IPSO JURE JOURNAL

IPSO JURE

Journal

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Digital Crime In The Era Of Society 5.0: Juridical Analysis Of Cyber And Victim Protection

Wahyu Handoko
Universitas Terbuka, Indonesia

Received: March 22, 2025
Revised: April 22, 2025
Accepted: April 25. 2025
Published: April 30. 2025

Corresponding Author:
Author Name : Wahyu Handoko
Email : wahyuyuuki54@gmail.com

Abstract: *The development of digital technology in the era of Society 5.0 has presented new challenges in the form of increasing cybercrime that is complex, cross-border, and difficult to trace. On the other hand, Indonesia's legal system still focuses on punishing perpetrators, while protection for victims of digital crime has not received adequate attention. This study aims to analyze the effectiveness of applicable regulations juridically and highlight the need to change the legal paradigm from a retributive approach to a restorative one. This research uses normative legal methods with legislative, conceptual, and case approaches. The analysis was carried out on three main regulations: Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), Law Number 27 of 2022 concerning Personal Data Protection (PDP), and Articles 373–379 in the Draft Criminal Code. Case studies of incidents of ransomware, phishing, and high-tech digital crime show weak victim protection, low public trust in the legal system, and the absence of a proper compensation scheme. The results of the study show that legal protection for victims is still scattered, not integrated, and lacks a restorative approach. Therefore, legal reform is needed through the drafting of a special law on cybercrime, improving the competence of law enforcement, establishing victim service centers, and strengthening international cooperation. Law enforcement in the era of Society 5.0 must transform, placing victim recovery as an essential part of fair, adaptive, and civilized criminal justice.*

Keywords: Cybercrime, digital crime, normative law, restorative justice, Society 5.0, victim protection

INTRODUCTION

The development of the Society 5.0 era has brought about major changes in the social structure and way of life of humans. This concept puts technology at the core of society, integrating the physical and digital worlds to create a more efficient and human-centric life. Technologies such as the Internet of Things (IoT), artificial intelligence (AI), and big data are being used to address

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

social problems and improve people's quality of life [1]. One of the impacts of this transformation is the expansion of digital space (cyberspace) which is borderless, fast, and globally connected.

However, the advancement of digitalization not only brings benefits, but also opens new loopholes for the emergence of digital crime. Cybercrime has increased significantly in terms of volume and complexity. The forms are also very diverse, ranging from hacking, personal data theft, online fraud, to attacks on vital infrastructure. These crimes are cross-border and the perpetrators often take advantage of the weaknesses of digital security systems to carry out their actions .

During the increasing risk of digital crime, people are becoming more and more vulnerable. The impact experienced by victims is not only limited to financial losses, but also extends to psychological and social aspects. Many victims experience stress, anxiety, defamation, and social isolation due to crimes that occur in the digital realm . Unfortunately, many cases of digital crime go unreported because victims feel distrustful of the legal system, do not understand their rights, or fear privacy violations (Bergh & Junger, 2018; Beloded, 2023).

Legal protection for victims of cybercrime in Indonesia is currently still relatively weak. Existing regulations, such as the Electronic Information and Transaction Law (ITE Law) and the Personal Data Protection Law (PDP Law), do regulate criminal sanctions against perpetrators, but have not specifically focused on restoring victims' rights. The prevailing legal approach is more retributive than restorative, so that the fulfillment of justice for victims is less optimal.

In addition, the protection of cybercrime victims has not been comprehensively integrated into the national legal system. The available protections are scattered in various general regulations, such as Law No. 31 of 2014 concerning the Protection of Witnesses and Victims, which do not

[1] Burhanuddin and Pharmacista, “Transformation of Companies and Trade in the Era of Society 5.0”; Fontes, Carpentras, and Mahajan, “Human Digital Twins Unlocking Society 5.0? Approaches, Emerging Risks and Disruptions”; Nair, Tyagi, and Sreenath, “The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges”; Saracel and Aksoy, “Toplum 5.0: Süper Akıllı Toplum.”

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

specifically reg[23456789]ulate forms and mechanisms of protection for victims of digital crimes. In fact, until now, there has been no special institution or national assistance system structured to help cyber victims .

Several studies underscore the importance of regulatory reform and the establishment of integrated protection mechanisms for victims of digital crime. It is necessary to strengthen legal aspects, which include compensation, psychological rehabilitation, legal assistance, and the protection of victims' identity and personal data. This is important to ensure that victims are not only protected from perpetrators, but also obtain justice and comprehensive restoration.

Therefore, the urgency of cyber law reform in Indonesia cannot be ignored. This update must be carried out with a balanced approach between prosecuting the perpetrator and supporting the victim. Juridical analysis of the effectiveness of existing laws is important as a foundation for formulating the direction of sustainable and inclusive legal protection policies in the ever-evolving digital era.

Based on the inequality between the pace of development of digital crime in the Society 5.0 era and the still weak regulations that specifically protect victims, there is an urgent need to conduct a legal study that is not only oriented towards the prosecution of perpetrators, but also on the protection and recovery of victims as a whole. The absence of an integrated mechanism in

[2] Wemmers, "Victims' Experiences in the Criminal Justice System and Their Recovery from Crime."
[3] Suzuki, "Victim Recovery in Restorative Justice: A Theoretical Framework."
[4] Apriandi, Sagala, and Basuki, "PERLINDUNGAN HUKUM BAGI KORBAN CYBERCRIME PENYEBARAN DATA PRIBADI SECARA ONLINE"; Qotrunnada, "Perlindungan Ham Terhadap Kebocoran Data Pribadi Pasien Akibat Cyber Crime."
[5] Apriandi, Sagala, and Basuki, "PERLINDUNGAN HUKUM BAGI KORBAN CYBERCRIME PENYEBARAN DATA PRIBADI SECARA ONLINE"; Sitihastuti and Solikhah, "The Urgency of Legal Protection for Victims of Cyberbullying in Indonesia."
[6] Apriandi, Sagala, and Basuki, "PERLINDUNGAN HUKUM BAGI KORBAN CYBERCRIME PENYEBARAN DATA PRIBADI SECARA ONLINE"; Djanggih et al., "The Effectiveness of Law Enforcement on Child Protection for Cybercrime Victims in Indonesia"; Sitihastuti and Solikhah, "The Urgency of Legal Protection for Victims of Cyberbullying in Indonesia."
[7] Apriandi, Sagala, and Basuki, "PERLINDUNGAN HUKUM BAGI KORBAN CYBERCRIME PENYEBARAN DATA PRIBADI SECARA ONLINE"; Qotrunnada, "Perlindungan Ham Terhadap Kebocoran Data Pribadi Pasien Akibat Cyber Crime"; Sitihastuti and Solikhah, "The Urgency of Legal Protection for Victims of Cyberbullying in Indonesia"; Wardhana, "TINJAUAN YURIDIS PERLINDUNGAN KORBAN TERHADAP KEJAHATAN CYBER BULLYING DALAM SISTEM HUKUM PIDANA DI INDONESIA."
[8] Beloded, "Some Psychological Features of Victims of Crime Committed Using Digital Technologies"; Tonellotto, "Crime and Victimization in Cyberspace"; Virtanen, "Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities."
[9] Bergh and Junger, "Victims of Cybercrime in Europe: A Review of Victim Surveys"; Cotrina et al., "Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches"; Dahiya, "Trends in Cyber Crime in India."

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

Indonesia's positive law, both in terms of substance and institutionality, shows that there is a normative and implementive gap that needs to be analyzed juridically. Therefore, this research is directed to examine in depth the forms of digital crime and the effectiveness of legal protection for victims, to formulate legal policy recommendations that are adaptive and responsive to the challenges of the evolving digital world.

METHOD

This research uses a normative legal research method, which is research that aims to examine legal principles, laws and regulations, and doctrines relevant to digital crime in the era of Society 5.0 and the protection of victims of cybercrime. The approach used in this study includes a statute approach, by analyzing regulations such as Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 27 of 2022 concerning Personal Data Protection. In addition, a conceptual approach is also used to understand basic concepts related to digital crime and victim protection, as well as a case approach by examining several examples of real cases of cybercrime that occur in Indonesia.

The sources of legal materials in this study consist of primary legal materials, namely laws and regulations and court decisions; secondary legal materials, in the form of literature, journal articles, and expert opinions; as well as tertiary legal materials such as legal dictionaries and legal encyclopedias. The technique of collecting legal materials is carried out through library research, by examining various legal documents, scientific literature, and other reliable sources. All legal materials collected were analyzed qualitatively, namely by systematically describing and interpreting data to produce an analytical description of legal protection for victims of digital crime in the era of Society 5.0.

RESULTS AND DISCUSSION

THE DYNAMICS OF DIGITAL CRIME IN THE ERA OF SOCIETY 5.0

The transformation towards Society 5.0, where the integration between the virtual world and the real world is getting closer, has expanded the space of crime to be unlimited in time and territory. Cyber crime now includes a series of crimes such as data theft, system hacking, online fraud, and attacks on critical infrastructure.

In this study, a study was conducted based on a statutory approach

- Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), which regulates electronic transactions, cybercrime, and electronic evidence.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

- Law Number 27 of 2022 concerning Personal Data Protection, which clarifies the rights of data subjects and the obligations of data controllers to protect personal information, which is often the object of digital crimes.
- Additional provisions in the Draft Criminal Code also cover crimes related to informatics and telematics (Articles 373–379).

However, the provisions in the ITE Law and the PDP Law have not been fully responsive to new technological developments, such as crimes involving artificial intelligence, blockchain, and large-scale cyberattacks. On the other hand, law enforcement still faces technical obstacles such as limited human resources and lack of advanced digital detection tools.

JURIDICAL STUDY OF LAWS AND REGULATIONS RELATED TO DIGITAL CRIMES

1. Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE)

The ITE Law is the earliest and main legal instrument in tackling digital crime in Indonesia. This law regulates various aspects of electronic activities, ranging from the recognition of electronic documents and signatures, to the regulation of cybercrimes such as illegal access, data manipulation, online defamation, to the dissemination of prohibited content. Juridically, the ITE Law provides a legal basis for accepting electronic evidence as valid evidence in judicial proceedings, as stipulated in Articles 5 and 6. This is important for the adaptation of criminal law to new forms of crime that do not leave physical traces, but digital traces. However, in practice, the various interpretations and application of certain articles (e.g. Article 27 paragraph (3) on defamation) have caused controversy, and even have the potential to limit freedom of expression in the digital space. The ITE Law also does not comprehensively protect victims of digital crime. The main focus of this law is still on the prosecution of the perpetrators, not on the recovery of the victims' losses. Therefore, it is necessary to strengthen the norms in the ITE Law that are oriented towards victims' rights and improve the recovery mechanism.

2. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)

The PDP Law is an important milestone in strengthening regulations on the protection of private rights in the digital era. In the era of Society 5.0, where data has become a strategic commodity, this law exists to balance the need for data utilization and the protection of individuals as data subjects. Juridically, the PDP Law establishes important principles such as explicit consent, the right to access and correction of data, and the right to be forgotten. Data controllers and data processors are required to maintain the security and confidentiality of personal data, and are

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

responsible in the event of leakage or misuse. The PDP Law also contains criminal provisions for serious violations of data protection, including unauthorized processing and illegal distribution of personal data. This is important because many cases of digital crimes (such as phishing, social engineering, and online fraud) start from the theft of personal data. However, the challenges in implementing the PDP Law are very large, especially due to the limited capacity of independent supervisory institutions, as well as low public literacy related to the right to personal data. Strengthening technical regulations and massive socialization are needed to encourage compliance and effective enforcement.

3. *Draft Criminal Code (RKUHP) Articles 373–379*

In the RKUHP, which is being prepared as a comprehensive update of the national criminal law, special regulations related to information and telematics crimes have been contained in Articles 373 to 379. This arrangement confirms that cybercrime is already an inherent part of the modern criminal law structure.
These articles include:

- Illegal access (access to electronic systems without permission),
- Illegal interception,
- Data and system interference,
- Domain name misuse, up to
- Electronic dissemination of child pornography content.

This arrangement is proof that Indonesia's substantive criminal law is beginning to recognize new forms of crime that were not previously explicitly covered in the old Criminal Code. From a normative point of view, the inclusion of this provision in the RKUHP is a step forward. However, to be effective, it needs to be aligned with the criminal procedure law that allows digital proof and pays attention to the principles of restorative justice, especially in the recovery of victims of digital crimes.

CYBERCRIME VICTIM PROTECTION: A NORMATIVE LEGAL PERSPECTIVE

Within the normative legal framework, the protection of victims of cybercrime is seen as an integral part of the human rights protection that the state must guarantee. This approach departs from the basic principle that the law does not only function to punish the perpetrator, but also to restore the victim's condition to its original state, according to the principle of restorative justice.
Through a conceptual approach, victim protection includes four main components:

- Restitution: Compensation for losses suffered by victims due to crimes.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

- Psychosocial rehabilitation: Medical, psychological, or social assistance to restore the victim's condition.
- Restoration of rights: Restoration of impaired personal, economic, or social rights.
- Information and legal assistance: The victim's right to obtain information about the legal process and to be accompanied in fighting for his rights.

In the Indonesian context, the protection of victims of cybercrime has not received optimal legislative attention. Normatively:

- Law Number 31 of 2014 concerning the Protection of Witnesses and Victims provides a general basis for protection, but its scope is broader in cases of physical violence, terrorism, or conventional crimes, not specifically cybercrimes.
- The ITE Law (Law Number 11 of 2008) regulates more criminal acts and sanctions against perpetrators (prison, fines), as well as the regulation of electronic evidence. Protection for victims, such as compensation or restoration of good faith, is not explicitly regulated.
- The PDP Law (Law Number 27 of 2022) clarifies the rights of data subjects, but when a violation occurs, the protection mechanism is still limited to administrative or criminal sanctions against the perpetrator, without an automatic compensation scheme for victims of personal data leaks.

Seeing this, from a normative legal perspective, legal protection for victims of cybercrime in Indonesia is still retributive: the main focus is on punishing the perpetrator, not restorative, which is restoring the victim's position as it was before the crime occurred.
This indicates that there is a normative gap in the national legal system. Ideally, every digital crime should be accompanied by arrangements that guarantee:

- The victim's right to obtain information about the legal process.
- The right to restitution, either from the perpetrator or through state mechanisms if the perpetrator is incapacitated.
- The right to psychosocial rehabilitation, especially in cases of online defamation or personal data breaches.

In the context of modern criminal law, this normative approach is in line with international principles, as contained in the Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law (UN, 2005), which requires states to adopt policies that restore the position of victims. Thus, through a normative legal approach, it can be emphasized that the protection of victims of cybercrime requires strengthening special regulations that are oriented to the interests of the victim, not solely the punishment of the perpetrator. Indonesia's criminal law in the future must move from a retributive

IPSO JURE JOURNAL

IPSO JURE

Journal

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

paradigm to a restorative paradigm, in order to realize substantive justice for all citizens in the digital era.

CASE STUDY: REFLECTION ON CYBER CASE HANDLING IN INDONESIA

The case approach in this normative legal research aims to explore real challenges in victim protection and law enforcement against cybercrime in Indonesia. Some prominent incidents can be used as illustrations to understand the complexity:

1. Ransomware Attacks on Government Agencies

The case of ransomware attacks that befell several local government agencies shows significant weaknesses in national cyber preparedness. The mode used involves encrypting the agency's important data, which is then held hostage with a ransom demand in the form of cryptocurrency.
From a normative point of view:

- The lack of digital forensic investigation capacity causes delays in data recovery and perpetrator tracking.
- Institutional victims are often reluctant to report incidents publicly to avoid reputational damage, thus slowing down national coordination in dealing with incidents.
- There is no protection scheme or compensation for losses suffered, either to disrupted public services or to individuals whose data is involved in attacks.

This condition indicates the need for emergency protocols and compensation regulations for third parties affected by cybersecurity failures in the public sector.

2. *Mass Phishing Scam Cases*

Phishing incidents that occur massively, especially attacking users of digital banking services, illustrate the challenges of public education in information security.
The findings of this case approach show:

- The low digital security literacy of the community increases the vulnerability of individuals to become victims.
- Victims who are deceived generally lose access to their financial accounts, but often do not get a fair recovery of funds because they are considered negligent by the banks.
- Legal processes to pursue phishing perpetrators are difficult because perpetrators often use anonymous networks and cross-border infrastructure.

From a normative legal perspective, phishing victim protection has not been explicitly regulated. There needs to be regulations that require digital service providers, especially the financial sector,

IPSO JURE JOURNAL

IPSO JURE

Journal

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

to take responsibility for the security of their services and compensate victims under certain conditions.

3. *Crimes Using High-Level Encryption*
The use of advanced encryption technology in digital crimes, such as the smuggling of confidential data or the obfuscation of identity in cyberattacks, further hampers the evidentiary process in the legal realm.

In this case study it was found:

- The limitations of digital forensic technology in Indonesia make it difficult for the authorities to open or trace the perpetrator's encrypted files.
- International cooperation in cybercrime investigations involving encryption is still minimal, prolonging the legal process.
- Often victims of this type of crime, both individuals and corporations, suffer financial and reputational losses without adequate recovery schemes or legal assistance.

This shows the need to strengthen the technical capacity of law enforcement officials through investment in advanced forensic tools and increased extradition cooperation for cybercrime.

General Reflections from Case Studies
From these three cases, several important patterns can be deduced:

- Lack of victim restitution: In almost all cases, victims rarely receive compensation or restoration of rights, underscoring the weak orientation of victim protection in national cyber law.
- Low public trust in the legal system: Many victims choose not to report because the legal process is considered complicated, expensive, or ineffective.
- The absence of specific regulations for the protection of victims of cybercrime leads to a gap between the needs of victims and the legal protections available.

Therefore, this approach to the case emphasizes the importance of Indonesia's cyber law reform to not only prioritize the prosecution of perpetrators, but also prioritize the recovery of victims as part of civilized criminal justice.

IPSO JURE JOURNAL

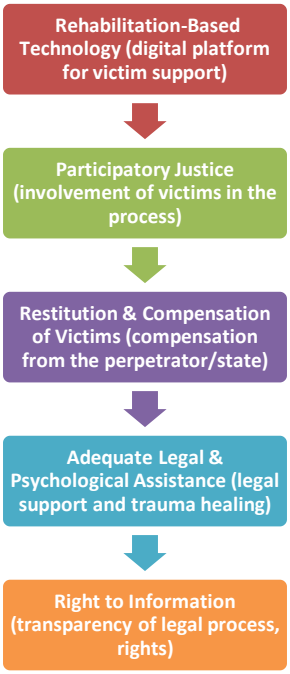
IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

LEGAL IMPLICATIONS AND RECOMMENDATIONS FOR STRENGTHENING PROTECTION



Based on the results of the analysis, reforms are needed in the Indonesian legal framework, namely:

- Drafting special cybercrime laws that are oriented towards victims' rights, including the obligation of restitution and compensation by perpetrators.
- Improving the competence of law enforcement officials through continuous digital forensic and cybersecurity training.
- Establish an integrated service center for victims of digital crime, providing legal, psychosocial, and technical support services.
- Strengthen international cooperation, both through the ratification of cyber crime conventions such as the Budapest Convention and the establishment of an effective extradition mechanism for transnational cybercrime.

Through a normative legal approach that examines the applicable principles, doctrines, and regulations, it is clear that the challenges of the Society 5.0 era demand not only regulatory adaptation, but also a paradigm shift in law enforcement: from a focus on punishing perpetrators to an orientation on victim recovery as part of civilized justice. Reflections from case studies on handling cybercrime in Indonesia show that there is an urgent need to change the legal approach

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

from simply focusing on punishing perpetrators to recovering victims. This paradigm shift is supported by various previous studies that emphasize the importance of a restorative justice approach in the modern legal system.

Suzuki (2023) emphasized that restorative justice, which was initially applied to misdemeanors, is now also relevant for serious crime cases, including digital crimes. Restorative justice is able to support the victim recovery process through the recognition of the perpetrator's mistakes, the victim's involvement in the legal process, and the provision of adequate social support. In addition, Wemmers (2013) shows that the treatment of victims in the criminal justice system has a significant influence on their psychological recovery. Fair procedures and respect for the victim's voice accelerate emotional recovery, while unfair treatment exacerbates trauma . This is in line with the findings of Macleod and Paton (1999), who developed a victim recovery model based on social-psychological support, especially for victims of crime who experience recurrent trauma [10]. Furthermore, Kunst et al. (2015) in their study found a positive relationship between victims' satisfaction with the justice system and their emotional recovery process.

However, the quality of the legal handling methodology applied to victims is a key factor in success [11]. In the context of Society 5.0 innovation, Dawiya et al. (2022) developed a technology-based guide for the social rehabilitation of victims of violence, which demonstrates the effectiveness of the use of digital platforms in supporting victim recovery. This kind of innovation is important for wider adoption in the protection of victims of cybercrime [12]. These studies consistently support the urgency of a paradigm shift in cyber law enforcement in Indonesia, from a retributive model to a model that prioritizes victim recovery through the principle of restorative justice. This is an important foundation for encouraging regulatory reform, law enforcement practices, and strengthening support services for victims of cybercrime in an increasingly complex digital era.

[10] Macleod and Paton, “Victims, Violent Crime and the Criminal Justice System: Developing an Integrated Model of Recovery.”
[11] Kunst, Popelier, and Varekamp, “Victim Satisfaction With the Criminal Justice System and Emotional Recovery.”
[12] Dawiya, Rinekasari, and Achdiani, “Developing Web-Based Practical Procedure Guidance for Social Rehabilitation in The Society 5.0 Era.”

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

CONCLUSIONS

In the era of Society 5.0, where the integration of digital technology and real life has become increasingly close, fundamental changes in the structure of society have occurred, accompanied by the rapid growth of digital or cybercrime in terms of volume, type, and complexity. Although Indonesia has enacted several regulations such as the ITE Law and the PDP Law, victim protection remains suboptimal both normatively and in implementation. This study reveals that Indonesia's national legal approach is still largely retributive—prioritizing the punishment of perpetrators—while neglecting the recovery and rights of victims. The protection of victims is still fragmented across various general laws and does not specifically address essential needs such as restitution, psychosocial rehabilitation, personal data protection, and access to legal aid. A review of the ITE Law, PDP Law, and Draft Criminal Code shows normative gaps in guaranteeing comprehensive victim rights. Case studies of cybercrime in Indonesia, including ransomware attacks, mass phishing, and advanced encryption misuse, further underscore the inadequacy of current victim protection mechanisms and the resulting low public trust in the justice system. Therefore, cyber law reform is urgently needed, focusing on the formulation of a victim-oriented cybercrime law, enhancement of law enforcement's digital forensic capabilities, establishment of integrated victim service centers, and reinforcement of international cooperation to address cross-border cybercrime. In this way, to effectively confront the challenges of digital crime in the Society 5.0 era, Indonesia must adopt a legal system that is not only repressive toward perpetrators but also transformative and restorative for victims, thereby promoting civilized and sustainable justice..

REFERENCES

Apriandi, Muliawansyah, Rotua Valentina Sagala, and Basuki Basuki. "PERLINDUNGAN HUKUM BAGI KORBAN CYBERCRIME PENYEBARAN DATA PRIBADI SECARA ONLINE." SINERGI : Jurnal Riset Ilmiah, November 20, 2024. https://doi.org/10.62335/rxca0x19.

Beloded, D. "Some Psychological Features of Victims of Crime Committed Using Digital Technologies." Victimology, July 13, 2023. https://doi.org/10.47475/2411-0590-2023-10-3-320-334.

Bergh, C. Reep-Van Den, and M. Junger. "Victims of Cybercrime in Europe: A Review of Victim Surveys." Crime Science 7 (April 4, 2018). https://doi.org/10.1186/s40163-018-0079-3.

Burhanuddin, Sisca Ferawati, and Gandhi Pharmacista. "Transformation of Companies and Trade in the Era of Society 5.0." International Journal of Science and Society, December 11, 2023. https://doi.org/10.54783/ijsoc.v5i5.973.

Cotrina, Lisseth Katherine Chuquitucto, Pedro Manuel Silva León, Carla Angélica Reyes Reyes, Marco Agustín Arbulú Ballesteros, María De Los Ángeles Guzmán Valle, Julie Catherine Arbulú Castillo, Rafael Martel Acosta, and Ana Elizabeth Paredes Morales. "Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches." Journal of Educational and Social Research, September 5, 2024. https://doi.org/10.36941/jesr-2024-0124.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

Dahiya, Kashish. "Trends in Cyber Crime in India." International Journal for Research in Applied Science and Engineering Technology, May 31, 2023. https://doi.org/10.22214/ijraset.2023.53073.

Dawiya, Naufal Libna, N. Rinekasari, and Y. Achdiani. "Developing Web-Based Practical Procedure Guidance for Social Rehabilitation in The Society 5.0 Era." Jurnal Ilmiah Pendidikan Teknik Dan Kejuruan, December 6, 2022. https://doi.org/10.20961/jiptek.v15i2.67586.

Djanggih, Hardianto, H. Thalib, H. Baharuddin, Nurul Qamar, and A. Ahmar. "The Effectiveness of Law Enforcement on Child Protection for Cybercrime Victims in Indonesia." Journal of Physics: Conference Series 1028 (June 1, 2018). https://doi.org/10.1088/1742-6596/1028/1/012192.

Fontes, Catarina, Dino Carpentras, and Sachit Mahajan. "Human Digital Twins Unlocking Society 5.0? Approaches, Emerging Risks and Disruptions." Ethics Inf. Technol. 26 (August 12, 2024): 54. https://doi.org/10.1007/s10676-024-09787-1.

Kunst, M., Lieke Popelier, and Ellen Varekamp. "Victim Satisfaction With the Criminal Justice System and Emotional Recovery." Trauma, Violence, & Abuse 16 (July 1, 2015): 336–58. https://doi.org/10.1177/1524838014555034.

Macleod, M., and D. Paton. "Victims, Violent Crime and the Criminal Justice System: Developing an Integrated Model of Recovery." Legal and Criminological Psychology 4 (September 1, 1999): 203–20. https://doi.org/10.1348/135532599167851.

Nair, M., A. Tyagi, and N. Sreenath. "The Future with Industry 4.0 at the Core of Society 5.0: Open Issues, Future Opportunities and Challenges." 2021 International Conference on Computer Communication and Informatics (ICCCI), January 27, 2021, 1–7. https://doi.org/10.1109/ICCCI50826.2021.9402498.

Qotrunnada, Salsabilla Diva. "Perlindungan Ham Terhadap Kebocoran Data Pribadi Pasien Akibat Cyber Crime." Global Education Journal, May 22, 2023. https://doi.org/10.59525/gej.v1i2.261.

Saracel, Nüket, and Irmak Aksoy. "Toplum 5.0: Süper Akıllı Toplum" 9 (June 15, 2020): 26–34.

Sitihastuti, Sholikah, and Solikhah Solikhah. "The Urgency of Legal Protection for Victims of Cyberbullying in Indonesia." Jurnal Cakrawala Hukum, September 26, 2024. https://doi.org/10.26905/idjch.v15i1.12025.

Suzuki, Masahiro. "Victim Recovery in Restorative Justice: A Theoretical Framework." Criminal Justice and Behavior 50 (October 18, 2023): 1893–1908. https://doi.org/10.1177/00938548231206828.

Tonellotto, Maurizio. "Crime and Victimization in Cyberspace," 2020, 248–64. https://doi.org/10.4018/978-1-7998-1286-9.ch014.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.3, April 2025
DOI : https://doi.org/10.62872/arpt6m43

Virtanen, S. “Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities.” Psychiatry, Psychology and Law 24 (May 4, 2017): 323–38. https://doi.org/10.1080/13218719.2017.1315785.

Wardhana, Abiil. “TINJAUAN YURIDIS PERLINDUNGAN KORBAN TERHADAP KEJAHATAN CYBER BULLYING DALAM SISTEM HUKUM PIDANA DI INDONESIA,” November 1, 2018. https://consensus.app/papers/tinjauan-yuridis-perlindungan-korban-terhadap-kejahatan-wardhana/e86d0c5ce591572e9ebe2962f788bd08/.

Wemmers, Jo-Anne. “Victims’ Experiences in the Criminal Justice System and Their Recovery from Crime.” International Review of Victimology 19 (July 15, 2013): 221–33. https://doi.org/10.1177/0269758013492755.

.