The Spirit of Society Journal
International Journal of Society Development and Engagement
LPPM - Universitas Narotama
ISSN : 2594 - 4777 (Online)
2597 - 4742 (Print)
https://jurnal.narotama.ac.id/index.php/scj/index

Personal Data Breaches by Online Loans as a Form of Cyber Crime

Criminology and Victimology Studies Post Personal Data Protection Law

Tjahjana Budiman

Faculty of Law, Universitas Narotama

Corresponding author: tjahjanabudiman@gmail.com

Abstract: The rapid growth of online lending platforms in Indonesia has accelerated financial inclusion while simultaneously generating new forms of cyber-crime, particularly the unlawful collection, processing, and dissemination of personal data by illegal operators. This research analyses personal data violations committed by online lending services as cyber-crime from criminological and victimological perspectives following the enactment of Law Number 27 of 2022 concerning Personal Data Protection. Using a normative juridical method with statutory and conceptual approaches, this study integrates cyber-crime theory, digital white collar crime theory, opportunity theory, anomie theory, and critical victimology to explain structural relations between perpetrators and victims in the digital financial ecosystem. The study finds that personal data exploitation constitutes cyber enabled financial crime characterized by asymmetry of information, technological dominance, weak enforcement mechanisms, and profit-oriented motives. Victims suffer layered victimization including financial losses, psychological harm, reputational damage, and secondary victimization. Although the Personal Data Protection Law strengthens legal safeguards, implementation challenges remain significant due to cross border operations, institutional limitations, and low digital literacy. The research proposes comprehensive penal and non penal strategies to enhance enforcement and victim protection.

Keywords: personal data violation, online lending, cyber-crime, criminology, victimology, data protection law

INTRODUCTION

The development of financial technology has transformed the structure of economic interactions in Indonesian society. Data from the Financial Services Authority (OJK) shows a significant increase in the number of users of technology-based lending services in recent years. However, this expansion has been accompanied by a rise in illegal online lending, which violates privacy rights and personal data protection.

The practice of excessive access to phone contacts, photo galleries, and even the distribution of information to third parties violates the principles of the Personal Data Protection Law and the Electronic Information and Transactions Law. This phenomenon is not only an administrative violation but has evolved into a cybercrime based on data exploitation.

RESEARCH METHODS

This research uses a normative juridical method that emphasizes the analysis of legal norms, principles, and doctrines to explain personal data breaches by online lenders as a form of cybercrime. This method was chosen because the issues studied concern not only technical violations of data processing but also aspects of the structure of the crime, economic motives, digital power relations, and the impact of victimization on the victims.

The first approach is a legislative approach, examining Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 1 of 2024, and Law Number 8 of 1999 concerning Consumer Protection. The analysis is conducted systematically to determine whether online lending practices comply with basic data protection principles, such as valid consent, limitation of processing purposes, data minimization, data controller accountability, and criminal and administrative sanction mechanisms.

The second approach is a conceptual approach using cybercrime theory, digital economic crime theory, opportunity theory, anomie theory, and victimology theory. This framework is used to explain how personal data becomes an instrument of power in the collection process and how victims experience multiple victimizations.

The third approach is a comparative analysis of previous research. Research on Google Scholar in the past three years has generally been descriptive-normative and focused on consumer protection and the legality of online lending. Research in reputable national journals indexed by SINTA tends to emphasize the accountability of data controllers and the effectiveness of law enforcement. Meanwhile, international literature indexed by Scopus often positions data misuse in fintech as part of digital economic crime and highlights issues of cross-jurisdictional enforcement and victimization prevention strategies.

Primary legal materials consist of statutory regulations, secondary legal materials consist of scientific journals and academic books, and tertiary legal materials consist of legal dictionaries and encyclopaedias. The analysis was conducted qualitatively using grammatical, systematic, and teleological interpretation methods to obtain comprehensive conclusions.

RESULTS AND DISCUSSION

The Concept of Cybercrime in Contemporary Criminology Perspective

In modern criminology, cybercrime is understood as a crime that uses information technology as a means, target, or environment for the crime. Wall (2023) explains that cybercrime has evolved from system hacking to data exploitation for economic gain. Yar (2022) emphasizes that the transformation of the digital economy has made personal information a high-value commodity.

In the context of online lending, misuse of personal data is not only an administrative violation but also an instrument of extortion and social pressure on victims. Smith and Brooks (2024) classify this phenomenon as a cyber-enabled financial crime because technology is a primary tool in the process of obtaining illegal profits.

Research on Google Scholar generally focuses on legality and norm violations. Pratama and Nugroho (2023) demonstrated that data breaches in illegal fintech practices involve unauthorized access and distribution of personal information through electronic systems. However, these studies often fail to deeply link this phenomenon to theories of digital economic crime.

In the Scopus literature, Levi and Lord (2023) emphasize that digital economic crime thrives through organizational structures that exploit the complexity of technological systems and weak oversight. This approach provides a broader framework for understanding illegal online lending as part of digital-based organized economic crime.

Personal Data Protection Post-National Regulation

Law Number 27 of 2022 concerning Personal Data Protection strengthens the national legal framework for protecting data subjects' rights. Santoso and Hidayat (2023) explain that this regulation adopts the principles of lawful processing, consent, purpose limitation, and proportionality. These

principles emphasize that all data processing must have a valid legal basis and be carried out in a limited manner, consistent with the purpose.

Research on Google Scholar following the enactment of this law has highlighted that the regulation provides a legal framework for prosecuting illegal online lenders. However, much of the research has focused on identifying the articles and has not detailed the compliance of app practices with the principles of data minimization and data controller accountability.

Rahman and Siregar (2024) in a national journal showed that the implementation of the Personal Data Protection Law faces challenges in the form of limited oversight capacity and cross-agency coordination. Chen and Lee (2024) in a Scopus journal emphasized that developing countries often face enforcement challenges due to limited resources and the complexity of cross-jurisdictional crimes.

Thus, even though the legal framework is normatively strong, the effectiveness of data protection still depends heavily on consistent enforcement and increased institutional capacity.

Online Loans and Data Abuse Patterns

Data misuse in online lending occurs in several stages. Early on, applications often request access to data irrelevant to credit analysis, such as contact lists and photo galleries. Wibowo (2023) points out that this practice contradicts the principle of data minimization.

During the processing stage, consent is often formally granted but without substantial understanding by the user. This creates an information gap between providers and consumers. Martinez and Singh (2023) state that fintech abuse exploits this asymmetry of information to gain economic advantage.

During the collection stage, data is used as a tool of social pressure. Kurniawati and Lestari (2024) found that data distribution to third parties is often used to expedite payments. This practice demonstrates the perpetrator's strong digital dominance over the victim.

Google Scholar research generally describes the billing methods and their impact on victims. Meanwhile, research in reputable national journals has begun to emphasize the responsibility of data controllers. Scopus literature further categorizes this practice as a form of digital economic crime with an organized and transnational character.

A Victimology Perspective on Data Breaches

From a victimology perspective, online loan victims experience primary and secondary victimization. Primary victimization involves financial losses due to unreasonable interest rates and fines. Secondary victimization occurs when data is disseminated, leading to psychological distress and social stigma.

Cross and Button (2023) explain that cybercrime victims often experience secondary victimization due to a lack of institutional support. Putri and Anwar (2023) show that victims of illegal online loans experience anxiety and depression due to the threat of data disclosure.

Duggan (2022) developed the concept of structural victimization, which arises from unequal access to information and digital power. In the context of online lending, victims are often in vulnerable economic positions and have low digital literacy, making them easily exposed to risk.

National research tends to emphasize legal protection for victims through criminal and administrative channels. International literature adds a dimension of victimization prevention through strengthening guardianship and designing safer systems.

Relevant Criminological Theories

Opportunity theory explains that crime thrives when there is opportunity and oversight is weak. Holt and Bossler (2023) state that cybercrime increases when the risk of being caught is low and social

controls are ineffective. In the context of illegal online lending, weak application oversight and low digital literacy increase the opportunity for crime.

Rahayu's (2024) theory of anomie links economic pressures and a digital consumer culture to the increased use of online loans. Levi and Lord (2023) classify this phenomenon as part of digital economic crime, exploiting the complexity of technology-based systems and organizational structures.

A comparison of previous research shows that Google Scholar studies focus more on the economic factors of victims, while Scopus literature places more emphasis on the structure of perpetrators, economic motives, and system-based prevention designs.

Personal data breaches involving online lenders meet the criteria of cybercrime because they are committed through electronic systems, primarily targeting personal data and aiming for economic gain. This practice demonstrates a pattern of cyber-enabled financial crime that exploits technological dominance and information inequality.

From a criminological perspective, driving factors include economic pressure, digital opportunities, and weak oversight. From a victimological perspective, victims experience financial loss, psychological distress, and reputational damage.

The implementation of the Personal Data Protection Law strengthens the legal basis for enforcement, but its effectiveness requires increased institutional capacity, cross-regional cooperation, and digital literacy education.

CONCLUSION

Personal data breaches by online lenders are a form of modern cybercrime, including digital economic crime. This practice exploits information gaps and technological dominance to gain profit. Victims experience multiple victimizations, encompassing financial, psychological, and social harm.

The Personal Data Protection Act regime has provided a strong legal basis, but the effectiveness of protection depends heavily on consistent law enforcement, accountability of data controllers, and increasing digital literacy among the public.

REFERENCES

Chen, L., & Lee, K. (2024). Data protection enforcement challenges in emerging economies. Computer Law and Security Review, 52, 105921.

Cross, C., & Button, M. (2023). Victims of cybercrime and secondary victimisation. Criminology and Criminal Justice, 23(4), 612 to 628.

Duggan, M. (2022). Digital vulnerability and critical victimology. Journal of Cyber Policy, 7(3), 355 to 372.

Holt, T., & Bossler, A. (2023). Cybercrime in the digital economy. Routledge.

Kurniawati, R., & Lestari, P. (2024). Penyalahgunaan data pribadi dalam praktik pinjaman online ilegal. Jurnal Hukum dan Teknologi, 5(1), 45 to 60.

Levi, M., & Lord, N. (2023). Economic crime in the digital age. British Journal of Criminology, 63(2), 289 to 307.

Martinez, J., & Singh, R. (2023). Fintech abuse and consumer exploitation. Journal of Financial Crime, 30(3), 845 to 860.

Pratama, D., & Nugroho, A. (2023). Kejahatan siber dalam praktik fintech ilegal. Jurnal Hukum IUS QUIA IUSTUM, 30(2), 210 to 228.

Putri, N., & Anwar, S. (2023). Dampak psikologis korban pinjaman online ilegal. Jurnal Kriminologi Indonesia, 19(1), 55 to 73.

Rahman, F., & Siregar, M. (2024). Implementasi Undang Undang Perlindungan Data Pribadi dalam layanan fintech. Jurnal Legislasi Indonesia, 21(1), 78 to 95.

Rahayu, T. (2024). Anomie digital dan perilaku konsumtif masyarakat. Jurnal Sosio Legal, 6(2), 134 to 150.

Santoso, B., & Hidayat, R. (2023). Prinsip perlindungan data pribadi dalam sistem hukum Indonesia. Jurnal RechtsVinding, 12(3), 401 to 420.

Smith, J., & Brooks, L. (2024). Cyber enabled financial crime in fintech platforms. Journal of Financial Regulation and Compliance, 32(1), 15 to 29.

Wall, D. (2023). Cybercrime and society in the information age. Polity Press.

Yar, M. (2022). The transformation of cybercrime. European Journal of Criminology, 19(5), 1023 to 1040.

Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang Undang Nomor 1 Tahun 2024.

Undang Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Otoritas Jasa Keuangan. (2023). Statistik fintech lending Indonesia.