RECHTSVINDING
Vol. 4, 1 (January-June, 2026), pp. 95-100
EISSN: 2987-4424, DOI: https://doi.org/10.59525/rechtsvinding.1339

Criminal Law Enforcement against the Abuse of Personal Data via the Internet in Indonesia

Mixon felly Melky Runtukahu[1], Dudik Djaja Sidarta[1], Vieta Imelda Cornelis[1]

[1] Universitas Dr Soetomo, Indonesia; mixonruntukahu@gmail.com

ARTICLE INFO

Keywords:

Law Enforcement;
Misuse of Personal Data;
Internet

Article history:

Received 2025-11-20
Revised 2025-12-23
Accepted 2026-01-22

ABSTRACT

The development of information technology and the increasingly massive use of the internet have increased the risk of criminal acts of misuse of personal data, especially through cybercrime modes such as phishing and online fraud. The misuse of personal data not only causes material harm to the victim, but also threatens the right to privacy as part of human rights. This article aims to analyze criminal law enforcement against perpetrators of the crime of misusing personal data through the internet and identify the factors that affect the effectiveness of law enforcement. This research uses normative legal research methods with legislative and conceptual approaches. The legal materials used include laws and regulations, especially the Law on Information and Electronic Transactions and Law Number 27 of 2022 concerning Personal Data Protection, supported by relevant scientific literature and journals. The results of the study show that although the legal framework related to personal data protection has been strengthened, law enforcement against the crime of misuse of personal data through the internet still faces various obstacles, including limited capabilities of law enforcement officials, inadequate technological facilities, and low public legal awareness. Therefore, it is necessary to strengthen the capacity of law enforcement officials, optimize information technology facilities, and increase people's digital literacy to realize effective and fair personal data protection.

Corresponding Author:
Mixon felly Melky Runtukahu
Universitas Dr Soetomo, Indonesia; mixonruntukahu@gmail.com

1. INTRODUCTION

The rapid development of information and communication technology has brought significant changes in various aspects of people's lives, especially in the use of the internet as a means of communication, economic transactions, and information exchange. On the one hand, these technological advances provide convenience and efficiency, but on the other hand they also pose various new risks, one of which is the increase in the crime of misuse of personal data through the internet. Personal data that should be protected is actually the object of exploitation by irresponsible parties for the benefit of fraud, identity theft, and other cybercrimes (Sutanto & Kurniawan, 2021).

Misuse of personal data through the internet is a form of cybercrime that has cross-border characteristics, is anonymous, and is difficult to track. Commonly used crime modes include phishing, account hacking, unauthorized dissemination of personal data, and misuse of personal information for illegal transactions. This crime not only causes material damage, but also has a serious impact on the victim's right to privacy and security as part of human rights (Widodo, 2020). In the context of a digital society, personal data protection is a crucial issue that demands an effective and adaptive legal response.

Juridically, personal data protection in Indonesia was previously partially regulated in various laws and regulations, such as Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments. However, the scattered arrangements are considered to be unable to provide comprehensive legal protection and legal certainty for the community. This condition prompted the birth of Law Number 27 of 2022 concerning Personal Data Protection, which specifically regulates the rights of data subjects, the obligations of data controllers and processors, as well as criminal sanctions for personal data breaches (Putri & Rahardjo, 2022).

Although the legal framework for personal data protection has been strengthened, criminal law enforcement against perpetrators of personal data misuse via the internet still faces various challenges. Law enforcement officials are faced with limited human resources who have special expertise in the field of information technology, limited digital forensic facilities and infrastructure, and the complexity of proving in cybercrime cases (Yudhistira, 2021). In addition, low digital literacy and public legal awareness also increase vulnerability to the crime of personal data misuse.

From the perspective of criminal law, the effectiveness of law enforcement is not only determined by the existence of adequate legal norms, but also by the ability of law enforcement officials to apply these norms consistently and professionally. Criminal law enforcement against the misuse of personal data through the internet requires a comprehensive approach, including strengthening regulations, increasing the capacity of law enforcement officials, and cooperation across sectors and countries (Marzuki, 2017). Without these efforts, personal data protection has the potential to be only normative and has not provided real protection for the public.

Based on this background, this article aims to examine the enforcement of criminal law against perpetrators of the crime of misuse of personal data via the internet in Indonesia and identify the factors that affect the effectiveness of law enforcement. This study is expected to make an academic and practical contribution to the development of cyber criminal law and strengthen the protection of personal data in the digital era.

2. METHODS

This research uses normative legal research methods, which are research that places law as a norm or rule that applies in society. This method was chosen because the focus of the study is directed at the analysis of legal regulations and criminal law enforcement against the crime of misuse of personal data through the internet, as regulated in the applicable laws and regulations. Normative legal research allows the author to examine the consistency, adequacy, and effectiveness of legal norms in providing protection for personal data (Soekanto & Mamudji, 2015).

The approaches used in this study include a statutory approach and a conceptual approach. The legislative approach is carried out by systematically examining legal provisions related to the misuse of personal data and cybercrime, including Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments, Law Number 27 of 2022 concerning Personal Data Protection, and other relevant laws and regulations. A conceptual approach is used to examine the concepts and principles of criminal law, protection of privacy rights, and law enforcement theories related to cybercrime.

The sources of legal materials in this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include laws and regulations, relevant court decisions, and official legal documents related to personal data protection. Secondary legal materials are in the form of legal textbooks, scientific journals, results of previous research, and scientific articles that discuss cyber criminal law and personal data protection. Tertiary legal materials are used as supporting materials, such as legal dictionaries and legal encyclopedias, to clarify the terms and concepts used in the research (Marzuki, 2017).

The technique of collecting legal materials is carried out through library research by tracing and inventorying laws and regulations, legal literature, and scientific publications relevant to the research topic. All legal materials that have been collected are then analyzed qualitatively by descriptive-analytical method, namely describing the applicable legal norms and interpreting them systematically to answer research problems. The analysis was carried out by assessing the conformity between legal norms and criminal law enforcement practices against the misuse of personal data via the internet, as well as identifying factors that affect the effectiveness of law enforcement.

3. FINDINGS AND DISCUSSION

1. Characteristics of Abuse of Personal Data over the Internet

The results of the study show that the misuse of personal data through the internet is a form of cybercrime that has special characteristics compared to conventional crimes. This crime is anonymous, crosses state borders, and takes advantage of the weaknesses of the technological system and low digital literacy of the community. The most common modes include phishing, identity theft, hacking of social media and banking accounts, as well as misuse of personal data for online fraud and illegal transactions. The misuse of personal data not only causes economic losses, but also has a serious impact on the victim's right to privacy and sense of security (Widodo, 2020).

From the perspective of cyber criminology, the crime of misuse of personal data is growing along with society's increasing dependence on digital technology. Sutanto and Kurniawan (2021) stated that the more internet-based community activities, the greater the chance of cybercrime that exploits personal data. This condition shows that the protection of personal data cannot be separated from national cybersecurity policies and the strengthening of the criminal law system.

2. Legal Framework for Criminal Law Enforcement against Abuse of Personal Data

Normatively, criminal law enforcement against the misuse of personal data through the internet in Indonesia is based on several legal instruments, especially the Law on Information and Electronic Transactions and Law Number 27 of 2022 concerning Personal Data Protection. The Personal Data Protection Law provides more comprehensive arrangements regarding the rights of data subjects, the obligations of data controllers and processors, as well as criminal sanctions for personal data breaches. The existence of this law marks a shift in the legal paradigm from a sectoral approach towards integrated personal data protection (Putri & Rahardjo, 2022).

However, the results of the study show that although the legal framework has been strengthened, there are still challenges in the effective implementation of criminal norms. Some provisions still require further interpretation, especially related to the elements of error, proof of losses, and criminal liability of cybercrime perpetrators. Marzuki (2017) emphasized that the success of law enforcement is not only determined by the completeness of norms, but also by the clarity of the norm formulation and the ability of the apparatus to implement them.

3. Implementation of Law Enforcement by Law Enforcement Officers

The results of the study show that the implementation of criminal law enforcement against the misuse of personal data through the internet still faces various practical obstacles. Law enforcement officials, especially the police and prosecutor's offices, are often faced with limited human resources who have expertise in the field of information technology and digital forensics. This limitation has an impact on the investigation and proving process of cybercrime cases that require high technical expertise (Yudhistira, 2021).

In addition, the complexity of proving in cases of misuse of personal data is also a challenge in itself. Digital evidence is easy to delete, modify, and store outside of Indonesian jurisdiction. This condition makes it difficult for law enforcement officials to uncover the perpetrators and prove the elements of the crime convincingly in court. Widodo (2020) emphasized that without the support of technological infrastructure and cross-border cooperation, criminal law enforcement against cybercrime tends to be not optimal.

4. Protection of Victims' Rights in Criminal Law Enforcement

From the perspective of victim protection, the results of the study show that victims of personal data abuse still do not receive maximum legal protection. The reporting and handling process often focuses on the aspect of proving a crime, while recovering losses and protecting victims' rights has not been a top priority. This shows that criminal law enforcement is still perpetrator-centric and not yet fully victim-oriented.

The Personal Data Protection Law has actually provided a legal basis for the protection of victims' rights, including the right to compensation and recovery. However, in practice, the mechanism has not been effective due to the lack of understanding of law enforcement officials and the public regarding the rights of victims. Putri and Rahardjo (2022) stated that without a victim-oriented approach, law enforcement against personal data breaches has the potential to lose its legal protection function.

5. Factors Affecting the Effectiveness of Law Enforcement

Based on the results of the discussion, the effectiveness of criminal law enforcement against the misuse of personal data through the internet is influenced by several main factors. First, legal factors, which include the clarity and consistency of laws and regulations. Second, the factors of law enforcement officials, which are related to competence, professionalism, and integrity. Third, facilities and infrastructure factors, especially the availability of technology and support systems for cyber law enforcement. Fourth, community factors, which include the level of digital literacy and legal awareness (Soekanto, 2014).

The low digital literacy of the community causes many victims to not realize that their personal data has been misused or do not know the legal mechanisms that can be taken. This condition strengthens the view that criminal law enforcement must be balanced with preventive efforts through education and increasing public awareness about the importance of personal data protection (Sutanto & Kurniawan, 2021).

6. Critical Analysis and Law Enforcement Implications

In the author's view, the enforcement of criminal law against the misuse of personal data through the internet in Indonesia is still in the transition stage towards a more effective and just system. Strengthening the legal framework through the Personal Data Protection Law is a step forward, but it is not enough without increasing the capacity of law enforcement officials and strengthening technological infrastructure. Criminal law enforcement should not only be repressive, but must be integrated with prevention and victim protection policies on an ongoing basis.

The implications of these findings suggest that personal data protection requires a multidimensional approach involving the state, law enforcement officials, business actors, and society. Without this synergy, criminal law enforcement has the potential to only become a symbolic norm that has not provided real protection for society in the digital era.

Based on the overall results of the study and discussion, the author is of the view that criminal law enforcement against the misuse of personal data through the internet in Indonesia still faces quite complex structural and substantive challenges. Although the state has demonstrated a normative commitment through the establishment of Law Number 27 of 2022 concerning Personal Data Protection, the implementation of its law enforcement has not fully reflected effective legal protection and is oriented towards the interests of victims. In practice, law enforcement still tends to be reactive and focused on the aspect of criminal proof alone, while the dimensions of victim recovery and crime prevention have not received balanced attention.

The author considers that the main problem in law enforcement against the misuse of personal data does not solely lie in the lack of legal norms, but in the limited capacity of law enforcement officials in dealing with the characteristics of cybercrime that are dynamic and cross-border. The limited number of human resources who have digital forensic expertise, coupled with the lack of optimal support for technological infrastructure, has direct implications for the low effectiveness of case handling. This condition shows that there is a gap between the development of cybercrime and the ability of the criminal justice system to respond quickly and appropriately.

In addition, the author is of the view that low digital literacy and public legal awareness also exacerbate the problem of misuse of personal data. Many victims are not aware that the actions they experienced are criminal acts, or do not know the legal mechanisms that can be taken. In this context, criminal law enforcement cannot stand alone, but must be integrated with public education policies and increasing public awareness of the importance of personal data protection as part of human rights.

Furthermore, the authors argue that the ideal criminal law enforcement approach to the misuse of personal data through the internet should adopt a more victim-oriented justice paradigm. This means that the law enforcement process is not only aimed at imposing sanctions on the perpetrators, but also ensuring a proper recovery for the victim, both in the form of compensation, rehabilitation, and protection from victimization. Without this approach, law enforcement has the potential to lose its social legitimacy and is unable to provide a sense of justice for the community.

Thus, the authors conclude that the effectiveness of criminal law enforcement against the misuse of personal data through the internet requires systemic and sustainable strengthening. The strengthening includes institutional reform, capacity building of law enforcement officials, optimizing the use of information technology, and building a community legal culture that respects and protects personal data. This comprehensive approach is what the author believes is the main key to realizing effective and fair personal data protection in the digital era.

4. CONCLUSION

Based on the results of the study and discussion, it can be concluded that the misuse of personal data through the internet is a form of cybercrime that is increasingly complex and has a serious impact on people's privacy and security rights. The characteristics of anonymous, cross-border, and technology-based crimes make criminal law enforcement against these criminal acts face significant challenges, both from normative and implementive aspects.

Juridically, Indonesia already has a more comprehensive legal framework through Law Number 27 of 2022 concerning Personal Data Protection which strengthens the protection of data subjects' rights and provides a criminal basis for personal data breaches. However, the effectiveness of criminal law enforcement is still not optimal due to the limited capacity of law enforcement officials, the lack of support for digital forensic facilities and infrastructure, and the complexity of proving in cybercrime cases.

In addition, low digital literacy and public legal awareness also affect the weak protection of personal data, because many victims are not aware of their rights or are reluctant to take legal proceedings. Therefore, criminal law enforcement against the misuse of personal data through the internet requires a more comprehensive and sustainable approach, not only through enforcement of perpetrators, but also through strengthening the capacity of law enforcement officials, optimizing technology, and increasing public education and legal awareness.

Thus, effective criminal law enforcement against the misuse of personal data must be directed at a protection system that is victim-oriented, preventive, and adaptive to technological developments, in order to realize legal certainty, justice, and protection of people's privacy rights in the digital era.

REFERENCES

Arief, B. N. (2018). Bunga rampai kebijakan hukum pidana. Jakarta: Kencana.

Chazawi, A. (2016). Hukum pidana positif Indonesia. Malang: Setara Press.

Direktorat Jenderal Aplikasi Informatika. (2021). Pedoman perlindungan data pribadi dalam sistem elektronik. Jakarta: Kementerian Komunikasi dan Informatika Republik Indonesia.

Hamzah, A. (2019). Hukum pidana Indonesia. Jakarta: Sinar Grafika.

Hiariej, E. O. S. (2016). Prinsip-prinsip hukum pidana. Yogyakarta: Cahaya Atma Pustaka.

Ilyas, A. (2018). Asas-asas hukum pidana. Yogyakarta: Rangkang Education.

Marzuki, P. M. (2017). Penelitian hukum. Jakarta: Kencana.

Moeljatno. (2015). Asas-asas hukum pidana. Jakarta: Rineka Cipta.

Muladi, & Arief, B. N. (2010). Teori-teori dan kebijakan pidana. Bandung: Alumni.

Nasution, B. J. (2022). Penegakan hukum terhadap pelanggaran data pribadi di Indonesia pasca Undang-Undang Perlindungan Data Pribadi. Jurnal Konstitusi, 19(3), 467–485.

Prasetyo, T. (2019). Hukum pidana. Jakarta: RajaGrafindo Persada.

Putusan Mahkamah Agung Republik Indonesia Nomor 1125 K/Pid.Sus/2020.

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

Republik Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.

Republik Indonesia. (2023). Kitab Undang-Undang Hukum Pidana. Jakarta: Kementerian Hukum dan HAM RI.

Sari, D. P. (2021). Perlindungan hukum terhadap data pribadi pengguna internet di Indonesia. Jurnal Ilmu Hukum, 9(1), 89–104.

Sitompul, A. (2012). Hukum internet (cyber law). Bandung: Citra Aditya Bakti.

Soekanto, S., & Mamudji, S. (2015). Penelitian hukum normatif. Jakarta: RajaGrafindo Persada.

Sutrisno, E. (2023). Penegakan hukum pidana terhadap penyalahgunaan data pribadi melalui media elektronik. Jurnal Hukum dan Pembangunan, 53(2), 210–226.

Widodo. (2020). Tindak pidana siber dan perlindungan data pribadi. Jurnal Legislasi Indonesia, 17(4), 523–538.