The Criminal Law Behind Digital Fingerprints: Biometric Data Protection in Modern Security Systems

Ni Putu Rai Yuliartini[1*], *Dewa Gede Sudika* Mangku[1], and *Gede* Sariasa[1]

[1]Ganesha University of Education, Buleleng, Indonesia

Abstract. Biometric data, such as fingerprints, facial recognition, retina scans, and voice scans, constitute unique and irreplaceable forms of personal identification. In the digital era, biometric data is increasingly used in electronic security systems for identity verification and user authentication. However, despite these benefits, there are potential risks of privacy violations and data misuse, which impact human rights. This study aims to analyze the legal protection of biometric data in digital security systems from a criminal law perspective and examine criminal liability in the event of biometric data leaks or misuse. The research method used is a normative juridical approach, examining relevant statutory provisions, such as Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), and the Criminal Code (KUHP). The results show that although biometric data has been recognized as legally protected personal data, criminal law enforcement mechanisms for biometric data-related violations are still suboptimal. This is due to the lack of clear technical regulations and limitations regarding the definition, storage, and use of biometric data by electronic system administrators. This study concludes that strengthening criminal law regulations and implementing policies is necessary to ensure comprehensive biometric data protection, including imposing strict sanctions on perpetrators of misuse and increasing corporate responsibility in maintaining the security of the public's digital data.

1 Introduction

The development of digital technology has brought about a major transformation in modern security systems that increasingly rely on artificial intelligence and automation to maintain data integrity and prevent cybercrime. One of the most significant innovations in this development is the use of biometric data, such as digital fingerprints, facial recognition, and retinal scans, as identity authentication tools that are considered the most secure and efficient. Biometric technology works by utilizing the unique biological or physiological characteristics of each individual that are difficult to fake or imitate, thus providing a much

* Corresponding author: raiyuliartini@undiksha.ac.id

higher layer of protection compared to conventional security systems based on passwords, identity cards, or PINs that are vulnerable to theft and misuse

In the context of law and security enforcement, the use of biometric data is a significant breakthrough that not only increases the effectiveness of surveillance and criminal identification systems but also strengthens the accuracy of evidence in criminal justice processes. Biometric data, such as digital fingerprints, is now widely used by law enforcement agencies, banking institutions, and government agencies to ensure the authenticity of user identities, prevent document forgery, and expedite verification processes in various public and private sector services. However, these advances also pose new legal and ethical challenges. The collection, storage, and processing of biometric data pose serious risks to privacy and human rights, particularly when the data is misused, leaked, or exploited without the individual's consent [1]. Therefore, the legal system is required to adapt quickly to provide a regulatory framework capable of protecting individuals from potential privacy violations and data misuse. In this context, biometric data protection is not only a technological issue, but also a criminal law and human rights issue that demands a balance between public security interests and the protection of individual rights in the digital age [2].

However, with the increasing reliance on biometric data in various aspects of modern life, from national security systems and banking services to access to personal devices, new and complex issues have emerged regarding privacy protection and the potential for misuse of personal data. Biometric data, such as digital fingerprints, facial patterns, or retinal scans, are highly sensitive because they are directly linked to each individual's unique biological identity [3]. When such data is collected, stored, and processed without adequate security mechanisms, the risk of data leaks, hacking, or illegal use becomes very high. Furthermore, misuse of biometric data can have serious implications for an individual's right to privacy, including the possibility of excessive surveillance (mass *surveillance)*, unauthorized activity tracking, and digital identity theft, which can threaten personal and social security [4]. In a legal context, this issue becomes increasingly important because the absence of regulations that clearly regulate criminal liability for violations involving biometric data can create legal uncertainty and hinder efforts to uphold justice. Therefore, the issue of biometric data protection is now a serious concern in the field of criminal law and personal data protection, considering the urgency to balance the need for security and respect for human rights in the increasingly connected digital era and the high risk of exploitation of personal information.

Various previous studies have highlighted the urgency of legal protection for personal data in the increasingly complex and globally connected digital era. A study by Muzairoh in *the Borobudur Law and Society Journal* (2024) shows that digital transformation has significant implications for the protection of individual privacy rights, especially when personal data is collected and managed by third parties without adequate legal oversight [5]. Research by Disemadi (2023) confirms that legal protection for personal data in Indonesia still focuses on the context of electronic transactions and consumer protection, where the aspect of monitoring the use of personal data has not been effective due to weak regulations and enforcement of sanctions. [6]. Meanwhile, a study by Yuyut Prayuti (2024) highlighted the increasing risk of privacy violations in the e-commerce ecosystem due to the intensive use of digital technology, including the practice of collecting biometric data such as fingerprints and facial recognition for user authentication. Early studies generally focused on the protection of electronic data and consumer information in general, while attention to biometric data as a stand-alone legal entity has only emerged in recent years, with the development of digital identity-based security systems [7]. These studies also show a gap between the development of biometric identification technology and the ability of national regulations to guarantee user security and privacy. When compared with international legal standards such as the General Data Protection Regulation (GDPR) in the European Union, which expressly regulates the processing and storage of biometric data as a special category

of personal data, the Indonesian legal system is considered fragmented and does not comprehensively regulate criminal liability for the misuse or leakage of biometric data. Therefore, this study aims to fill this gap by examining the relationship between criminal law and biometric data protection, in order to strengthen the national legal basis so that it aligns with globally recognized privacy protection principles

The research gap is apparent in the absence of a comprehensive discussion regarding the relevance of criminal law in regulating data protection. Biometrics as part of a modern security system. Many studies focus on administrative or civil regulations, but the criminal aspects of violators are rarely examined in depth. Furthermore, there is no legal framework that explicitly explains how biometric digital evidence can be used and protected in legal proceedings, creating a tension between security needs and the right to privacy. Thus, there is an urgent need to examine the position of criminal law in balancing these two interests—namely, public security and the protection of individuals' rights to their personal data.

This research offers a conceptual approach by linking legal theory Modern criminal law and biometric data protection principles serve as the basis for building a comprehensive protection model. This approach is based on the view that criminal law serves not only as a repressive tool after a violation occurs, but also as a preventive tool that regulates the safe and ethical governance of biometric data. In this context, this article will examine the potential application of criminal law to biometric data breaches, whether in the form of illegal access, data misuse, or unauthorized distribution, by considering practices and regulations in several countries as a comparison.

The purpose of this study is to analyze the basis and limitations of the application of criminal law to biometric data breaches in modern security systems, and to identify the need for national legal reforms to address increasingly complex digital security challenges. Methodologically, this study employs a normative-comparative approach by analyzing national and international regulations and reviewing relevant court decisions. Thus, the results of this study are expected to provide theoretical contributions to the development of cybercriminal law and practical contributions to the formation of biometric data protection policies in Indonesia.

2 Methods

The research method used in this study is normative legal research, also known as doctrinal legal research, which examines legal norms, principles, and legal doctrine through literature review. This research focuses on analyzing the legal framework governing the protection of biometric data, particularly digital fingerprints, in modern security systems.

This research employs two approaches: a legislative approach and a conceptual approach. The legislative approach examines and analyzes various laws and regulations related to personal data protection and cybercrime, both at the national and international levels. The national legal instruments referenced include Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), the Criminal Code (KUHP), and regulations related to information technology and electronic transactions. Internationally, this research refers to the European Union's General Data Protection Regulation (GDPR) and international human rights norms that guarantee the protection of privacy and personal data.

A conceptual approach is used to develop a framework and theoretical basis for biometric data protection, including key concepts such as the right to privacy, data security, consent , and legal responsibilities in the use of digital identification systems [8]. This approach helps explain the legal doctrines that form the basis for assessing data protection obligations and the criminal law implications of misuse or unauthorized access to biometric information.

The legal data collection techniques used in this study include primary, secondary, and tertiary legal data. Primary legal data includes laws and regulations, government decisions,

and international legal instruments relevant to biometric data protection and digital security . Secondary legal data consists of academic literature, scientific articles, expert opinions, and previous research findings addressing data security and cybercriminal law. Tertiary legal data, such as legal dictionaries, encyclopedias, and legal indexes, are used to provide additional explanations of the concepts analyzed

The legal materials analysis was conducted by classifying each legal material based on its hierarchy and relevance, then interpreting and evaluating it to assess the extent to which existing legal norms are adequate in providing protection for biometric data. This analysis also includes an assessment of the effectiveness of the application of criminal law in addressing violations involving digital fingerprints and other biometric data. Thus, the results of this study are expected to provide a comprehensive picture of the extent to which national and international legal systems are able to respond to the challenges of biometric data protection in the digital era, as well as how criminal law can play a role in ensuring accountability and protecting individual privacy rights.

3 Results and discussion

3.1 Results

The research results show that legal protection for biometric data, particularly digital fingerprints in modern security systems, is still fragmented and has not been optimally harmonized between national and international legal frameworks. In normative studies, this is evident in the absence of comprehensive and integrated regulations regarding biometric data governance that cover aspects of protection, processing, and legal accountability for misuse of such data. Although a number of legal instruments have regulated personal data in general, the legal concept of biometric data as an object of special protection is still developing conceptually and requires normative confirmation in the national legal system.

Through a legislative approach, this study found that Indonesia has begun to recognize the importance of personal data protection as a fundamental right of citizens through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law is an important milestone in the history of cyber law in Indonesia because it provides explicit recognition for the first time to biometric data as a category of personal data that has sensitive characteristics and must be protected with a higher level of security. Normatively, Article 4 paragraph (2) of the PDP Law states that specific personal data includes health data, biometric data, genetic data, criminal records, child data, personal financial data, and other data in accordance with the provisions of laws and regulations. This provision confirms that biometric data has its own legal status and is within the scope of strict protection, given its nature that cannot be changed or replaced like passwords or conventional identity numbers.

Conceptually, the legal recognition of biometric data in the PDP Law indicates a shift in the legal paradigm from mere administrative data protection to the protection of constitutional rights to privacy and personal integrity [9]. From a human rights perspective, biometric data protection is not only a technical issue of information management, but also part of the right to privacy as stipulated in Article 28G of the 1945 Constitution of the Republic of Indonesia. [10]. Thus, the regulations regarding biometric data in the PDP Law emphasize the state's responsibility to protect citizens from potential privacy violations resulting from increasingly complex digital data processing.

Furthermore, the PDP Law also regulates basic data protection principles in line with international practice, such as the validity of data collection, purpose limitation, transparency, accuracy, security, and accountability. These principles indicate that biometric data processing cannot be carried out arbitrarily and must be based on the explicit consent of the

data owner. Within the normative legal framework, this consent serves as the basis for the legal legitimacy of the collection and use of biometric data by any party, whether government or private institutions. The absence of consent makes the data processing contrary to the principle of validity and can be classified as a violation of the law that gives rise to criminal and administrative consequences[11].

From a normative regulatory perspective, the Personal Data Protection Law does provide criminal provisions for violations of personal data protection principles. For example, Articles 67 through 73 stipulate criminal sanctions for parties who unlawfully obtain, disclose, or use personal data without authorization. However, in the context of biometric data, the formulation of these offenses remains general and does not explicitly define the specific form of violation or level of legal responsibility for misuse of biometric data. This indicates that although the Personal Data Protection Law normatively includes biometric data as an object of protection, the specific criminal norms for biometric data violations still require strengthening in implementing regulations or more detailed legal revisions.

From a comparative legal perspective, the provisions of the PDP Law can be compared with the General Data Protection Regulation (GDPR) in force in the European Union. The GDPR clearly and comprehensively regulates biometric data as part of the special category of personal data, with a strict prohibition on processing such data except for legitimate and proportionate purposes. The GDPR also contains an accountability principle that requires every data controller *to* be fully responsible for the security, confidentiality, and accuracy of the biometric data they manage. Meanwhile, in the PDP Law, the principle of legal accountability has been mentioned, but it has not been accompanied by a strong oversight and law enforcement mechanism as stipulated in the GDPR, for example the existence of an independent data protection authority with the authority to impose administrative and criminal sanctions [12].

In the context of national law, it is important to emphasize that the PDP Law does not stand alone, but rather interacts with various other regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and the Criminal Code (KUHP). Both of these instruments are relevant in providing additional protection against the criminal aspects of biometric data misuse, for example in cases of illegal access to electronic systems or unauthorized data dissemination. However, based on normative studies, the provisions in the ITE Law and the Criminal Code are still general in nature and do not yet accommodate the specificities of biometric data, which pose a high risk to individual privacy. Therefore, in the context of future legal development, it is necessary to clarify criminal norms that specifically regulate the misuse of biometric data, including the type of violation, the type of perpetrator, and the level of legal responsibility for the violation.

Furthermore, from a conceptual perspective in modern criminal law, biometric data protection must be understood as part of preventive and repressive legal efforts to address cybercrime and digital privacy violations. Strict criminal provisions for perpetrators of biometric data misuse serve not only a retributive function but also an educational and preventive function to raise legal awareness among businesses and public institutions to be more careful in managing the public's biometric data. Thus, criminal law functions as a social engineering tool that encourages the creation of ethical, secure, and human rights-respecting data governance.

Furthermore, this study also found that legal protection for biometric data cannot be separated from the principle of the right to control personal information (right to informational self-determination), namely the right of every individual to regulate and determine the extent to which their personal information may be accessed, stored, and used by others. This principle normatively serves as a moral and philosophical basis for personal data protection in the digital era, where individual control over their personal information is often threatened by technological power and commercial interests. In this context,

strengthening criminal law against biometric data violations is important not only to provide a deterrent effect, but also to emphasize respect for human dignity and freedom as legal subjects who have full rights over their digital identities.

3.2 Discussion

Based on the research findings, it is clear that the legal framework in Indonesia is still developing towards a comprehensive and effective biometric data protection system. In this context, Indonesia has taken an important step with the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) as the normative basis for protecting citizens' personal information. However, although this law recognizes biometric data as part of a specific category of sensitive personal data, its provisions remain general and do not guarantee strong protection against criminal violations. Conceptually, these findings confirm that biometric data, such as digital fingerprints, facial recognition, or retinal scans, constitute irreplaceable personal identities, stemming from each individual's unique biological characteristics[13]. Therefore, breaches of biometric data have far more serious legal and ethical consequences than breaches of ordinary personal data. Once biometric data is leaked, there is no way to replace it, as with passwords or identity cards. This means that biometric data leaks result in permanent losses, not only material but also the loss of individual control over their identity in the digital realm.

When compared to the European Union's General Data Protection Regulation (GDPR), it appears that the regulation has a much stricter criminal and administrative liability structure for personal data protection violations. The GDPR explicitly prohibits the processing of biometric data without a valid legal basis and grants data protection authorities broad authority to impose significant fines, even up to millions of euros, on perpetrators or corporations found to have violated the law [14]. In addition to administrative sanctions, the GDPR also provides for criminal liability for misuse of personal data that results in serious harm to data subjects. Meanwhile, in Indonesia, the Data Protection and Personal Data Protection Law still emphasizes administrative enforcement, such as written warnings, temporary suspension of data processing activities, or deletion of personal data. While the criminal aspects of the Data Protection and Personal Data Protection Law are regulated, they are still general in nature and do not define specific offenses for biometric data violations. This indicates that the national legal protection framework still focuses on the administrative compliance dimension, rather than on substantive protection of human rights, which should be the primary foundation of personal data protection regulations.

A comparison of the PDP Law and the GDPR also reveals differences in legal paradigms. The GDPR positions personal data protection as an integral part of the fundamental rights to privacy and human dignity, while the PDP Law still tends to position data protection within the framework of bureaucratic compliance with information management procedures. Therefore, the development of the national legal system still requires strengthening in terms of internalizing human rights values into the legal regulations for biometric data protection. The principle that every individual has the right to control, regulate, and determine the use of their own data must be the basis for all processes of biometric data collection, processing, and storage in Indonesia[15].

From a criminal law doctrinal perspective, these findings reinforce the urgency of criminal law as the primary instrument in ensuring the protection of biometric data. In modern legal systems, criminal law serves not only as a means of punishment, but also as a tool of social control and crime prevention. The absence of criminal provisions specifically governing the misuse of biometric data demonstrates the need for legislative reform to provide a stronger legal basis for upholding justice. Criminal sanctions should not only be imposed on the direct perpetrators who misuse biometric data, but also on corporations or

institutions that are negligent in maintaining the security of the biometric data they manage. In this regard, the principle of vicarious liability or corporate criminal responsibility needs to be emphasized in the context of biometric data breaches, considering that most data controllers today are technology-based corporate entities. Furthermore, the integration between the PDP Law and the ITE Law needs to be clarified to avoid overlapping regulations and law enforcement. The ITE Law essentially prohibits illegal access, hacking, and unauthorized data dissemination, but it does not specifically regulate the characteristics of biometric data as a legally protected object. Therefore, normative harmonization between the two laws is needed to create a complementary, rather than overlapping, legal system. Within the framework of normative criminal law, this integration is crucial to provide legal certainty and strengthen the effectiveness of sanctions against digital privacy violations.

Theoretically, this research supports the principle of the right to control personal information (right to informational self-determination) which essentially gives every individual the right to control the use, storage, and dissemination of their personal data. This principle originates from the development of privacy law in Europe which places individuals as full owners of their own data. In the Indonesian context, this principle is in line with the mandate of Article 28G paragraph (1) of the 1945 Constitution which guarantees the right of every person to protect their privacy and honor. Thus, any act of processing biometric data without valid consent can be considered a violation of citizens' constitutional rights. Therefore, the law must provide a mechanism for recovery and enforcement of criminal sanctions as a form of protection and prevention against the misuse of biometric data. Without a firm criminal mechanism, the function of law as a means of protection becomes weak, and public trust in digital security systems can decrease significantly.

In conjunction with previous research, these results also confirm that effective personal data protection must be multi-layered, encompassing administrative, civil, and criminal aspects. The administrative layer serves to ensure institutional compliance with regulations, the civil layer provides protection for victims through compensation mechanisms, and the criminal layer serves as the final instrument (*ultimum remedium*) to address violations committed through intent or gross negligence. This multi-layered approach has been implemented in various international jurisdictions, such as the European Union and the United States, where criminal law plays a complementary role to administrative regulations. In this context, the Indonesian legal system needs to adopt a similar approach to address the increasingly complex dynamics of new threats to digital privacy.

Thus, the development of biometric regulations is not solely a technological issue but also involves legal philosophy and legal ethics in balancing public security interests with the protection of individual rights. The law must not simply follow technological developments but must also be able to guide technological progress so that it remains on the side of humanity. Protection of biometric data reflects the state's efforts to safeguard human dignity in an increasingly open digital space.

In closing, this discussion emphasizes that legal reform in Indonesia needs to be directed toward harmonization with international standards, particularly with the principles embodied in the GDPR. The government needs to strengthen criminal norms regarding biometric data breaches, accelerate the establishment of an independent oversight body with law enforcement authority, and expand international cooperation on cross-border data protection. Strengthening regulations, institutions, and public legal awareness will be key to creating a just and effective biometric data protection system. With these steps, digital fingerprint technology and other forms of biometrics can function as trusted security tools, rather than threats to privacy rights. This allows the law to play a role in maintaining the balance between technological progress and the protection of human dignity in the digital age.

4 Conclusion

Based on the research and discussions conducted, it can be concluded that legal protection for biometric data, particularly digital fingerprints in modern security systems, still lacks a solid and comprehensive legal basis in Indonesia. Although Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) recognizes biometric data as a special category of personal data that must be strictly protected, regulations regarding criminal liability for misuse or leakage of biometric data have not been specifically regulated. This creates a gap between legal norms and law enforcement practices in the field.

From a criminal law perspective, research findings indicate that Indonesia still relies on general provisions in the Electronic Information and Transactions Law (UU ITE) and the Criminal Code, which are unable to address the complexity of biometric data-related violations. Meanwhile, at the international level, the European Union's General Data Protection Regulation (GDPR) provides stronger protection standards by emphasizing the principles of accountability, transparency, and imposing strict sanctions for violations of personal data protection. This comparison demonstrates the need for Indonesia to harmonize its laws with global standards to strengthen the protection of individual privacy rights.

Conceptually, the results of this study emphasize the importance of implementing criminal law as an instrument for protecting personal data, particularly in the context of biometric-based digital security. Administrative protection alone is insufficient, given the potential for biometric data breaches to permanently impact an individual's rights and identity. Therefore, integration between the Personal Data Protection Law (PDP), the Electronic Information and Transactions Law (UU ITE), and specific criminal regulations is necessary to ensure effective legal protection and address potential abuses.

This research's primary contribution to the development of legal science lies in its emerging understanding that biometric data protection is an integral part of human rights in the digital age, which must be safeguarded through a combination of administrative, civil, and criminal legal approaches. This research also emphasizes that modern criminal law must adapt to technological developments, so that it can function not only as a repressive tool but also as a preventive one in safeguarding the security of people's personal data.

As a recommendation, this study suggests that the government immediately formulate specific criminal provisions related to the misuse of biometric data, strengthen the capacity of data protection oversight bodies, and enhance international cooperation in cybersecurity oversight and law enforcement. This way, the protection of digital fingerprints and other biometric data can be effectively guaranteed, in line with the principles of justice, legal certainty, and respect for human rights in the digital age.

References

1. R. Pakina and M. Solekhan, "Pengaruh teknologi informasi terhadap hukum privasi dan pengawasan di indonesia: keseimbangan antara keamanan dan hak asasi manusia," *Journal of Scientech Research and Development*, vol. 6, no. 1, 2024.
2. D. Nirwan and A. Sampurna, "Menyelaraskan teknologi dengan perlindungan hak privasi," 2025.
3. A. M. Junaedi, "Urgensi perlindungan data pribadi dalam era digital: analisis undang-undang nomor 27 tahun 2022 tentang perlindungan data pribadi," *Knowledge: Jurnal Inovasi Hasil Penelitian dan Pengembangan*, vol. 5, no. 2, pp. 247–257, Jun. 2025, doi: 10.51878/knowledge.v5i2.5269.

4. R. Rambe and L. Abdurrahman, "Implikasi etika dan hukum dalam penggunaan teknologi pengenalan wajah," *Jurnal Hukum Caraka Justitia*, vol. 4, no. 2, pp. 90–104, Nov. 2024, doi: 10.30588/jhcj.v4i2.1828.
5. E. Muzairoh, S. Suharso, D. Trisna Noviasari, and H. Muhsin Syafingi, "Analisis perlindungan hukum terhadap privasi data pribadi di era digital dalam prespektif hak asasi manusia," *Borobudur Law and Society Journal*, vol. 3, no. 1, pp. 31–36, Jan. 2024, doi: 10.31603/11824.
6. H. S. Disemadi, L. Sudirman, J. Girsang, and A. M. Aninda, "Perlindungan data pribadi di era digital: mengapa kita perlu peduli?," *Sang Sewagati Journal*, 2023.
7. Y. Prayuti, "Dinamika perlindungan hukum konsumen di era digital: analisis hukum terhadap praktik e-commerce dan perlindungan data konsumen di indonesia," *Jurnal Interpretasi Hukum*, vol. 5, pp. 2746–5047, 2024, doi: 10.55637/juinhum.5.1.8482.903-913.
8. R. Tahir, *Metodologi penelitian bidang hukum : Suatu Pendekatan Teori dan Praktik*. Jambi: Sonpedia Publishing Indonesia, 2023.
9. H. Hansen Samin, "Perlindungan hukum terhadap kebocoran data pribadi oleh pengendali data melalui pendekatan hukum progresif," *Jurnal Sains Student Research*, vol. 1, no. 2, pp. 1–15, 2023.
10. U. Mutiara and R. Maulana, "Perlindungan data pribadi sebagai bagian dari hak asasi manusia atas perlindungan diri pribadi," *Indonesian Journal of Law and Policy Studies*, vol. 1, no. 1, p. 42, May 2020.
11. N. P. Rai Yuliartini, I. B. Wyasa Putra, G. M. Wija Atmaja, and D. G. Sudika Mangku, "Legal protection for women and children as victims of human trafficking in indonesia," *Jurnal Hukum Novelty*, vol. 13, no. 1, p. 26, Jul. 2022, doi: 10.26555/novelty.v13i1.a18738.
12. P. H. Simanjuntak, "Perlindungan hukum terhadap data pribadi pada era digital di indonesia: studi undang-undang perlindungan data pribadi dan general data protection regulation (GDPR)," *Jurnal ESENSI HUKUM,* vol. 9, no. 2, p. 61, 2024.
13. N. P. R. Yuliartini, H. Hartana, L. N. Kbarek, and S. Monteiro, "From retribution to restoration: human rights-based legal protection for women victims of sexual violence," *Jurnal Media Hukum*, vol. 32, no. 2, pp. 281–300, 2025, doi: 10.18196/jmh.v32i2.26214.
14. V. Manua, E. V T Senewe, and F. Sesca Wewengkang, "Perbandingan perlindungan hukum terhadap data pribadi dalam undang-undang nomor 27 tahun 2022 negara indonesia dengan federal act on data protection negara switzerland 1," *Jurnal Fakultas Hukum Lex Crimen*, vol. 14, no. 5, 2024.
15. D. G. S. Mangku, N. P. R. Yuliartini, and N. G. A. H. Hadi, "Digital contact tracking as a prevention of covid-19 and the problem of data privacy protection," 2022, p. 020011. doi: 10.1063/5.0104104.