IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

Cybercrime and Transnational Criminal Law: Tackling Online Fraud and Identity Theft

Yusep Mulyana
[1]Universitas Pasundan, Jawa Barat, Indonesia

Received: July 23, 2025
Revised: August 27, 2025
Accepted: September 01 , 2025
Published: September 24, 2025

Corresponding Author:
Author Name*: Yusep Mulyana
Email*:
yusepmaulana09@gmail.com

***Abstract*:** *The development of information and communication technology has presented new opportunities as well as challenges in the life of the global community. One of the negative impacts of digital transformation is the emergence of various forms of cybercrime, especially online fraud and identity theft. These two crimes have transnational characteristics so that they are difficult to deal with with national law alone. This study uses a normative juridical method with a qualitative approach to analyze national regulations and relevant international legal instruments in countering cybercrime. The results of the study show that Indonesia already has a legal basis through the ITE Law, the Criminal Code, and the Personal Data Protection Law, but still faces obstacles in terms of jurisdiction, capacity of law enforcement officials, and limitations of international agreements. At the global level, the Budapest Convention on Cybercrime and the United Nations Convention against Transnational Organized Crime (UNTOC) are important instruments, although their implementation is limited by the lack of universal state participation. Therefore, it is necessary to strengthen national regulations, increase international cooperation through extradition mechanisms and mutual legal assistance, and digital literacy of the public to prevent the widespread impact of online fraud and identity theft.*

Keywords: Cybercrime, Transnational Criminal Law, Online Fraud, Identity Theft

INTRODUCTION

The development of information and communication technology in the last two decades has brought fundamental changes to the social, economic, and cultural interaction patterns of the global community. Digital transformation, which is characterized by the widespread use of the internet, social media, and electronic commerce (e-commerce), has opened up new opportunities to increase efficiency, speed up transactions, and facilitate access to information regardless of geographical boundaries. However, this technological advancement not only brings benefits, but also gives birth to serious challenges in the form of cybercrime or known as cybercrime. Cybercrime develops along with human dependence on digital technology and is very dynamic, because the mode used by perpetrators continues to adapt to the development of security and technology systems.[1]

[1] Amory, J. D. S., & Mudo, M. (2025). Transformasi ekonomi digital dan evolusi pola konsumsi: Tinjauan literatur tentang perubahan perilaku belanja di era internet. Jurnal Minfo Polgan, 14(1), 28-37.

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

The two forms of cybercrime that stand out and cause the most victims are online fraud and identity theft. Online fraud is carried out by exploiting the vulnerability of internet users through various modes, such as fictitious investments, online shopping scams, to phishing and scamming schemes that trap victims to provide personal data or transfer funds[2]. On the other hand, identity theft is often carried out by taking or misusing a person's personal information, such as credit card numbers, social media accounts, and population data, for criminal purposes, including opening a new bank account, applying for a loan, or making illegal purchases. This crime not only harms the victim materially, but also has an impact on psychological and social aspects, and can even cause reputational damage that is difficult to recover.[3]

Both forms of crime have complex characteristics, one of which is transnational. An online fraudster, for example, may be in country A, while the victim is in country B, and the server or network used to commit the crime is located in country C. This cross-border configuration poses serious problems in law enforcement, especially related to jurisdiction, court competence, and differences in criminal law regulations between countries[4]. The borderless nature of cybercrime makes the state unable to solve the problem unilaterally, so a comprehensive international cooperation mechanism is needed. The challenge is even greater when a country's national law has not fully accommodated cybercrime adequately, or even has no special regulations regarding these crimes.[5]

In the context of transnational criminal law, the issue of handling cybercrime receives special attention because of its impact that is not limited to one jurisdiction alone. International instruments such as the United Nations Convention against Transnational Organized Crime (UNTOC) and the Budapest Convention on Cybercrime have become a foothold in building a common legal framework[6]. However, implementation at the national and regional levels still faces obstacles, both in terms of regulatory limitations, lack of capacity of law enforcement officials, and low public awareness of the dangers of cybercrime. Efforts to counter online fraud and identity theft require synergy between various countries through extradition mechanisms, mutual legal assistance, and harmonization of material and formal criminal laws relevant to the characteristics of digital crime.

To explain this problem, this study uses a transnational criminal law theory framework that emphasizes the importance of recognizing the principle of jurisdiction, both territorial jurisdiction, active and passive personality, and universal jurisdiction. This framework is important because cybercrime often involves multiple jurisdictions at once, creating conflicts of authority in the law enforcement process. In addition, cybercrime theory is used to understand the distinctive nature of digital crime which is characterized by

[2] Butarbutar, R. (2023). Cybercrime against individuals: Types, analysis and development. Technology and Economics Law Journal, 2(2), 3.

[3] BAKARA, P. L. (2024). Perlindungan Hukum Terhadap Korban Pencurian Identitas Digital Dalam Kejahatan Cybercrime.

[4] Budiyanto, S. H. (2025). Introduction to Cybercrime in the Criminal Law System in Indonesia. And the Library of Congress.

[5] Tekayadi, S., Sumerah, S., & Efendi, S. (2025). Challenges of Cyber Law Enforcement in the Cross-Border Era and Global Harmonization Efforts. Journal of Notary Treatises, 6(1), 265-276.

[6] Sinaga, W. S. (2023). Efforts to counter transnational crime are organized in cases of human smuggling. The Threat of Transnational Crime, 225.

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

anonymity, speed, and the ability to transcend national borders. This perspective helps to see that online fraud and identity theft are not just classic criminal acts that have been moved into the digital space, but are new forms of criminality that demand the adaptation of criminal law. This framework is strengthened by the theory of international cooperation in law enforcement which emphasizes the importance of multilateral and bilateral instruments to ensure the effectiveness of cross-border crime action.[7]

The existing literature shows that cybercrime, particularly online fraud and identity theft, has been widely discussed in technological studies and national laws. Several studies emphasize the global economic losses caused, where online fraud is said to cost billions of dollars every year, while identity theft is a serious threat to the security of personal data which is now an important asset in the digital economy[8]. In Indonesia, legal studies underscore the still weak national regulations and the limited capacity of law enforcement officials to deal with cross-border crimes. Although the Electronic Information and Transaction Law (ITE Law) regulates cybercrimes, implementation is often constrained by differences in jurisdiction, limited access to electronic evidence, and the lack of international agreements that can support extradition processes and mutual legal assistance.[9]

At the international level, the Budapest Convention on Cybercrime is often referred to as the most comprehensive legal instrument in dealing with cybercrime. This convention promotes the harmonization of national laws of member states, facilitates international cooperation, and regulates information exchange mechanisms in handling cyber cases. However, not all countries are parties to this convention, including most developing countries, so its effectiveness is still limited. On the other hand, UNTOC provides a general framework for cooperation between countries in tackling cross-border crime, although its scope is not specific to the issue of cybercrime. This literature review shows that although international legal instruments have existed, studies that specifically examine the relationship between online fraud, identity theft, and transnational criminal law are still rare.[10]

Thus, there is a research gap that needs to be filled, namely the lack of studies that emphasize a transnational approach in tackling online fraud and identity theft. Most previous studies have focused on normative analysis at the national level, while research on the implementation of international legal instruments, mechanisms of cooperation between countries, and barriers to cross-jurisdictional law enforcement is still limited. Therefore, this research is here to make an academic contribution by examining more deeply how transnational criminal law can be used as a normative framework in dealing with online fraud and identity theft, while offering a new perspective on the importance of global cooperation in facing the challenges of cybercrime in the digital era.[11]

[7] Ba'abud, M. F. R. (2023). Application of the Principle of Extraterritorial Jurisdiction to Perpetrators of Personal Data Theft Committed Across Borders (Doctoral Dissertation, Islamic University of Indonesia).

[8] DHARMAYANTI, Y. P. (2025). Criminal Law Policy In An Effort To Overcome Artificial Intelligence (AI) In Cyber Crime (Doctoral dissertation, Sultan Agung Islamic University Semarang).

[9] IQBAL, M. (2025). The Role Of The Police Intelligence Unit In The Investigation Of Murder (Case Study At The Natuna Resort Police) (Doctoral dissertation, Sultan Agung Islamic University Semarang).

[10] Febrian, W. R., Faturrahman, R. M. R., Rahmadina, H. S., & Deni, F. (2024). The role of international law in handling cyber crime cases. JOURNAL OF SAHID DA'WATII, 3(02), 1-7.

[11] Chandra, E. (2024). Effectiveness of the Investigation of Love Scamming Mode Fraud at the Barelang Resort Police, Batam City (Doctoral dissertation, Sultan Agung Islamic University, Semarang).

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

METHOD

This study uses a normative juridical method with a comparative and qualitative approach. The normative juridical approach is chosen to examine the legal norms contained in national regulations and international legal instruments. The primary legal sources used include Law Number 11 of 2008 jo. Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE Law), Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), Criminal Code (KUHP), Budapest Convention on Cybercrime 2001, and United Nations Convention against Transnational Organized Crime (UNTOC) 2000. Secondary legal sources are obtained from academic literature, such as articles from international journals indexed by Scopus and Web of Science, international criminal law books, reports of international institutions (UNODC, Interpol), and national data from the State Cyber and Cryptography Agency (BSSN). The analysis was carried out through legal interpretation, comparison of regulations between countries (Indonesia, the European Union, the United States, and Singapore), and association with cross-border cybercrime case studies. The research limits are set on two forms of cybercrime, namely online fraud and identity theft, so that the analysis can be more focused and in-depth.

In the international literature, the issue of cybercrime has been widely discussed. Several studies highlight the importance of cybersecurity literacy (Bada & Sasse, 2019), the challenges of legal harmonization in the implementation of the Budapest Convention (Chawki, 2016), and Southeast Asia's high vulnerability to phishing and love scams (Broadhurst et al., 2021). The European Union through the implementation of the General Data Protection Regulation (GDPR) is considered successful in tightening the protection of personal data (Voigt & Von dem Bussche, 2017), while the United States relies on the Identity Theft and Assumption Deterrence Act to strengthen the legal protection of its citizens. In Asia, Singapore through the Personal Data Protection Act (PDPA) is also an example of relatively advanced regulation. Nonetheless, most of the literature is still limited to domestic analysis or focuses on the protection of personal data. There have not been many studies that specifically link online fraud and identity theft to the transnational criminal law framework, especially in Southeast Asia which faces jurisdictional fragmentation and weak legal harmonization. This research is here to fill this gap by connecting national legal norms, international legal instruments, and actual case studies. Thus, this article offers novelty in the form of theoretical contributions in enriching the discourse of transnational criminal law as well as relevant policy recommendations at the national, regional, and global levels.

DISCUSSION

1. Characteristics of Online Fraud and Identity Theft as Cybercrimes

Online fraud and identity theft basically show the evolution of forms of crime that adapt to the advancement of digital technology. If conventional fraud is usually carried out through face-to-face interaction, then in cyberspace, the mode used is more sophisticated because it takes advantage of trust gaps, system weaknesses, and low digital literacy of the community. Forms of online fraud are not only limited to fake advertisements in e-commerce or phishing messages, but also penetrate the financial sector with business email compromise modes, fake crypto investments, and fraud based on illegal online lending applications[12]. The impact is not only individual, but also systemic, as it can undermine public trust in digital platforms and electronic payment systems that are the backbone of the modern economy. On the other hand, identity theft has become one of the most threatening forms of crime in the digital age as it concerns the loss of an

[12] Simanungkalit, J. A. R., Hertadi, R., & ul Hosnah, A. (2024). Analysis of Online Fraud Crimes in the Context of Criminal Law How to Deal With and Prevent It. *ACADEMIC: Journal of Humanist Students*, *4*(2), 281-294.

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

individual's control over his or her personal data. Stolen personal data is not only used for short-term financial gain, but can also be traded on the digital black market (dark web), and even used for broader criminal activities, including terrorism financing and cross-border money laundering. Thus, the main characteristic of these two forms of crime is losses that are multidimensional, covering economic, social, and national security aspects[13].

In addition, the uniqueness of online fraud and identity theft is that they are transnational, anonymous, and very difficult to trace. Technologies such as virtual private networks (VPNs), end-to-end encryption, the use of cryptocurrencies, and the existence of the dark web make perpetrators virtually untouched by the territorial-based national legal system. This situation creates a serious challenge for law enforcement officials who have to deal with digital evidence that is volatile, easily manipulated, and often spread across several different jurisdictions. For example, a perpetrator may be in country A, the server used is in country B, the victim is in country C, and financial transactions take place through a distributed global system. This complexity shows that cybercrime, especially online fraud and identity theft, is not just a shift in the form of classic crimes, but a new category of digital crime that demands a holistic approach. This approach not only includes national criminal law instruments, but also requires international cooperation mechanisms, strengthening digital investigation technology, and active participation of the public in maintaining the security of personal data. With these characteristics, cybercrime puts transnational criminal law in a strategic position to become the main instrument in the face of the ever-increasing threat of modern criminality.[14]

2. National and International Regulations in Cybercrime Prevention

Indonesia's national regulations in dealing with cybercrime have basically undergone significant developments since the enactment of Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE) which was later revised through Law Number 19 of 2016. The ITE Law serves as the main legal instrument to ensnare various criminal acts in the digital space, including online fraud and identity theft. For example, Article 28 paragraph (1) regulates the prohibition of the dissemination of false information that harms consumers in electronic transactions, while Articles 30 and 32 ensnare perpetrators of illegal access and data manipulation that are closely related to identity theft. However, the implementation of these articles faces serious challenges in practice, especially related to the proof and availability of digital evidence that is often outside Indonesia's jurisdiction. The Criminal Code also remains relevant in certain contexts, for example through Article 378 on fraud and Article 263 on forgery, although its application does not specifically target digital [15]crimes. Another legal breakthrough is the presence of the Personal Data Protection Law (PDP Law) in 2022, which provides a stronger legal basis to protect individuals from misuse of personal data. Even so, the effectiveness of the PDP Law is still waiting for the ratification of more technical derivative rules, as well as the readiness of law enforcement agencies to implement them optimally. This shows that even though national legal instruments are available,

[13] Kadir, Z. K. (2025). Digital Identity-Based Crime: Initiating Criminal Policy for the Metaverse World. Amsir Journal of Litigation, 12(2), 124-137.

[14] Butarbutar, J. M. (2025). The Digital Revolution and Criminological Challenges: An Analysis of Crime Trends in the Digitalization Era. *Media Legal Indonesia (MHI), 3*(2).

[15] Hutabarat, S. A., Praja, S. J., Suhariyanto, D., Paminto, S. R., Kusumastuti, D., Fajrina, R. M., ... & Abas, M. (2023). CYBER-LAW: Quo Vadis Regulation of the ITE Law in the Industrial Revolution 4.0 Towards the Era of Society 5.0. PT. Sonpedia Publishing Indonesia.

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

Indonesia's regulatory framework still needs to be strengthened in technical aspects, institutional capacity, and inter-institutional synergy[16].

Meanwhile, at the international level, the Budapest Convention on Cybercrime (2001) was an important milestone in the global effort to tackle cybercrime. The Convention is considered the first legal instrument to specifically regulate computer-based crimes, while promoting the harmonization of substantive law between countries and strengthening international cooperation mechanisms. One of the innovations is the provision on expedited preservation of stored computer data, which provides a legal basis for member states to immediately secure digital evidence across jurisdictions before it is lost or destroyed. However, the effectiveness of this convention is still limited because it is not universal, considering that major countries such as Russia, China, and some Southeast Asian countries, including Indonesia, have not ratified it. In addition, the United Nations Convention against Transnational Organized Crime (UNTOC) 2000 also provides an important framework through extradition mechanisms, mutual legal assistance, and cross-border asset freezes[17]. Although not specifically designed for cybercrime, UNTOC can be applied to cases of online fraud and identity theft carried out in an organized cross-border manner. Thus, both at the national and international levels, the legal framework is actually in place, but gaps are still evident, especially in the aspects of regulatory harmonization, cross-border coordination, and political commitment to strengthen legal connectivity in the face of the transnational nature of cybercrime.

In Indonesia, the implementation of national regulations in cases of online fraud can be seen in a number of cases handled by the police through Cyber Patrol. For example, in the case of online shopping fraud on e-commerce platforms, perpetrators often use fake accounts and take advantage of consumer negligence to gain profits. Several cases were successfully charged with Article 28 paragraph (1) of the ITE Law regarding the spread of fake news that is detrimental to consumers, as well as Article 378 of the Criminal Code regarding fraud. However, challenges arise when transactions involve overseas third parties, making investigations difficult to conduct without cross-border cooperation. Another example is the Tokopedia data leak case in 2020, which involved around 91 million user accounts. This case shows the relevance of the Personal Data Protection Law (PDP Law), as well as showing the gap in law enforcement because until now there has been no clarity regarding criminal liability from the parties involved in the data leak. This reinforces the argument that national regulation, while important, still has limitations when dealing with cybercrime that is transnational in nature.[18]

At the international level, the effectiveness of the Budapest Convention on Cybercrime can be demonstrated through the handling of cross-border phishing cases by European authorities. One example is a joint operation in 2019 involving Spanish and Romanian police with the support of Europol. The operation successfully dismantled a criminal network that defrauded hundreds of victims in Europe through fake emails that resembled official banks, as well as stealing credit card data to conduct illegal transactions. The success of this operation cannot be separated from the legal framework of the Budapest Convention which allows member states to provide mutual legal assistance quickly, including in the exchange of electronic evidence across jurisdictions. This is in contrast to non-member countries, such as Indonesia, which often

[16] Buana, S. E. W. (2022). Legal Protection of Personal Data to Personal Data Owners in the Implementation of Fintech Peer to Peer Lending Services.

[17] Wibowo, A., & Yulianingsih, S. (2025). Information Technology Law. *Publisher of Prima Agus Teknik Foundation*.

[18] Wahyudin, J., Renggong, R., & Hamid, A. H. (2024). Analysis of Online Fraud Crimes in the South Sulawesi Regional Police Area. *Indonesian Journal of Legality of Law*, *6*(2), 273-282.

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

have difficulty enforcing the law when the perpetrators and servers are abroad. Thus, this national and international case study shows that existing regulations can be used, but jurisdictional limitations and lack of legal harmonization are still major obstacles in tackling online fraud and identity theft.[19]

3. The Challenges of Law Enforcement in a Transnational Perspective

The main obstacle in handling cybercrime is the issue of jurisdiction. It is often difficult to determine which country has the primary authority to prosecute perpetrators. For example, the perpetrator is in the Philippines, the server is in the United States, the victim is in Indonesia, while the proceeds of the crime are transferred to an account in Singapore. This situation gives rise to complex jurisdictional conflicts.[20] In addition, the limited capacity of law enforcement officials is also a serious obstacle. Law enforcement requires digital forensic experts, tracking devices, network analysis capabilities, and cryptocurrency transaction tracking technology. Developing countries often face limited budgets and human resources that master this technology, so investigations are slow and prone to losing volatile digital evidence.[21]

Differences in regulations between countries are also an inhibiting factor. Some countries have not criminalized identity theft specifically, or do not have personal data protection regulations. This creates a "safe haven" for perpetrators who can easily change countries to avoid legal proceedings. Another obstacle is low public awareness. Many victims are reluctant to report cases because they feel embarrassed, fear of being blamed, or consider the amount of losses to be relatively small. In fact, the accumulation of these small cases is what actually makes online fraud even more prevalent.

Another aspect that is also important is the limitation of extradition mechanisms and mutual legal assistance. Not all countries have bilateral agreements with Indonesia, so the process of requesting legal aid is often hampered by bureaucratic procedures or even rejected for political and rule of law reasons. This condition has led to many cross-border cybercrime cases that end without a complete legal settlement.

4. Countermeasures and International Cooperation

Facing this complexity, a multidimensional strategy is needed. At the national level, the government needs to strengthen the implementation of the ITE Law and the PDP Law with clear technical rules, expand the competence of law enforcement officials in the field of digital forensics, and improve coordination between agencies, both the police, the prosecutor's office, Communication and Informatics, as well as banking and financial institutions. In addition, ratification of the Budapest Convention on Cybercrime will provide strategic advantages for Indonesia in establishing international cooperation. At the international level, cross-border cooperation should be strengthened through multilateral and bilateral agreements. The mechanism of mutual legal assistance must be optimized so that the exchange of digital evidence and intelligence information can be carried out more quickly and efficiently. The role of international and

[19] Ba'abud, M. F. R. (2023). *Application of the Principle of Extraterritorial Jurisdiction to Perpetrators of Personal Data Theft Committed Across Borders* (Doctoral Dissertation, Islamic University of Indonesia).

[20] Ginting, P. (2008). *Policy on Countering Information Technology Crimes Through Criminal Law* (Doctoral dissertation, Diponegoro University Undergraduate Program).

[21] Apriliansah, L., & Yusuf, H. (2024). The effectiveness of law enforcement in economic crimes: A study on money laundering cases in Indonesia. *Journal of Intellectual and Scholars of the Archipelago*, *1*(6), 9922-9937.

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

regional organizations is also important, for example ASEAN has launched the ASEAN Cybersecurity Cooperation Strategy to strengthen regional cybersecurity.[22]

In addition to law enforcement, preventive efforts are no less important. People's digital literacy needs to be improved through public campaigns, educational curricula, and collaboration with the private sector. Strengthening public awareness of the dangers of phishing, online fraud, and the importance of maintaining the confidentiality of personal data can be the first bulwark of defense before law enforcement officials intervene. These repressive, preventive, and collaborative efforts are in line with modern criminal law principles that emphasize not only punishment, but also community protection and prevention of criminal acts. Therefore, the ideal strategy in dealing with online fraud and identity theft must include aspects of regulation, law enforcement, international cooperation, and community participation.[23]

International case studies show how serious the impact of identity theft is. One of them was the Equifax Data Breach case in the United States in 2017, where about 147 million Americans' personal data, including social security numbers and financial data, was successfully stolen by hackers. This case is one of the largest data breaches in the world and has caused massive financial and reputational losses, while demonstrating the urgency of protecting personal data on a global scale. At the regional level, love scam cases involving Nigerian criminal networks in Malaysia and Singapore show an online fraud mode that exploits the emotional relationships of victims. According to an Interpol report (2020), the losses from this case reached millions of US dollars and involved thousands of victims in various countries. This case illustrates how online fraud is carried out in an organized manner by taking advantage of jurisdictional gaps between countries in the Southeast Asian region.[24]

Indonesia has also experienced major cases related to data theft, such as the Tokopedia data leak in 2020 involving around 91 million user accounts sold on the dark web. In addition, in 2023 there will be a leak of 1.3 billion SIM card data which shows the weakness of the national data security system. These cases show how weak personal data protection in Indonesia can have implications for the increased risk of identity theft and online fraud[25]. By studying these cases, it is clear that cybercrime not only inflicts individual harm, but also threatens national security and the integrity of the international legal system. Therefore, the urgency of strengthening transnational criminal law through harmonization of regulations, increasing the capacity of law enforcement officials, and international cooperation is becoming increasingly real.

CONCLUSIONS

Cybercrime in the form of online fraud and identity theft is a serious challenge in the digital era that has cross-border characteristics, the complexity of modus operandi, and the difficulty of proving due to the

[22] Rafid, R., & Nurita, R. F. (2025). The Dynamics of Education and Law in the Digital Era: Challenges and Opportunities in Facing Technological Transformation. *MLJ Merdeka Law Journal*, *6*(1).

[23] Anshori, A. Y., & Hidayat, M. E. N. (2024). Building Defense Against Hoaxes: Strengthening Information Literacy in the Digital Era. *Literacy*, *2*(01).

[24] Pangalila, F. C. Y. Y., De Fretes, C. H. J., & Seba, R. O. C. (2023). Peran National Central Bureau (NCB)-Interpol Indonesia dalam Penanganan Cybercrime (Romance Scam) 2018-2021. *Intermestic: Journal of International Studies*, *8*(1), 356-381.

[25] Nugraha, S., Andayani, D., & Tumanggor, M. S. (2023). Legal Liability of E-Commerce Business Actors for the Theft of Consumer Data Through the Tokopedia Application Based on Article 19 and Article 62 of Law Number 8 of 1999 concerning Consumer Protection. *UNES Law Review*, *6*(2), 4896-4909.

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

anonymity of the perpetrator and the vulnerability of digital evidence. National regulations, such as the ITE Law, the Criminal Code, and the Personal Data Protection Law, have provided a legal basis for cracking down on such crimes, but their implementation still faces limitations, especially in terms of jurisdiction and capacity of law enforcement officials. At the international level, legal instruments such as the Budapest Convention on Cybercrime and UNTOC have provided a legal framework for global cooperation, but their effectiveness is still limited due to the lack of universal ratification. This condition shows the need for legal harmonization between countries, increased cooperation in extradition mechanisms and mutual legal assistance, and the use of regional forums such as ASEAN to strengthen collective strategies to deal with cybercrime. In addition to the repressive aspect, prevention through people's digital literacy and personal data protection are important keys in reducing the risk of online fraud and identity theft. Thus, the countermeasures strategy must be comprehensive, including strengthening national regulations, increasing law enforcement capacity, international cooperation, and active community participation. Only through such an integrated approach can cybercrime be effectively dealt with within the framework of transnational criminal law. Therefore, beyond normative harmonization, this study recommends that Indonesia ratify the Budapest Convention, ASEAN establish a regional cybercrime task force, and states invest in digital forensic capacity. Simultaneously, public awareness campaigns on digital literacy must be strengthened, ensuring that transnational criminal law responses are complemented by preventive societal measures.

ACKNOWLEDGMENTS

The author would like to express sincere gratitude to Universitas Pasundan for providing academic support and access to research resources during the preparation of this article. The author also wishes to thank colleagues and the anonymous reviewers for their valuable comments and suggestions, which significantly enhanced the final version of this manuscript.

REFERENCES

Book

Budiyanto, S. H. (2025). Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia. Sada Kurnia Pustaka.

Sinaga, W. S. (2023). Upaya Penanggulangan Kejahatan Transnasional Terorganisir Dalam Kasus Penyelundupan Manusia. Ancaman Kejahatan Transnasional, 225.

Hutabarat, S. A., Praja, S. J., Suhariyanto, D., Paminto, S. R., Kusumastuti, D., Fajrina, R. M., ... & Abas, M. (2023). CYBER-LAW: Quo Vadis Regulasi UU ITE dalam Revolusi Industri 4.0 Menuju Era Society 5.0. PT. Sonpedia Publishing Indonesia.

Wibowo, A., & Yulianingsih, S. (2025). Hukum Teknologi Informasi. *Penerbit Yayasan Prima Agus Teknik*.

Journal Article

Amory, J. D. S., & Mudo, M. (2025). Transformasi ekonomi digital dan evolusi pola konsumsi: Tinjauan literatur tentang perubahan perilaku belanja di era internet. Jurnal Minfo Polgan, 14(1), 28-37.

Butarbutar, R. (2023). Kejahatan siber terhadap individu: Jenis, analisis, dan perkembangannya. Technology and Economics Law Journal, 2(2), 3.

Tekayadi, S., Sumerah, S., & Efendi, S. (2025). Tantangan Penegakan Hukum Siber Di Era Lintas Negara Dan Upaya Harmonisasi Global. Jurnal Risalah Kenotariatan, 6(1), 265-276.

Febrian, W. R., Faturrahman, R. M. R., Rahmadina, H. S., & Deni, F. (2024). Peran Hukum Internasional Dalam Menangani Kasus Cyber Crime. JURNAL SAHID DA'WATII, 3(02), 1-7.

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

Simanungkalit, J. A. R., Hertadi, R., & ul Hosnah, A. (2024). Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya. *AKADEMIK: Jurnal Mahasiswa Humanis*, *4*(2), 281-294.

Kadir, Z. K. (2025). Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse. *Jurnal Litigasi Amsir*, *12*(2), 124-137.

Butarbutar, J. M. (2025). Revolusi Digital dan Tantangan Kriminologis: Analisis terhadap Tren Kriminalitas dalam Era Digitalisasi. *Media Hukum Indonesia (MHI)*, *3*(2).

Wahyudin, J., Renggong, R., & Hamid, A. H. (2024). Analisis Tindak Pidana Penipuan Secara Online di Wilayah Kepolisian Daerah Sulawesi Selatan. *Indonesian Journal of Legality of Law*, *6*(2), 273-282.

Thesis or Dissertation

Anshori, A. Y., & Hidayat, M. E. N. (2024). Membangun Pertahanan Terhadap Hoaks: Penguatan Literasi Informasi di Era Digital. *Literasiana*, *2*(01).

Apriliansah, L., & Yusuf, H. (2024). Efektivitas penegakan hukum dalam tindak pidana ekonomi: Studi pada kasus pencucian uang di Indonesia. *Jurnal Intelek Dan Cendikiawan Nusantara*, *1*(6), 9922-9937.

Ba'abud, M. F. R. (2023). Penerapan Prinsip Yurisdiksi Ekstrateritorial Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi Yang Dilakukan Secara Lintas Batas Negara (Doctoral dissertation, Universitas Islam Indonesia).

Ba'abud, M. F. R. (2023). *Penerapan Prinsip Yurisdiksi Ekstrateritorial Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi Yang Dilakukan Secara Lintas Batas Negara* (Doctoral dissertation, Universitas Islam Indonesia).

BAKARA, P. L. (2024). Perlindungan Hukum Terhadap Korban Pencurian Identitas Digital Dalam Kejahatan Cybercrime.

Buana, S. E. W. (2022). Perlindungan Hukum Terhadap Data Pribadi Kepada Pemilik Data Pribadi Dalam Penyelenggaraan Jasa Fintech Peer To Peer Lending.

Chandra, E. (2024). Efektivitas Pelaksanaan Penyidikan Tindak Pidana Penipuan Modus Love Scamming Di Kepolisian Resort Barelang Kota Batam (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

DHARMAYANTI, Y. P. (2025). Kebijakan Hukum Pidana Dalam Upaya Menanggulangi Artifical Intelligance (AI) Dalam Cyber Crime (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

Ginting, P. (2008). *Kebijakan Penanggulangan Tindak Pidana Teknologi Informasi Melalui Hukum Pidana* (Doctoral dissertation, Program Sarjana Universitas Diponegoro).

IQBAL, M. (2025). *Peran Satuan Intelijen Kepolisian Dalam Penyelidikan Tindak Pidana Pembunuhan (Studi Kasus Di Kepolisian Resor Natuna)* (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

Nugraha, S., Andayani, D., & Tumanggor, M. S. (2023). Pertanggungjawaban Hukum Pelaku Usaha E-Commerce Atas Terjadinya Pencurian Data Konsumen Melalui Aplikasi Tokopedia Berdasarkan Pasal 19 dan Pasal 62 Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. *UNES Law Review*, *6*(2), 4896-4909.

Pangalila, F. C. Y. Y., De Fretes, C. H. J., & Seba, R. O. C. (2023). Peran National Central Bureau (NCB)-Interpol Indonesia dalam Penanganan Cybercrime (Romance Scam) 2018-2021. *Intermestic: Journal of International Studies*, *8*(1), 356-381.

Rafid, R., & Nurita, R. F. (2025). Dinamika Pendidikan Dan Hukum Di Era Digital: Tantangan Dan Peluang Dalam Menghadapi Transformasi Teknologi. MLJ Merdeka Law Journal, 6(1).

IPSO JURE JOURNAL

IPSO JURE

Journal

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

Vol.2. No.8, September 2025
DOI : https://doi.org/10.62872/zep90829

Legal Documents

Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Indonesia. (n.d.). Kitab Undang-Undang Hukum Pidana (KUHP).