West Science Law and Human Rights
Vol. 2, No. 03, July 2024, pp. 175~183

Protecting Digital Society: Policies for Criminalizing Illegal Smartphone Applications Through Cyber Law Frameworks

Kity Tokan[1], Muhammad Erham Amin[2], Ahmad Syaufi[3], Mispansyah[4]
[1,2,3,4]Universitas Lambung Mangkurat

Article Info

Article history:

Received July, 2024
Revised July, 2024
Accepted July, 2024

Keywords:

smartphone applications
cyber law
criminal law policies
digital society
unauthorized applications

ABSTRACT

This research aims to contribute to the development of criminal law policies addressing the widespread distribution of smartphone applications, both APK and iOS, that are used as tools for unauthorized online loan activities, online fraud, threats, and intimidation. These applications often disguise themselves as legitimate online loan platforms, wedding invitation apps, and parcel delivery services. Upon download, they illicitly debit mobile banking accounts or present themselves as government auction platforms for criminal goods at discounted prices, posing significant threats to consumers, debtors, and the general public. Theoretical framework: The foundation of this research lies in cyber law theory, which endeavors to create legal strategies to address cybercrimes and safeguard the digital community. This study utilizes a multidisciplinary approach, integrating legal analysis, policy assessment, and collaboration with stakeholders. Methods: This study utilized the normative juridical method to examine digital policies by criminalizing illegal smartphone applications through cyber law policies. This approach involves a systematic legal analysis of current regulations, assessing their effectiveness, and suggesting formal legal measures to address new threats posed by unauthorized applications, with an emphasis on protecting digital society from harm. Results and Conclusions: This indicates a pressing need for comprehensive criminal law policies specifically designed to effectively combat these unauthorized applications. Such policies are crucial in preventing and mitigating the harms caused by these applications before they impact society. The author's contribution lies in proposing formal offenses against the creators and disseminators of these applications. malicious applications, thereby bridging the current gap in legal measures to counteract digital criminal activities. Originality/Value: This research underscores the urgency of formulating and implementing cyber law policies to safeguard the public from the detrimental effects of illicit smartphone applications. Its originality lies in proposing innovative legal strategies to proactively address emerging digital threats.

Corresponding Author:

Name: Kity Tokan
Institution: Universitas Lambung Mangkurat
e-mail: kitytokan30@yahoo.com

1. INTRODUCTION

The swift progression of information technology in the current era of globalization, termed Industry 4.0, has brought significant changes, especially in the economic sector. The first major transformation, initiated in the 18th century with the introduction of steam engines, is known as Industry 1.0. Today, we are amidst the fourth industrial revolution, Industry 4.0, also called Society 4.0. This period is distinguished by the extensive use of electronic devices, like computers, to manage complex human tasks. Society 4.0 coincided with the Third Industrial Revolution, which began in 1969 with the advent of electronic devices and computers. Technology-based lending and borrowing services are regulated by the Financial Services Authority Regulation (POJK) No. 77/2016. This regulation covers information technology-based money lending and borrowing services, detailing rules on legal entities, capital requirements, maximum loan limits, agreement formats, and oversight of borrowers and lenders, whether individuals or businesses. The main objective is to create a framework for responsible business operations while ensuring the protection of consumers and business entities [1].

However, there has been a surge in online lending crimes that significantly impact society and present substantial challenges. Recently, police uncovered 15 cases of illegal online loans involving 45 suspects across various regions. From 2020 to 2021, the police received 371 public reports regarding illegal lending activities. Out of these, 91 cases have been investigated, while 280 cases remain under review. Setyo Budiantoro, a senior economic researcher from Perkumpulan Prakarsa, attributed the rise in illegal lending to a weak regulatory framework for fintech. Technology often evolves faster than regulations can keep up. Given the ongoing digital revolution, there is a pressing need for exceptional measures to protect individuals from becoming victims. [2]. The presence of illegal fintech platforms is deeply concerning due to their abnormal regulations, lack of transparency, exorbitant interest rates, susceptibility to data breaches, and their utilization for fraudulent and extortionate purposes, which can be even more dangerous than traditional loan sharks who physically coerce borrowers. It is evident that these illegal fintech entities are not registered with Indonesia's Financial Services Authority as they lack standardized billing procedures and maintain unclear company profiles. This has given rise to new issues where loan interest rates surpass those offered by banks. Many loan users fail to recognize this and neglect to compare these rates with those offered by traditional banks. Collections are often conducted in a harsh manner, employing tactics such as threats, blackmail, deceit, intimidation, defamation, and slander when payments are delayed, and interest rates are excessively high. These adverse experiences are not only endured by the borrowers but also affect others whose contact numbers are registered when the borrower initially signed up. Consequently, loan collection activities can disrupt the lives of these individuals.

The distribution of unauthorized loan applications that lack approval from the Ministry of Communication and Information poses significant regulatory challenges. These applications circumvent official Android and iOS app stores, such as the Google Play Store and Apple App Store, by being disseminated through SMS and social media platforms like WhatsApp, Telegram, and others. This issue involves both foreign and domestic entities distributing these unauthorized loan apps without government permission, bypassing the official app stores. As of May 3, 2020, 161 fintech companies were registered and licensed by the OJK (Financial Services Authority). However, SWI (Investment Alert Task Force) data reported 3,734 cases of illegal lending, which decreased to 151 by May 2021. Many suspects operate from abroad, particularly from countries like China, making it difficult to apprehend foreign perpetrators. Peer-to-peer (P2P) lending platforms are often suspected of facilitating illegal online loans, engaging in intimidation and extortion, and distributing customers' personal data in violation of the law [3].

Regarding the online loan cases mentioned, law enforcement authorities mainly concentrate on prosecuting material offenses, taking legal action only after a victim has been harmed. However, there is a notable lack of preventive measures, creating new challenges [4]. Moreover, a recent trend has seen the emergence of illegal Android applications shared through various social media and communication platforms. These apps are specifically designed to compromise mobile phones and illegally extract funds from digital transactions and online or mobile banking accounts [5].

This paper seeks to answer the main research question: "How can a criminal law policy be formulated to prosecute unauthorized online loan activities?" It investigates the creation of legal mechanisms and policies to combat the rise of unapproved online lending. The paper contributes significantly by proposing a comprehensive criminal law policy framework to address unauthorized online loans. It assesses the existing legal environment and recommends strategies to effectively prosecute those involved in such practices. By providing insights and suggestions, this research aids in developing legal instruments to protect consumers, prevent fraud, and strengthen the regulatory framework for online lending.

2. LITERATURE REVIEW

Cyber law theory recognizes the evolving landscape of technology and its impact on legal systems [6]. It acknowledges the need to adapt and evolve legal frameworks to address new digital challenges. Central to this concept is cybersecurity, which focuses on protecting digital assets, data, and the overall integrity of digital environments. This study specifically examines the area of cyber law related to the distribution and misuse of smartphone applications within this framework [7]. Cyber law theory is a multidisciplinary field that encompasses legal, technological, and policy aspects to establish legal mechanisms for combating cybercrimes and safeguarding digital society [8]. Cyber law theory is grounded in traditional legal principles adapted to the digital realm. Scholars explore how existing legal frameworks apply to cybercrimes, intellectual property issues, privacy concerns, and digital contracts [9]. This includes the examination of fundamental legal concepts such as jurisdiction, liability, and due process in the context of cyberspace. Furthermore, a significant focus of cyber law theory is on the identification and classification of cybercrimes [10]. Researchers examine the legal definitions of hacking, identity theft, online fraud, and other types of digital misconduct. Furthermore, the field investigates cybersecurity measures, legal responsibilities for data protection, and the legal consequences of data breaches. [11].

One key aspect explored is the typology of cybercrimes, which encompasses a wide range of activities such as hacking, identity theft, online fraud, cyberbullying, phishing, and ransomware [12]. Marwan & Prayogo [13] delve into the motivations and methods behind each type, providing insights into the ever-evolving tactics employed by cybercriminals. Another critical area of study is victimology, which examines the demographics of cybercrime victims and their experiences. This includes an analysis of the emotional and financial toll on individuals, organizations, and even nations [14]. Victim-blaming and the psychological effects of cybercrimes are also discussed, shedding light on the human impact of these offenses. Criminal profiling is an essential endeavor in understanding and identifying cybercriminals Kipane [15] and Perkins & Howell [16] analyze offender characteristics, modus operandi, and behavioral patterns. This profiling aids law enforcement agencies in developing strategies for the apprehension of cybercriminals. Additionally, the literature reviews legal frameworks, cybersecurity measures, law enforcement challenges, the dark web, cybersecurity policies, digital forensics, cybersecurity awareness, emerging threats, ethical considerations, and international cooperation—all contributing to a holistic understanding of the complex world

of cybercrime and the efforts to combat it effectively [17]. Previous studies have classified cybercrimes into various typologies, including hacking, identity theft, online fraud, cyberbullying, phishing, ransomware, and more [18], [19]. Each type is thoroughly examined, shedding light on the characteristics, motivations, and methods associated with these cybercrimes. This comprehensive categorization helps in understanding the evolving tactics employed by cybercriminals [20]. Victimology is another crucial area of study within this domain. Oksanen & Keipi [21], Abubakari & Blaszczyk [22] explore the demographics of cybercrime victims and delve into their experiences. This includes an analysis of the emotional and financial impacts on individuals, organizations, and even entire nations. Notté et al. [23], and Cross [24] discussed victim-blaming and the psychological effects endured by those targeted by cybercrimes. Criminal profiling is a complex but essential endeavor in the fight against cybercrime. Hernandez-Castro & Boiten [25] analyze offender characteristics, modus operandi, and behavioral patterns to gain a deeper understanding of cybercriminals. This profiling aids law enforcement agencies in developing effective strategies for identifying and apprehending cybercriminals [26]. Additionally, Basheer & Alkhatib [27], Maglaras et al. [28], Kavallieros et al. [29] discuss on legal frameworks, cybersecurity measures, law enforcement challenges, the dark web, cybersecurity policies, digital forensics, cybersecurity awareness, emerging threats, ethical considerations, and international cooperation.

3. METHODS

This study aims to investigate and contribute to the development of criminal law policies targeting the widespread distribution of illicit smartphone applications, particularly those involved in unauthorized online loan activities, online fraud, threats, and intimidation. It uses a normative juridical research design, involving a systematic legal analysis of existing regulations concerning digital crimes and the dissemination of harmful applications. This methodological approach is consistent with the theoretical framework of cyber law theory. It systematically examines current regulations, including those addressing cybercrimes and digital policies, to assess their effectiveness in mitigating the threats posed by unauthorized applications.

Additionally, it proposes formal legal measures to protect digital society from harm. The normative juridical method is in line with the principles of cyber law theory, which highlight the importance of legal safeguards against digital threats. This approach includes assessing the effectiveness of current regulations and proposing new legal measures to tackle emerging threats. Using a qualitative descriptive methodology, the study combines legal analysis with policy evaluation and stakeholder collaboration. It acknowledges the complex nature of digital crimes and aims to develop comprehensive solutions. Data is gathered through an extensive review of existing cyber law regulations, case studies, and relevant legal literature. The analysis thoroughly examines the legal framework, identifying gaps and deficiencies in current regulations. Policy evaluation is conducted to assess the effectiveness of existing measures, and the study proposes new legal strategies to address the challenges posed by unauthorized applications and safeguard digital society from harm.

4. RESULTS AND DISCUSSION

Unauthorized online loan applications are disseminated through social media platforms such as WhatsApp and Telegram as Android APK files. Users are lured by advertisements and readily download these unapproved loan APKs. These applications then operate without complying with statutory interest rate limits, often charging exorbitant and unjustifiable interest rates. They function outside the legal framework and without the required

licensing from the Ministry of Communication and Information or other relevant authorities [30].

The adverse consequences of these online loan applications are notably high interest rates, exploiting the financial vulnerability of customers, which can lead to a cycle of increasing debt.

When customers fail to make payments, these applications gain access to their personal data, which can be exploited for coercive collection practices such as threats, intimidation, or unauthorized sharing of personal information, including sensitive content. Consequently, customers often face distress while trying to repay these illegal online loans. Moreover, these unauthorized loans lack adequate dispute resolution mechanisms, leading to considerable financial losses for consumers [31]. Beyond the issue of online loan applications, there is a parallel phenomenon involving the distribution of applications created for criminal purposes, which is discussed in Table 1.

Table 1. Modus and Mechanism of Illegal Applications in social media

No	Modus	Mechanism
1.	Chat Mode	This type of fraud, involving APK messages, also became widespread in Bali in February 2023. This new hacking method uses wedding invitations, with fraudsters sending invitation letters that contain APKs from sources outside the Play Store. Once installed, these APKs steal OTP credentials from the victim's device.
2.	Fraudulent mode under the guise of sending packages by express expedition	On social media, a viral scam has surfaced on WhatsApp, where fraudulent messages mimic package notifications from a courier service. The scammer impersonates an express courier, claiming to need to verify the recipient's identity. They send an attachment labeled 'VIEW Package Photo' in .apk image format. This deceptive tactic involves posing as a courier service provider and sending an attachment with an APK extension. Unaware users, focusing only on the file title, might be tempted to click and download the file, falling for the scam.
3.	Fraud under the guise of Trading Robots	Recently, there has been significant discussion about fraudulent activities involving trading robots, resulting in numerous victims. The common tactic in recent years involves using Ponzi schemes or money game-like structures to trap victims. Initially, many consumers are unaware of the fraud because they earn profits by recruiting new members into the system. However, this scheme is like a ticking time bomb, gradually revealing its fraudulent nature. Typically, traders are unaware of the deceit at first, as this method consistently produces profits in the early stages, thereby maintaining participants' trust. However, as victims begin to invest and trust the system, the fraud is executed by intentionally causing malfunctions in the autopilot trading robot, making it inaccessible to the victims.
4.	Creating a fake website	Resembling legitimate websites in structure and character, these deceptive sites employ a technique known as Punycode in information technology. This method substitutes letters or characters in the official website address with similar-looking Unicode counterparts. Unaware of the manipulation, victims perceive the altered addresses as correct, falling into a deceptive trap. As a result, their devices become susceptible to malware infections that transmit personal data to cybercriminals. This stolen information enables criminals or hackers to access the victim's financial resources. Therefore, it is essential to understand this deceptive technique to reduce the risk of becoming a victim of such malicious activities.

According to Table 1, instances of online fraud perpetrated through APK files have become increasingly prevalent. Typically, victims of such fraud experience financial losses, including the depletion of funds in their bank application accounts and balances in digital wallets or online platforms. Various modes of online fraud involving APK files are executed by sending deceptive wedding invitations or fraudulent package delivery schemes to unsuspecting victims. These methods are designed to pilfer personal information and data from the victims. In light of this scenario, the author's analysis focuses on multimedia-related crimes, which center not on the perpetrator but on the tools employed, specifically the APK mode or the websites utilized for criminal activities. Consequently, there is a need for formal legal provisions when an action is deemed to have the potential to cause harm, enabling the prosecution of those who create and distribute such applications before the actual material offense is proven. Collaborative efforts among relevant stakeholders are essential for proactive identification, technological analysis, and the subsequent criminalization of these applications [32].

Musyafah [33] highlights the challenge of prosecuting individuals who create and distribute unauthorized online loan applications. The growth of financial technology (Fintech) crime has been rapid, primarily due to the absence of preventative measures in the form of formal criminal offenses and a lack of legal provisions for formal criminal sanctions. It's noteworthy that the regulations governing Fintech lending, established by the OJK (Financial Services Authority), remain administrative in nature and do not encompass formal criminal penalties. Law enforcement authorities, when dealing with the organizers of criminal activities associated with illegal online lending, rely on regulations that pertain to substantive criminal penalties. These regulations encompass various legal provisions, including those found in: - Law No. 8 of 1999 on consumer protection, particularly Article 62 paragraph (1) in conjunction with Article 8 paragraph (1) letter f; Law No. 19 of 2016 amending Law No. 11 of 2008 on information and electronic transactions, including Article 45 paragraph (1) in conjunction with Article 27 paragraphs (1, 3, 4) and Article 28 paragraph (1, 2) in conjunction with Article 45 paragraph (2); Law No. 7 of 2014 on trade, especially Article 65 paragraph (2) in conjunction with Article 115; Law No. 44 of 2008 on pornography, particularly Article 6 in conjunction with Article 32; Law No. 8 of 2010 on the prevention and eradication of money laundering crimes, encompassing Articles 3, 4, and 5; Law No. 36 of 1999 on telecommunications, especially Article 42 paragraph (1) in conjunction with Article 57; Law No. 10 of 1998 amending Law No. 7 of 1992 on banking, particularly Article 40 paragraph (1) in conjunction with Article 47 paragraph (1, 2); Law No. 27 of 2022 on the protection of personal data, covering Article 67 and Article 68; Law No. 42 of 1999 on fiduciary guarantees, including Article 35 and Article 36; Provisions related to threats, insults, defamation, slander, and blackmail as specified in Articles 345, 346, 437, 348, and Article 434 of Law No. 1 of 2023 concerning the Criminal Code. These regulations collectively provide the legal framework for pursuing criminal charges against those involved in illegal online lending activities.

However, perpetrators (organizers) of these criminal acts persist in their activities. In light of this, the recommendation is that the government should establish legislation concerning Financial Technology, explicitly outlining formal criminal sanctions and officially designating criminal acts related to illegal online loans as prosecutable offenses, without requiring reports from the victimized community. Furthermore, law enforcement agencies and relevant authorities should collaborate consistently to take resolute and concrete actions in addressing the surge in criminal activities within the realm of unauthorized online loans. They should also provide public guidance regarding the associated risks of engaging with non-legitimate Fintech providers, thereby reducing the likelihood of individuals falling victim to such schemes [34]. In this context,

the introduction of regulations for criminal penalties pertaining to formal criminal offenses needs to be incorporated into the Information and Electronic Transactions (ITE) Law and the Personal Data Protection Law. Thus far, these laws have lacked provisions for criminal penalties regarding formal offenses [35]. Prior to discussing the formulation of penalties for illegal Fintech Peer-to-Peer lending smartphone applications, including Misuse of Device, it is imperative to identify similar cases as benchmarks. Presently, instances of crimes involving APK smartphone applications have become a pervasive trend, inflicting considerable harm on society.

One of the noteworthy applications in this context is the Virtual Caller application developed by Niu Xin Network Technology Co., Ltd. This online service provides companies with an integrated telephone terminal featuring specialized functions such as group calls, caller ID spoofing (utilizing random telephone numbers), and SMS/MMS messaging. Typically, this type of service application finds extensive use among Call Center service providers. The actors responsible for spreading online loan applications employ various methods, including advertising, SMS blasts (broadcasting), and the WhatsApp Business application, which operates similarly to other instant messaging services. They share these applications by posting them, with or without online loan application file attachments, from one account to another, either privately or to multiple accounts (broadcast), and also within chat groups [36]. When examining the penalties associated with material offenses related to unauthorized online loans and the distribution of applications without permission, it becomes apparent that neither Law (UU) Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 regarding Information and Electronic Transactions nor Law (UU) Number 27 of 2022 concerning Data Protection contain provisions for formal offenses in criminal cases, particularly material offenses. As a result, law enforcement agencies can only take action after victims have suffered losses and submitted reports, rather than proactively addressing potential harm before it occurs. This approach entails penalizing individuals not for causing harm but for engaging in formal offenses associated with illegal loan applications and their distribution. Contrary to Law Number 44 of 2008 concerning Pornography, where criminal sanctions in Chapter VII pertain to provisions of criminal acts outlined in Article 29, Article 31, Article 32, Article 33, and Article 36, which are categorized as formal offenses, Article 30, Article 34, Article 35, Article 37, and Article 38 in the same law are classified as material offenses. This distinction in Law No. 44 of 2008 concerning Pornography ensures comprehensive legal protection. However, it's important to note that punishment within the context of law should be equitable and just to prevent overcriminalization, especially when formulating criminal articles for individuals involved in the creation and distribution of online loan applications without permission, particularly when no actual harm has occurred yet.

5. CONCLUSION

The purpose of this analysis is to highlight the absence of specific Indonesian laws that include formal criminal penalties as proactive and preventive measures against online loan crimes. It aims to underscore the limitations of the current legal framework, which predominantly focuses on remedies after losses have occurred, thereby necessitating reactive rather than proactive actions by law enforcement agencies. This analysis seeks to emphasize the need for legal provisions that protect the public from the creators and distributors of illegal online loan applications and APKs, which exploit the mobile banking accounts of unsuspecting victims.

This substantial gap in the legal framework has important practical and theoretical implications. Practically, it leaves individuals susceptible to online loan scams and APK-related fraud, as there is no

preventive legal protection for potential victims. Law enforcement agencies are often unable to act until after the damage has been done. Theoretically, this gap highlights the necessity for legal reforms that consider the changing digital landscape and the proactive protection of individuals against new cyber threats. Implementing formal criminal sanctions within the law would serve as a critical preventive measure, deterring potential offenders and improving the legal framework's ability to address the challenges posed by illegal online loans and APKs intended for illicit activities. In summary, this analysis emphasizes the urgent need to fill this legal void to protect the public in an increasingly digital and interconnected world.

In light of the prevailing challenges associated with illegal online loan applications and the distribution of unauthorized APKs, it is imperative that Indonesia takes proactive steps to address this issue through legal reforms. To that end, Indonesia should consider amending the Information and Electronic Transactions (ITE) Law to include provisions for the criminalization of formal offenses related to the creation and distribution of illegal applications (APKs). This amendment should encompass not only the illegal online loan applications but also any applications intended for criminal activities. By explicitly recognizing these offenses, the law would serve as a deterrent, dissuading potential wrongdoers. The legal framework should be established in a way that clearly defines the scope of illegal online loan applications and APKs created and distributed for malicious purposes. Clarity in the law will aid law enforcement agencies in effectively identifying, investigating, and prosecuting offenders. Moreover, incorporating formal criminal sanctions will promote preventive efforts by ensuring that legal consequences are in place before any harm is inflicted on victims. This proactive approach can deter individuals from engaging in such activities, reducing the likelihood of victimization. To complement legal reforms, collaboration between relevant stakeholders, including government bodies, law enforcement agencies, and the private sector, is crucial. Additionally, public awareness campaigns and educational initiatives should be implemented to inform individuals about the risks associated with illegal online loans and malicious APKs. By adopting these measures, Indonesia can strengthen its legal framework, enhance cybersecurity, and better protect its citizens from the threats posed by unauthorized applications and online loan scams. These proactive steps will contribute to a safer digital environment and a more resilient society in the face of evolving cyber threats.

REFERENCES

[1] Suryowati, E. (2019). Ini Poin Penting Aturan"Peer-to-Peer Lending. Available: https://money.kompas.com/read/2017/01/03/120000326/ini.poin.penting.aturan.peer-topeer.lending.untuk.fintech

[2] Pakpahan, E. F., Chandra, K., & Tanjaya, A. (2020). Urgensi Pengaturan Financial Technology di Indonesia. *Jurnal Darma Agung*, *28*(3), 444-456.

[3] Nasution, A. (2017). Sekilas hukum perlindungan konsumen. *Jurnal Hukum & Pembangunan*, *16*(6), 568-581.

[4] Novita, W. S., & Imanullah, M. N. (2020). Aspek Hukum Peer to Peer Lending (Identifikasi Permasalahan Hukum dan Mekanisme Penyelesaian). *Jurnal Privat Law*, *8*(1), 151-157.

[5] Setyanawati, D. P. W. Y. (2015). Tinjauan Viktimologi Dan Perlindungan Hukum Korban Kekerasan Dalam Pacaran. *Serambi Hukum*, *8*(02), 23094.

[6] Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & security*, *30*(8), 719-731.

[7] Kolomoets , E., Shoniya, G., Mekhmonov, S., Abdulnabi, S., Karim, N. A., & Mohammad , T. A. (2023). The Employee's Right to Work Offline: A Comparative Analysis of Legal Frameworks in Different Countries. *Revista De Gestão Social E Ambiental*, *17*(5), e03470.

[8] Mariyam, S., & Setiyowati, S. (2021). Legality of Artificial Intelligence (AI) Technology in Public Service Transformation: Possibilities and Challenges. *Lex Publica*, *8*(2), 75-88.

[9] Yanto, O. (2020). Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development. *Lex Publica*, *7*(2), 24-43.

[10] Suwadi, P., Manthovani, R., & Assyifa, A. K. (2023). Legal Comparison of Electronic Contract in Electronic Commerce Between Indonesia and the United States Based on the United Nations Commission on International Trade Law. *Journal of Law and Sustainable Development, 11(*3), e714.
[11] Wardani, A., Ali, M., & Barkhuizen, J. (2022). Money Laundering through Cryptocurrency and Its Arrangements in Money Laundering Act. *Lex Publica*, *9*(2), 49-66.
[12] Astuti, S. A. (2016). Penerapan Uu ITE Dan Surat Edaran Kapolri Mengenai Ujaran Kebencian Hate Speech Terhadap Penyimpangan Penggunaan Kebebasan Berekspresi Dalam Kajian Pasal 28 UUD 1945 Tentang HAM Di Ruang Maya Cyber Space. *Lex Publica*, *2*(2).
[13] Marwan, M., & Prayogo, G. (2019). Justice and Legal Certainty in Regulating Cryptocurrency in Malaysia. *Lex Publica*, *6*(2), 1-7.
[14] Sukmareni, S. (2016). Hak Perlindungan Penduduk Sipil Atas Serangan Langsung dalam Konflik Bersenjata Menurut Hukum Humaniter Internasional (Cek Similarity). *Lex Publica*, *2*(2), 341-350.
[15] Kipane, A. (2019). Meaning of profiling of cybercriminals in the security context. In *SHS Web of Conferences* (Vol. 68, p. 01009). EDP Sciences.
[16] Perkins, R. C., & Howell, C. J. (2021). Honeypots for cybercrime research. *Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches*, 233-261.
[17] Syaufi, A., Zahra, A. F., & Gholi, F. M. I. (2023). Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes. *International Journal of Cyber Criminology*, *17*(1), 85-101.
[18] Howell, C. J., & Burruss, G. W. (2020). Datasets for analysis of cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 207-219.
[19] Alubaidi, A. (2023). Challenges to Implementing the International Digital Law to Protect Digital Rights. *Journal of Law and Sustainable Development, 11*(5), e554.
[20] Prayogo, G., & Chornous, Y. (2020). Conceptualization of Future Cryptocurrency Laws in Indonesia and Ukraine. *Lex Publica*, *7*(2), 56-68.
[21] Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable children and youth studies*, *8*(4), 298-309.
[22] Abubakari, Y., & Blaszczyk, M. (2023). Politicization of Economic Cybercrime: Perceptions Among Ghanaian Facebook Users. *Deviant Behavior*, 1-20.
[23] Notté, R., Leukfeldt, E. 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.
[24] Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, *21*(2), 187-204.
[25] Hernandez-Castro, J., & Boiten, E. (2014). Cybercrime prevalence and impact in the UK. *Computer Fraud & Security*, *2014*(2), 5-8.
[26] Zahynei-Zabolotenko, Z., Tkachenko, I., Suprun, V., Kvasha, O., Prysiazhniuk, I., & Moisieienko, L. (2023). Legal Aspects of Pedagogical Education in a Digital Society Under the Implementation of the Social Function of the State. *Journal of Law and Sustainable Development, 11*(6), e1253.
[27] Maglaras, L., Ferrag, M., Derhab, A., Mukherjee, M., Janicke, H., & Rallis, S. (2018). Threats, countermeasures and attribution of cyber attacks on critical infrastructures. *EAI Endorsed Transactions on Security and Safety*, *5*(16).
[28] Basheer, R., & Alkhatib, B. (2021). Threats from the dark: A review over dark web investigation research for cyber threat intelligence. *Journal of Computer Networks and Communications*, *2021*, 1-21.
[29] Kavallieros, D., Chalanouli, C., Kokkinis, G., Panathanasiou, A., Lissaris, E., Leventakis, G., ... & Germanos, G. (2018, June). Searching for crime on the web: Legal and ethical perspectives. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE.
[30] Sugangga, R., & Sentoso, E. H. (2020). Perlindungan Hukum Terhadap Pengguna Pinjaman Online (Pinjol) Ilegal. *Pakuan Justice Journal of Law (PAJOUL)*, *1*(1), 47-61.
[31] Wahyuni, R. A. E., & Turisno, B. E. (2019). Praktik Finansial Teknologi Ilegal Dalam Bentuk Pinjaman Online Ditinjau Dari Etika Bisnis. *Jurnal Pembangunan Hukum Indonesia*, *1*(3), 379-391.
[32] Hanifawati, S. D. (2021). Urgensi Penegakan Hukum Pidana pada Penerima Pinjaman Kegiatan Peer To Peer Lending Fintech Ilegal dan Perlindungan Data Pribadi. *Jurnal Penegakan Hukum Dan Keadilan*, *2*(2), 162-172.
[33] Musyafah, A. A. (2019). Peran Otoritas Jasa Keuangan (OJK) Dalam Hal Perlindungan Nasabah Pada Lembaga Keuangan Mikro Syariah. *Law, Development and Justice Review*, *2*(2), 194-211.
[34] Nurwahridya, M. M. (2020). Peranan Polri dalam Penanggulangan Tindak Pidana Siber oleh Desk Collector Pinjaman Online. *RECIDIVE*, *9*(1), 43-49.
[35] Hartini, S., Sudrajat, T., & Bintoro, R. (2012). Model Perlindungan Hukum terhadap Kebijakan Pelayanan Kesehatan Masyarakat Miskin di Kabupaten Banyumas. *Jurnal Dinamika Hukum*, *12*(3), 523-534.
[36] Lumbanraja, A. D. (2020). Perkembangan Regulasi dan Pelaksanaan Persidangan Online di Indonesia dan Amerika Serikat Selama Pandemi Covid-19. *Crepido*, *2*(1), 46-58.