

Criminal Liability for Data Protection Violations in Police Digital Services (A Study of the North Sumatra Regional Police)

Heru Kurniawan, Henry Aspan, Fitri Rafianti

Abstract

The development of digital services within the Indonesian National Police, particularly within the North Sumatra Regional Police, has improved the efficiency of public services, including in the management of public data. However, on the other hand, this digitalization also poses potential risks of violations of personal data protection. This study aims to analyze the forms of criminal liability for violations of data protection in police digital services, as well as to examine its implementation at the North Sumatra Regional Police. The research method used is a legal-empirical approach with a legislative and case study perspective. Data was collected through interviews, observations, and document reviews related to data management practices within the police force. The research findings indicate that criminal liability for personal data breaches in police digital services can be imposed based on provisions in Law No. 27 of 2022 on Personal Data Protection as well as internal police regulations. However, its implementation still faces various challenges, including limited human resources, suboptimal information security systems, and low legal awareness among police personnel regarding the importance of personal data protection. Furthermore, law enforcement mechanisms regarding data breaches within the police environment have not been fully operational, whether in terms of reporting, investigation, or the imposition of criminal sanctions.

Keywords: *Criminal Liability, Personal Data Protection, Digital Police Services, Law Enforcement.*

Heru Kurniawan¹

¹Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: niaserukur@gmail.com¹

Henry Aspan², Fitri Rafianti³

^{2,3}Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: henryaspan@yahoo.com², fitrirafianti@dosen.pancabudi.ac.id³

2nd International Conference on Islamic Community Studies (ICICS)

Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era

<https://proceeding.pancabudi.ac.id/index.php/ICIE/index>

Introduction

Advances in information technology have brought significant changes to public service systems in Indonesia, including within the Indonesian National Police. The digital transformation undertaken by the police aims to improve the effectiveness, transparency, and accessibility of services to the public.[1] Digital services such as online crime reporting, public complaints, and electronic data management are part of these modernization efforts. [2] However, the use of this technology has also raised new issues, particularly regarding the security and protection of citizens' personal data managed by police institutions.[3]

In practice, the management of personal data in police digital services carries the potential risk of leaks, misuse, or unauthorized access by third parties.[4] This situation raises concerns about the weakness of data protection systems, particularly when the data being managed is sensitive and directly related to individuals' identities and privacy. [5] Therefore, the enactment of Law No. 27 of 2022 on Personal Data Protection serves as a crucial legal foundation for ensuring the public's right to personal data protection while also providing a basis for law enforcement against any violations that occur.[6]

Normatively, violations of personal data protection may be subject to criminal penalties if they meet the elements specified in the applicable laws and regulations. [7] The concept of criminal liability in this context applies not only to individual perpetrators but may also involve institutions if negligence or intentional misconduct in data management is proven. This aligns with the principle that every operator of an electronic system is obligated to ensure the security and confidentiality of the data it manages (Suhariyanto, 2023).[8]

At the empirical level, the implementation of personal data protection within the police force, particularly at the North Sumatra Regional Police Headquarters, still faces various challenges. [9] These challenges include limited cybersecurity infrastructure, a lack of understanding among officers regarding data protection regulations, and suboptimal internal oversight mechanisms.[10] Furthermore, the absence of comprehensive standard operating procedures regarding digital data management also has the potential to create legal loopholes in the enforcement of criminal liability.[11]

One of the cases previously handled by the North Sumatra Regional Police involved the use of electronic evidence and digital forensic examinations in the Langkat Regency PPPK case. During the investigation into alleged corruption in the 2023 PPPK recruitment in Langkat, investigators from the North Sumatra Regional Police examined electronic devices and digital data to strengthen the evidence in the case. During this process, they accessed electronic documents, participant identities, administrative data, and digital communications of the parties involved. The North Sumatra Regional Police even enlisted the help of digital forensic experts to strengthen the electronic evidence in the case.

Given this background, this study is important for conducting a more in-depth examination of the nature of criminal liability for data protection violations in police digital services, as well as how such liability is implemented at the local level. This study is expected to contribute to strengthening the legal system and data protection policies within the police force, while also enhancing public trust in the digital services provided by law enforcement agencies.

Literature Review

1. The Concept of Criminal Liability

Criminal liability is a fundamental concept in criminal law that determines whether a person can be held accountable for an act committed. In criminal law doctrine, criminal liability requires the existence of an unlawful act (*actus reus*) and criminal intent (*mens rea*). [12] According to Moeljatno, a person can only be punished if their act fulfills the elements of a criminal offense and there is culpability that can be attributed to them. This concept also emphasizes the importance of accountability (*toerekeningsvatbaarheid*) and the absence of exculpatory or justifying grounds.[13]

In the modern context, criminal liability is not only imposed on individuals but also on corporations or institutions. This is particularly relevant in the provision of digital services by state institutions such as the Indonesian National Police, where errors in system management can have far-reaching consequences for the public. Therefore, the concept of criminal liability has evolved to accommodate forms of institutional negligence and system failures as grounds for criminal prosecution.[14]

2. Personal Data Protection from a Legal Perspective

The protection of personal data is a fundamental human right related to the right to privacy. In Indonesia, comprehensive regulations regarding personal data protection are set forth in Law No. 27 of 2022 on Personal Data Protection. This law establishes the fundamental principles of data management, the rights of data subjects, the obligations of data controllers, as well as administrative and criminal penalties for violations.[15]

Personal data protection encompasses the entire process of collecting, storing, using, and destroying data, all of which must be carried out lawfully and responsibly. Additionally, data controllers are required to ensure adequate security systems are in place to prevent data breaches. This aligns with the principle of accountability, which places full responsibility on electronic system operators for the security of the data they manage.[16]

In the international context, personal data protection is also influenced by global standards such as the General Data Protection Regulation (GDPR) in the European Union, which serves as a reference for the formulation of national policies. Principles such as lawful processing, consent, and data minimization have also been adopted into Indonesia's legal system to strengthen protection for the public.[17]

3. Police Digital Services and the Risk of Data Breaches

The digital transformation within the Indonesian National Police has led to various innovations in electronic public services, such as online reporting systems, the issuance of Police Clearance Certificates (SKCK), and app-based public complaint systems. While this digitization aims to improve efficiency and transparency, it also introduces new potential risks, particularly regarding data security.[18]

Advances in information technology are always accompanied by the potential for cybercrime, including the theft and misuse of personal data. In the context of law enforcement, this risk becomes even more complex because the data handled is often sensitive and relates to law enforcement processes. Therefore, robust security systems and clear regulations are needed to prevent violations.[19]

Previous research has shown that weaknesses in security systems, a lack of staff training, and insufficient internal oversight are the main factors contributing to data breaches in the public sector. This indicates that digital transformation requires not only technological innovation but also legal and institutional readiness.[20]

Several previous studies have examined the issues of personal data protection and legal liability in the digital age.

- a. In his research, emphasizes that the protection of personal data in Indonesia still faces challenges in implementation, particularly regarding law enforcement, which remains suboptimal.[21] Meanwhile, states that the legal responsibilities of electronic system operators must be strengthened through strict regulations and effective oversight mechanisms.[22]
- b. Notes that criminal liability for personal data breaches is often difficult to enforce due to evidentiary challenges and the lack of clarity regarding the division of responsibility between individuals and institutions. This is particularly important in the context of digital police services, where operations are collective and technology-driven.[23]

Based on this study, it can be concluded that there remains a gap between regulations and the implementation of personal data protection in Indonesia. Therefore, this study aims to

address this gap by focusing on the analysis of criminal liability for data breaches within the police force, specifically at the North Sumatra Regional Police Headquarters.

Research Methodology

1. Type and Nature of the Research

This study employs an empirical legal research method using an empirical juridical approach. The empirical juridical approach involves an examination of applicable legal provisions regarding personal data protection and their implementation in digital police services within the North Sumatra Regional Police. This study not only examines the legal norms contained in legislation but also observes the implementation and enforcement practices regarding violations of data protection in digital police services. The nature of this study is descriptive-analytical, meaning it aims to systematically describe the forms of criminal liability for violations of personal data protection and to analyze the application of legal provisions in the practice of police digital services. This study also identifies various obstacles encountered in the implementation of personal data protection within the North Sumatra Regional Police.

2. Research Approach

The approaches used in this study include:

a. Statutory Approach (statute approach)

This approach involves examining various laws and regulations related to personal data protection and criminal liability, including:

- i. Law No. 27 of 2022 on Personal Data Protection;
- ii. Law No. 19 of 2016 Amending Law No. 11 of 2008 on Electronic Information and Transactions;
- iii. Law No. 2 of 2002 on the National Police of the Republic of Indonesia;
- iv. Police regulations regarding digital services and the management of electronic data.

b. Conceptual Approach

This approach is used to understand the concepts of criminal liability, personal data protection, cybersecurity, and the principles of criminal law related to the misuse of electronic data.

c. Case Approach

The case approach involves analyzing practices and incidents related to alleged data protection violations in police digital services, particularly within the North Sumatra Regional Police.

3. Research Location

The study was conducted at the North Sumatra Regional Police Headquarters, an institution that provides digital public services and has authority over the management of public data. The choice of research location was based on the fact that the North Sumatra Regional Police Headquarters has implemented various electronic service systems directly related to the collection and management of citizens' personal data.

Results

1. Forms of Criminal Liability for Data Protection Violations in Police Digital Services (A Study at the North Sumatra Regional Police Headquarters)

Digital transformation in police services—such as the use of electronic reporting systems, online registration, public identity databases, and app-based complaint services—has improved the effectiveness of public services. However, this digitalization also poses new risks in the

form of misuse and leaks of citizens' personal data. In the context of digital services within the North Sumatra Regional Police, forms of data protection violations can include illegal access to public data, the dissemination of information without the data owner's consent, the use of data for personal gain, or weak electronic security systems leading to data breaches. This situation underscores that the security of personal data is a critical component in the delivery of electronic public services.[24]

Based on the research findings, criminal liability for data protection violations in police digital services can be categorized into individual liability and institutional liability. Individual liability applies to officials or specific parties who intentionally access, obtain, transfer, or disseminate personal data without authorization. Such acts constitute criminal offenses as stipulated in Law No. 27 of 2022 on Personal Data Protection and the Law on Information and Electronic Transactions. The element of fault in these criminal offenses lies in the presence of intent (*dolus*) or negligence (*culpa*) that results in harm to the data subject.

In practice, law enforcement officers with access to internal data systems have the potential to abuse their authority if there are no strict oversight mechanisms in place. For example, using citizens' identity data for purposes outside official duties, granting data access to third parties, or collecting data without a valid legal basis. Such actions may be subject to criminal penalties as they violate the principles of lawful processing and the confidentiality of personal data. In addition to imprisonment and fines, perpetrators may also face administrative sanctions or disciplinary action under the police code of ethics.[25]

In addition to individual accountability, the police institution as the controller of personal data also has legal responsibility if it is proven negligent in maintaining the security of electronic systems. Failure to provide adequate cybersecurity systems can be categorized as a form of institutional negligence, especially if a data breach occurs due to weak internal supervision or lack of information technology security standards. From a modern criminal law perspective, corporate or institutional accountability can be applied if a criminal act is committed within the scope of the institution's duties and authority. Therefore, if a data breach occurs in police digital services due to systemic negligence, the institution can be held legally accountable in accordance with the provisions of the Personal Data Protection Law.[26]

This study also found that the implementation of personal data protection in the police environment still faces various obstacles. Some of these obstacles include limitations in human resources in the field of cyber security, suboptimal supervision of internal data access, and the absence of integrated standard operating procedures regarding the management of citizens' personal data. These conditions have resulted in data protection not being fully effective and have opened up opportunities for violations by certain individuals.

From the criminal law perspective, the application of accountability for personal data violations within the police digital services is a form of protection for the public's privacy rights. The state has an obligation to ensure the security of citizens' data, especially when such data is managed by law enforcement agencies. Therefore, law enforcement against personal data violations not only aims to provide a deterrent effect to the perpetrators but also to build public trust in the police institution in the implementation of safe and accountable digital services.[27]

2. Implementation of Personal Data Protection in Digital Police Services at the Regional Level

The implementation of digital services within the North Sumatra Regional Police is part of the policy of modernizing public services based on information technology. This implementation can be seen through the use of community reporting applications, electronic administration systems, online Police Record Certificates (SKCK) services, as well as digital-based case data management. The presence of these electronic systems is essentially aimed at improving service efficiency and accelerating public access to police services. However, the use of digital technology also requires stricter personal data protection because the police institution manages large amounts of confidential public data.[28]

Based on the results of the research, the implementation of personal data protection at the regional level is still in the stage of adjusting to the provisions of Law Number 27 of 2022 concerning Personal Data Protection. In the environment of the North Sumatra Regional Police, data protection efforts are carried out through restricting access to internal systems, the use of special accounts for personnel, as well as the application of network security in electronic-based services. However, the implementation has not yet been fully optimal because weaknesses in monitoring data usage are still found and personnel understanding of personal data protection principles is not yet evenly distributed.

In its implementation, the management of personal data of the public in police digital services involves various work units with different authorities. This condition creates its own challenges in maintaining data security because the more parties that have access to the electronic system, the greater the potential for data misuse. Therefore, strict internal control mechanisms are required, such as recording data access activities (log activity), limiting user authorization, and periodic audits of the police information system. These measures are important to prevent data leaks as well as the use of information outside the interests of law enforcement.[29]

This research shows that the implementation of personal data protection at the regional level is also influenced by human resource factors. Not all personnel have technical abilities in the field of cybersecurity and electronic data governance. As a result, there are still negligence issues in account management, the use of personal devices for official purposes, as well as a weak awareness of the importance of community data confidentiality. These conditions indicate that personal data protection does not only depend on technological systems, but is also influenced by the professionalism of the officers operating those systems.[30]

In addition to human resource constraints, the implementation of data protection at the regional level also faces infrastructure obstacles. Some digital service systems in the regions still have limitations in terms of network security, server capacity, and the integration of information systems between units. These weaknesses have the potential to cause cyber security disturbances that can result in illegal access as well as personal data breaches of the public. Therefore, improving the quality of information technology infrastructure becomes an important part of supporting the effectiveness of personal data protection within regional police environments.[31]

From the perspective of administrative law and criminal law, the implementation of personal data protection at the regional level must be carried out based on the principles of accountability, prudence, and legal certainty. The police institution, as the data controller, has an obligation to ensure that every collection, storage, use, and destruction of data is carried out in accordance with applicable legal procedures. If violations occur due to the negligence of officers or weaknesses in the security system, the responsible institution or individuals can be subject to administrative sanctions, codes of ethics, and even criminal sanctions in accordance with the laws and regulations.

The research results also show that internal supervision is an important factor in the successful implementation of personal data protection within regional police departments. Regular supervision can minimize the potential misuse of data by certain individuals. In addition, it is necessary to establish more detailed standard operating procedures regarding digital data management, including mechanisms for handling data breach incidents and the responsibilities of each work unit. Thus, the implementation of personal data protection at the North Sumatra Regional Police can run more effectively and be able to increase public trust in the police's digital services.

Conclusion

Based on the results of the research and discussion regarding criminal liability for data protection violations in police digital services (a study of the North Sumatra Regional Police), the following conclusions can be drawn:

1. Criminal liability for violations of data protection in police digital services can be imposed on both individuals and institutions. Individual liability is attributed to officers or parties who intentionally or negligently perform illegal access, misuse, dissemination, or disclosure of citizens' personal data without authorization. Such actions can be subject to criminal sanctions under Law Number 27 of 2022 on Personal Data Protection and the Electronic Information and Transactions Law. In addition to criminal sanctions, offenders can also be subject to ethical and administrative sanctions in accordance with internal police regulations. Meanwhile, institutional accountability can arise if there is negligence in supervising, securing electronic systems, or managing personal data that results in the leakage of public data. In this case, the police institution has a legal obligation to ensure the security of data managed in digital services.
2. The implementation of personal data protection within the North Sumatra Regional Police has been carried out through the use of electronic security systems, data access restrictions, and internal supervision of police digital services. However, its application is still not optimal due to several obstacles, such as limited human resources in the field of cybersecurity, weak supervision of internal data access, and the suboptimal implementation of standard operating procedures regarding personal data protection. In addition, there is still a need to improve information technology infrastructure, provide training for personnel, and strengthen internal supervision systems so that personal data protection in police digital services can be carried out more effectively, safely, and in accordance with the principles of legal certainty and the protection of public privacy rights.

References

- [1] "Transformasi Digital Pelayanan Publik di Indonesia." *Jurnal Administrasi Publik*, Vol. 12 No. 2, 2021.
- [2] "Digitalisasi Pelayanan Kepolisian dan Tantangan Perlindungan Data Pribadi." *Jurnal Hukum dan Teknologi Informasi*, Vol. 5 No. 1, 2022.
- [3] "Modernisasi Sistem Pelayanan Kepolisian Berbasis Elektronik." *Jurnal Reformasi Hukum*, Vol. 7 No. 3, 2023.
- [4] "Risiko Keamanan Data Pribadi dalam Pelayanan Publik Berbasis Digital." *Jurnal Keamanan Siber dan Hukum*, Vol. 4 No. 2, 2022.
- [5] "Perlindungan Privasi dan Data Sensitif dalam Sistem Elektronik Pemerintah." *Jurnal Hukum Teknologi Indonesia*, Vol. 6 No. 1, 2023.
- [6] "Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia." *Jurnal Legislasi Indonesia*, Vol. 19 No. 4, 2022.
- [7] "Pertanggungjawaban Pidana terhadap Pelanggaran Data Pribadi di Indonesia." *Jurnal Ius Constitutum*, Vol. 7 No. 2, 2022.
- [8] Suhariyanto. "Perlindungan Data Pribadi dan Keamanan Sistem Elektronik dalam Perspektif Hukum Pidana." *Jurnal RechtsVinding*, Vol. 12 No. 1, 2023.
- [9] "Implementasi Perlindungan Data Pribadi dalam Institusi Kepolisian." *Jurnal Hukum dan Teknologi*, Vol. 8 No. 2, 2023.
- [10] "Tantangan Keamanan Siber dan Pengawasan Internal pada Lembaga Penegak Hukum." *Jurnal Keamanan Nasional*, Vol. 6 No. 1, 2022.
- [11] "Urgensi Standar Operasional Pengelolaan Data Digital dalam Penegakan Hukum." *Jurnal Legislasi dan Penegakan Hukum*, Vol. 5 No. 3, 2023.
- [12] "Analisis Unsur Actus Reus dan Mens Rea dalam Hukum Pidana Modern." *Jurnal Hukum Pidana*, Vol. 8 No. 1, 2024.
- [13] "Kemampuan Bertanggung Jawab dan Alasan Penghapus Pidana dalam KUHP Nasional." *Jurnal Legislasi Hukum*, Vol. 5 No. 1, 2025.
- [14] "Kelalaian Institusional dan Kegagalan Sistem sebagai Dasar Pertanggungjawaban Pidana." *Jurnal Legislasi dan Kebijakan Publik*, Vol. 6 No. 1, 2025.

- [15] “Sanksi Hukum terhadap Pelanggaran Perlindungan Data Pribadi menurut UU No. 27 Tahun 2022.” *Jurnal Hukum dan Teknologi Informasi*, Vol. 8 No. 3, 2023.
- [16] “Prinsip Akuntabilitas dalam Pengelolaan Data Pribadi oleh Penyelenggara Sistem Elektronik.” *Jurnal Legislasi dan Kebijakan Digital*, Vol. 7 No. 1, 2024.
- [17] “Adopsi Prinsip GDPR dalam Undang-Undang Perlindungan Data Pribadi Indonesia.” *Jurnal Legislasi dan Teknologi Informasi*, Vol. 8 No. 1, 2024.
- [18] “Digitalisasi Layanan Kepolisian dan Risiko Keamanan Data.” *Jurnal Teknologi Informasi dan Hukum*, Vol. 7 No. 1, 2024.
- [19] “Regulasi dan Sistem Keamanan Siber dalam Pelayanan Publik Elektronik.” *Jurnal Legislasi Digital*, Vol. 9 No. 1, 2024.
- [20] “Kesiapan Hukum dan Kelembagaan dalam Transformasi Digital Pelayanan Publik.” *Jurnal Administrasi Negara dan Kebijakan Publik*, Vol. 9 No. 1, 2023.
- [21] Widodo. “Problematisasi Implementasi Perlindungan Data Pribadi di Indonesia.” *Jurnal Hukum dan Pembangunan*, Vol. 50 No. 3, 2020.
- [22] Edmon Makarim. “Tanggung Jawab Hukum Penyelenggara Sistem Elektronik dalam Perlindungan Data Pribadi.” *Jurnal Legislasi Indonesia*, Vol. 19 No. 2, 2022.
- [23] “Pertanggungjawaban Pidana terhadap Pelanggaran Data Pribadi dalam Sistem Elektronik.” *Jurnal RechtsVinding*, Vol. 12 No. 1, 2023.
- [24] “Metode Penelitian Yuridis Empiris dalam Kajian Hukum Kontemporer.” *Jurnal Ilmu Hukum*, Vol. 14 No. 2, 2022.
- [25] Barda Nawawi Arief, *Masalah Penegakan Hukum dan Kebijakan Hukum Pidana dalam Penanggulangan Kejahatan*, Kencana, Jakarta, 2021.
- [26] Teguh Prasetyo, *Hukum Pidana*, Rajawali Pers, Jakarta, 2022.
- [27] Johan Alfred Sarades Silalahi, Yuspika Yuliana Purba, dan Muhammad Fadly Nasution, “Analisis Yuridis terhadap Mekanisme Perlindungan Data Pribadi dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana di Indonesia,” *Jurnal Minfo Polgan*, 2025.
- [28] Barda Nawawi Arief, *Kebijakan Hukum Pidana: Perkembangan Penyusunan Konsep KUHP Baru*, Kencana, Jakarta, 2021.
- [29] Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, RajaGrafindo Persada, Jakarta, 2020.
- [30] Abdul Kadir Muhammad, *Hukum dan Penelitian Hukum*, Citra Aditya Bakti, Bandung, 2021.
- [31] Johan Alfred Sarades Silalahi, Yuspika Yuliana Purba, dan Muhammad Fadly Nasution, “Analisis Yuridis terhadap Mekanisme Perlindungan Data Pribadi dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana di Indonesia,” *Jurnal Minfo Polgan*, 2025