., & Pooley, J. (2021). An exploration of the psychological impact of hacking victimization. Sage Open, 11(4). https://doi.org/10.1177/21582440211061556

Partin, R., Meldrum, R., Lehmann, P., Back, S., & Trucco, E. (2021). Low self-control and cybercrime victimization: an examination of indirect effects through risky online behavior. Crime & Delinquency, 68(13-14), 2476-2502. https://doi.org/10.1177/00111287211061728

Robalo, T. and Rahim, R. (2023). Cyber victimisation, restorative justice and victim-offender panels. Asian Journal of Criminology, 18(1), 61-74. https://doi.org/10.1007/s11417-023-09396-9

Shukurov, E. and Jafarov, U. (2023). Legal professionals' perspectives on the challenges of cybercrime legislation enforcement. ISSLP, 2(4), 25-31. https://doi.org/10.61838/kman.isslp.2.4.5

Weijer, S., Leukfeldt, R., & Zee, S. (2021). Cybercrime reporting behaviors among small- and medium-sized enterprises in the netherlands., 303-325. https://doi.org/10.1007/978-3-030-60527-8_17

Willits, D. and Nowacki, J. (2016). The use of specialized cybercrime policing units: an organizational analysis. Criminal Justice Studies, 29(2), 105-124. https://doi.org/10.1080/1478601x.2016.1170282