

Criminal Sanctions as a Consequence of Negligence by Data Controllers In Personal Data Breaches

Yanu Romansyah Melvando, Milda Istiqomah, Yuliati Yuliati

Faculty of Law, Brawijaya University, Malang City, Indonesia
yanuromansyah7@student.ub.ac.id

Abstract

This research aims to analyse criminal sanctions due to negligence of personal data controllers that cause data leaks based on Law No. 27 of 2022 on Personal Data Protection (PDP Law). The increasing incidents of personal data leakage in Indonesia indicate weak legal protection related to personal data control. Meanwhile, the PDP Law does not explicitly regulate culpa, resulting in legal uncertainty and potential impunity for perpetrators. This research is important because there is a legal vacuum related to the liability of negligent data controllers and the weak deterrent effect of administrative sanctions that have been applied so far. This research uses a normative juridical method with a statutory approach, examining existing legal norms related to personal data protection, especially the PDP Law. The results show that the PDP Law has not expressly regulated the negligence of data controllers, resulting in a legal vacuum and weakening the enforcement of personal data protection. Therefore, this research offers a new norm formulation that explicitly regulates criminal sanctions for data controller negligence and criminal liability for negligent data controllers. Thus, there is a need for reformulation of criminal norms against negligence to increase legal certainty and protect the rights of personal data owners in Indonesia.

Keywords: *Criminal Sanctions; Legal Vacuum; Personal Data Controller*

1. INTRODUCTION

Personal data protection has become a central issue in modern information governance. In the midst of rapid digitalisation, personal data is no longer just administrative information, but has turned into a vital asset with strategic and economic value. Therefore, the management and protection of personal data cannot be separated from the recognition of the right to privacy as part of human rights. In this context, the protection of personal data is a concrete form of respect for human dignity.¹

Indonesia, as a legal state that upholds human rights as affirmed in the 1945 Constitution of the Republic of Indonesia (UUD 1945), has a constitutional obligation to guarantee the protection of personal data of each of its citizens. Article 28G paragraph (1) of the 1945 Constitution states that everyone has the right to protection of self, family, honour, dignity, and property, including the right to security.² Along with the development of information and communication technology, personal data is increasingly exposed in digital systems connected through the internet. Rapid digital transformation has facilitated administrative, business, and public service activities, but at the same time, increased the risk of leakage, misuse, and hacking of personal

¹ Mery Christian Putri Erlina Maria Christin Sinaga, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0," *Jurnal RechtVinding* 9, no. 2 (2020): 237–56, <https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v9i2.428>.

² Erna Priliasari, "Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman," *Majalah Hukum Nasional* 49, no. 2 (2019): 1–27.

data. Society now lives in a digital ecosystem that records traces of identity, preferences, habits, through various applications and digital platforms.³

This phenomenon shows that technology provides convenience, but also brings real threats to individual data security. In Indonesia, various cases of large data leaks have occurred and become the public spotlight. The Tokopedia case in 2020, which resulted in 91 million users' data being leaked, the BPJS Health data leak in 2021 involving the data of more than 279 million participants, as well as the hacking of IndiHome and Bank Syariah Indonesia services, to the most recent cyberattack on the National Data Centre in 2024, all show the weakness of the data protection system in Indonesia. These incidents not only threaten data security, but also cause material and psychological harm to data subjects, as well as lowering public trust.⁴

This situation emphasises the need for a strong and responsive legal framework. After a long period of relying on general articles in the ITE Law and human rights protection instruments, the government finally responded by enacting Law No. 27 of 2022 on Personal Data Protection (PDP Law). The presence of UU PDP is an important milestone in Indonesia's legal system, because for the first time, a special regulation that comprehensively regulates personal data has been enacted. This law establishes the principles of personal data processing, the obligations of data controllers, the rights of data subjects, and supervisory mechanisms.⁵ However, although UU PDP provides a clearer legal structure, in practice, there are still serious weaknesses, especially in the aspect of criminal liability. The PDP Law places more emphasis on the imposition of administrative sanctions on data controllers who violate their obligations, while the regulation on negligence (*culpa*) has not been explicitly regulated as a basis for criminal liability. This phenomenon raises questions about the effectiveness of UU PDP in protecting the rights of data subjects, especially in cases where data controllers do not implement adequate security standards. This raises doubts as to whether the sanctions stipulated in the PDP Law are effective enough to protect the rights of personal data owners.

Data controller negligence can take many forms, such as failure to implement adequate digital security systems, lack of data encryption, absence of backup and mitigation systems, and slow response to detected security incidents. Even neglecting the obligation to report incidents to authorities and data subjects is a form of negligence that has serious repercussions. In the context of Indonesian criminal law, such acts can theoretically be categorised as *culpa*, which is a form of error that does not contain the element of intent, but still has legal consequences.⁶

³ Juan Matheus and Ariawan Gunadi, "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital : Kajian Perbandingan Dengan KPPU," *Justisi* 10, no. 1 (2023): 20–35, <https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.

⁴ Erna Priliasari, "Legal Protection of Consumer Personal Data in E-Commerce According To Laws Dan Regulations in Indonesia," *Jurnal Rechts Vinding* 12, no. 2 (2023): 261–79, <https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v12i2.1285>.

⁵ Danil Erlangga Mahameru et al., "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia," *Jurnal Esensi Hukum* 5, no. 2 (2023): 115–31, <https://doi.org/https://doi.org/10.35586/jsh.v5i2.240>.

⁶ Hari Sutra Disemadi, "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia," *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99, <https://doi.org/10.25072/jwy.v5i2.460>.

Unfortunately, the current PDP Law places more emphasis on administrative sanctions without providing clear arrangements regarding criminal sanctions for negligent data controllers. The PDP Law does not explicitly regulate criminal liability for negligence (*culpa*), and this is a legal loophole. In the Criminal Code (KUHP), negligence has long been recognised as a basis for criminal liability. This concept should also be adopted in the context of the PDP Law.

To address this problem, reformulation of the PDP Law is an urgent step. The reformulation should include strengthening the criminal provisions for data controller negligence, either in the form of explicit new provisions or through the adoption of relevant general criminal law norms.⁷ This is very reasonable because the absence of criminal sanctions for negligence creates impunity for perpetrators and weakens the protection of victims' rights. Furthermore, this legal vacuum can hamper the role of supervisory authorities and create uncertainty in judicial practice.

Various academic studies that have been conducted also show that the weak application of sanctions against negligence contributes to the prevalence of personal data breaches. In a study by Salsabila (2025), it was found that the implementation of the PDP Law is still weak due to a lack of supervision, low legal literacy, and unpreparedness of digital infrastructure.⁸ Putri's research (2024) also confirms that although the PDP Law has a strong legal basis, in practice, many cases of data leakage are not dealt with firmly.⁹ Meanwhile, research by Edbert (2023) shows weak legal liability for negligence in fintech platforms that caused millions of data leaks.¹⁰ Different from previous studies, this research specifically raises the issue of the absence of criminal norms on negligence as the core of the problem. This research shows that as long as there is no strict regulation on negligence as a form of criminal liability, data controllers will tend to neglect their responsibilities. Since administrative sanctions such as fines are often considered light and not proportional to the potential profits from data management, data controllers tend to have no incentive to implement maximum security systems.

2. METHOD

This research is a normative legal research (legal research) that aims to examine and analyse the norms contained in positive law, specifically related to the concept of negligence of personal data controllers that causes data leakage. The approach method used is a statutory approach, which involves an in-depth review of all relevant laws and regulations, including Law No. 27 of 2022 on Personal Data Protection and other relevant regulations. A conceptual approach to

⁷ Moh Hamzah Hisbulloh, "Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi," *Jurnal Hukum* 37, no. 2 (2021): 119–33, <https://doi.org/10.26532/jh.v37i2.16272>.

⁸ Sidi Ahyar Wiraguna Shafa Salsabila, "Pertanggungjawaban Hukum Atas Pelanggaran Data Pribadi Dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia," *Konsensus : Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi* 2, no. 2 (2025): 145–57, <https://doi.org/https://doi.org/10.62383/konsensus.v2i2.736>.

⁹ Ni Made Puspasutari Ujjanti Ni Made Dwi Gayatri Putri, Ni Luh Made Mahendrawati, "Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Jurnal Preferensi Hukum* 5, no. 2 (2024): 240–45, <https://doi.org/https://doi.org/10.22225/jph.5.2.2024.240-245> Perlindungan.

¹⁰ Felicia Edbert and Moody Rizqy Syailendra Putra, "Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi Pada Perusahaan Pengelola Jasa Keuangan Berbasis IT," *Unes Law Review* 6, no. 2 (2023): 5966–77, <https://doi.org/https://doi.org/10.31933/unesrev.v6i1>.

examine the concept of culpa/negligence in criminal law. The legal materials used are divided into two categories: primary legal materials consisting of relevant laws and regulations, and secondary legal materials, which include legal literature such as books, scientific journals, articles, and expert opinions. The technique of collecting legal materials is done through literature study, while the technique of analysing legal materials applies the method of grammatical interpretation and syllogism analysis.

3. RESULTS AND DISCUSSION

3.1 Legal Implications Related to the Legal Lack of the Concept of Negligence in Personal Data Protection in the Personal Data Controller

Law No. 27 of 2022 on Personal Data Protection (PDP Law), which became effective on 17 October 2024, is a national legal instrument that establishes the principles of personal data protection as part of fundamental human rights.¹¹ Under these provisions, personal data controllers have a legal obligation to ensure the security of the data they manage, including by implementing technical and administrative measures to prevent unauthorised access, disclosure, alteration, or destruction of personal data.¹² However, the PDP Law does not explicitly regulate the concept of negligence (culpa) as a basis for criminal liability in the context of personal data protection offences, especially those related to the operation of electronic systems. The absence of legal norms regulating the objective standard of negligence creates legal uncertainty, as there are no clear guidelines on when an act or omission can be qualified as a criminal offence.¹³ As a result, data controllers or electronic system organisers who fail to protect personal data, either due to unintentional actions or weak security systems, are difficult to hold criminally liable with certainty.

As for culpa in criminal law is a form of error that can lead to criminal liability even without malicious intent. In general, culpa is divided into two forms, namely: (1) negligence due to lack of care, where the perpetrator fails to fulfil the standard of care that should be taken; and (2) negligence with awareness of the possible consequences, namely when the perpetrator knows the risks that may arise from his actions but still does it. In both forms, the main element of culpa is the non-fulfilment of the duty of care that could have prevented the consequences prohibited by the law.¹⁴ In criminal law doctrine, the essential element of negligence (culpa) is the awareness or knowledge of the perpetrator of the possibility of the consequences prohibited by law. The

¹¹ M. Syamsudin Desti Fitri Anggranei, Ikama Dewi Setia Triana, "Perlindungan Hukum Bagi Pengguna Akun Shopee Paylater Dari Tindak Pidana Peretasan Data," *Cakrawala Hukum* 27, no. 1 (2025): 1–9, <https://doi.org/https://doi.org/10.51921/chk.Secj0j76>.

¹² Kadek Ariesta et al., "Analisis Hukum Terhadap Pencurian Data Administrasi Kependudukan Dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *Jurnal Analogi Hukum* 6, no. 3 (2024): 330–35, <https://doi.org/https://doi.org/10.22225/jah.6.3.2024.330-335>.

¹³ Hezkiel Bram Setiawan and Fatma Ulfatun Najicha, "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data," *Jurnal Kewarganegaraan* 6, no. 1 (2022): 976–82, <https://doi.org/https://doi.org/10.31316/jk.v6i1.2657>.

¹⁴ Leden Marpaung, *Asas-Teori-Praktik Hukum Pidana* (Jakarta: Sinar Grafika, 2005).

perpetrator is considered negligent when he or she should have foreseen the consequences but failed to take reasonable precautions.¹⁵

From the explanation of the culpa theory in criminal law, it becomes very relevant when analysed in the context of personal data protection, especially against personal data controllers as legal subjects who are directly responsible for the security, integrity, and confidentiality of individual data. In criminal law doctrine, fault (*schuld*) is an essential element in determining criminal liability, and one of the universally recognised forms of fault is negligence. Culpa is defined as the failure of the perpetrator to perform the legal obligation to act carefully, which, if done properly, could prevent the occurrence of consequences prohibited by law.

In this context, Law No. 27 of 2022 on Personal Data Protection (PDP Law) has explicitly stipulated that personal data controllers have a legal responsibility to ensure that the data managed is protected from leakage, misuse, manipulation, or illegal access. Such responsibilities contain proactive and preventive dimensions, which, if ignored, provide a strong basis for assessing negligence. Negligence in the form of non-implementation of adequate data security systems, inaction in responding to leakage incidents, or disregard for minimum standards of data protection are clear indications that the controller has failed to fulfil the legal obligations inherent in its role and function.

In this framework, the culpa element as a form of criminal guilt has been fulfilled. If this kind of negligence is not subject to criminal liability, then the state has essentially created a space for impunity, which is a condition in which the perpetrator is free from legal sanctions even though it clearly violates the rights of others. Impunity is not only contrary to the principles of criminal justice but also undermines the preventive and protective functions of criminal law itself. Criminal law is not only present as a tool of retaliation, but as a mechanism of prevention and protection of the fundamental rights of citizens, including the right to privacy and control over personal data. Therefore, the negligence of personal data controllers cannot be viewed solely as an administrative offence.

In a digital age characterised by a high risk of data exploitation, such negligence should be positioned as a potential form of crime against human rights, especially when it results in real harm to individuals, whether in the form of identity abuse, financial fraud, discrimination or loss of personal dignity.¹⁶ By referring to the culpa theory, criminal law provides a strong normative and rational basis to ensnare negligent data controllers with criminal sanctions, of course, while taking into account the principles of proportionality and *ultimum remedium*. Ignoring this negligence from the criminal realm will only weaken the legal protection system for victims and furthermore, ignore the constitutional mandate that places the right to privacy as an integral part of human rights that must be guaranteed, protected, and fulfilled by the state.

¹⁵ Aruan Sakijo, *Hukum Pidana Dasar Aturan Umum Hukum Pidana Kodifikasi* (Jakarta: Ghalia Indonesia, 1990).

¹⁶ Albert Lodewyk Sentosa Siahaan, "Urgency of Personal Data Protection on Marketplace Platforms Against Technological Advances," *Majalah Hukum Nasional* 52, no. 2 (2022): 209–23, <https://doi.org/10.33331/mhn.v52i2.169>.

In the practice of implementing personal data protection, data controllers, both from the private and government sectors, have a primary obligation to ensure the security of the data they manage.¹⁷ However, in the absence of juridically formulated parameters of negligence in Law No. 27 of 2022 on Personal Data Protection, the assessment of fault is subjective and inconsistent. The absence of clear standards regarding negligence creates a legal vacuum that hinders effective law enforcement. Under these conditions, when a personal data protection breach occurs, law enforcement officials find it difficult to determine whether the data controller's actions qualify as a criminal offence, especially if the breach occurs not due to *mens rea*, but due to ignorance or the absence of adequate data protection procedures. As a result, offences that do occur often cannot be responded to with fair and proportionate law enforcement.

In the analysis of legal syllogism, it can be formulated as follows: The major premise states that an action can only be punished if it fulfils the elements of an unlawful act, the existence of fault (either intentional or negligent), and has been expressly regulated in the legislation. However, the minor premise shows that Law Number 27 Year 2022 on Personal Data Protection does not explicitly regulate negligence and its objective indicators. As a result, the actions of negligent data controllers cannot be definitively punished under the PDP Law. This syllogistic analysis reveals a void between acts and legal norms, which in criminal law is a serious problem. This violates the principle of *nullum crimen sine lege certa*, which requires that legal norms must be formulated clearly and unequivocally. Without definite provisions, the law loses its main function in providing certainty, opening up room for interpretation that is detrimental to the public interest..

In the basic principles of criminal law and the protection of human rights, victims have the main position that must be protected.¹⁸ However, in the context of Law No. 27 of 2022 on Personal Data Protection, the victim's position is weakened due to the unclear arrangements regarding criminal and civil liability for the negligence of data controllers. When a personal data leak occurs due to negligence, the victim as a data subject is in a legally unfavourable situation. The PDP Law does not provide legal certainty for victims to claim criminal or civil liability from negligent data controllers. The absence of explicit provisions regarding the standard of negligence and the mechanism for the restoration of victims' rights creates a detrimental legal vacuum, as victims lose access to effective legal channels to claim compensation or fair legal protection. This is contrary to the principles of justice and protection of human rights.

Victims of personal data breaches not only suffer material losses, such as identity theft, financial fraud, or misuse of personal accounts, but also experience immaterial losses in the form of

¹⁷ Thiara Dewi Purnama and Abdurrakhman Alhakim, "Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia," *E-Journal Komunitas Yustisia* 4, no. 3 (2021): 273–83, <https://doi.org/https://doi.org/10.23887/jatayu.v4i3.44370>.

¹⁸ Hanifan Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)," *Jurnal Yuridis* 7, no. 1 (2020): 105–19, <https://doi.org/10.35814/selisik.v6i1.1699>.

psychological distress, discomfort, and loss of security.¹⁹ However, until now, there has been no concrete and easily accessible mechanism for compensation or remediation for the community. The absence of a remediation mechanism reflects the state's failure to fulfil its responsibility to protect the rights of victims, especially in realising the principle of restorative justice. The principle of restorative justice emphasises restoring the rights and dignity of victims through fair compensation.

As an illustration, in the case of the alleged leak of voter data managed by the General Election Commission (KPU), although the personal data of the general public was exposed, no compensation or recovery scheme was available to the affected data owners. This condition reflects the weak personal data protection system in Indonesia, which fails to put victims at the centre of legal protection. The lack of clarity on legal liability due to the absence of negligence norms in the PDP Law not only creates legal uncertainty but also results in the lack of effective legal protection. The state, through the law, has an obligation to provide effective legal instruments, ensuring that every citizen has access to claim compensation or a remedy when their right to personal data is violated. Without this clarity, justice for victims cannot be realised.

Thus, the lack of norms on negligence in the PDP Law creates an impunity gap for personal data controllers who fail to implement minimum security measures. When a data leak occurs, data controllers only face light administrative sanctions, without adequate criminal liability.²⁰ As a result, victims lose access to effective legal mechanisms to demand justice and restoration of rights. This situation not only harms victims but also erodes public trust in the legal system and weakens the state's role as a protector of citizens' basic rights.

In addition, the result of the absence of negligence provisions in the Personal Data Protection Law has a direct impact on the effectiveness of supervision conducted by Data Protection Authorities (DPOs) in Indonesia. Without a normative definition of negligence, DPOs face difficulties in sanctioning or issuing corrective policies against data controllers who are found to be negligent. The absence of clear benchmarks causes the role of DPOs to be weak, limited to ceremonial functions without effective enforcement capabilities. From a constitutional law perspective, this situation contradicts Article 28G paragraph (1) of the 1945 Constitution, which guarantees everyone's right to protection of self, family, honour, dignity, and property. Personal data protection is an extension of the constitutionally guaranteed right to privacy. Therefore, the state has a constitutional obligation to ensure the security of its citizens' personal data through adequate regulation. As a corrective step, the state must immediately draft implementing regulations that explicitly regulate the concept of negligence in personal data management. In addition, technical guidelines from the OPD are needed that can be used as an objective measure

¹⁹ Rista Maharani and Andria Luhur Prakoso, "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital," *Jurnal USM Law Review* 7, no. 1 (2024): 333–47, <https://doi.org/10.26623/julr.v7i1.8705>.

²⁰ Abdul Hadi and Bima Guntara, "Pembaharuan Hukum Nasional Dalam Upaya Perlindungan Data Pribadi Di Era Distrupsi Kecerdasan Buatan (Artificial Intelligence)," *Jurnal Hukum Mimbar Justitia* 8, no. 1 (2022): 233–53, <https://doi.org/10.35194/jhmj.v8i1.2426>.

in assessing negligence. Another alternative is to revise the PDP Law to accommodate the development of cyber threats and strengthen personal data protection comprehensively.

3.2 Formulation of Criminal Sanctions Arrangements Against Negligence of Personal Data Controllers Resulting in Data Leaks in the Future

Indeed, the law is a concrete manifestation of the state's responsibility in maintaining and protecting the rights of each individual, so that the community can enjoy all the rights that have been guaranteed by law in a fair and proportional manner.²¹ Law Number 27 Year 2022 on Personal Data Protection is an important legal foundation in recognising the right to personal data as part of the privacy rights of every Indonesian citizen. The passing of the PDP Law confirms the government's commitment to protecting citizens' personal data, especially in the digital era that is full of challenges and risks of data leakage.²²

However, a closer analysis of the PDP Law reveals significant weaknesses in the aspect of criminal law enforcement against data controllers who are negligent or negligent in protecting personal data.²³ One of the main weaknesses lies in Article 46 paragraphs (1) and (3) of the PDP Law, which only requires data controllers to provide notification to data owners and the general public in the event of a data protection failure. This notification is informative as a form of transparency, but is not followed by a strict criminal law enforcement mechanism. This causes the notification obligation to only function as an administrative acknowledgement that a data leak has occurred, without any criminal law liability for negligent parties.²⁴

Article 57 paragraph (2) of UU PDP also shows another weakness in law enforcement, by only stipulating administrative sanctions in the form of written warnings, temporary suspension of personal data processing activities, data deletion, and/or administrative fines. These sanctions are corrective and administrative in nature, not penal or repressive. Consequently, this arrangement does not provide an adequate deterrent effect for violators, as there is no threat of strict criminal sanctions for negligent data controllers.²⁵ As a state of law that upholds the principle of legal certainty and the protection of human rights, Indonesia cannot rely solely on administrative regulations. Proactive efforts are needed to strengthen criminal law instruments to protect

²¹ Satjipto Raharjo, *Ilmu Hukum* (Bandung: PT. Citra Aditya Bakti, 2000). 53

²² Khetrina Maria Angnesia and Sidi Ahyar Wiraguna, "Analisis Pertanggungjawaban Hukum Pemerintah Dalam Menegakkan Pelindungan Data Pribadi Di Era Digital," *Perspektif Administrasi Publik Dan Hukum* 2, no. 2 (2025): 176–87, <https://doi.org/https://doi.org/10.62383/perspektif.v2i2.249>.

²³ Fatnan Setyo Hariwibowo, "Analisis Regulasi Telemedicine: Perlindungan Hukum Dan Implikasi Bagi Tenaga Kesehatan," in *Masyarakat Hukum Kesehatan Indonesia*, 2024, 149–58.

²⁴ Amiludin Fikriatul Nabila, Imran Bukhari Razief, "Evaluasi Terhadap Kebocoran Data Dalam Sistem Perbankan Di Indonesia (Studi Kasus Ransomware Pada Bank Syariah Indonesia)," *Al-Qisth Law Review* 7, no. 2 (2024): 295–310, <https://doi.org/https://doi.org/10.24853/al-qisth.7.2.295-310>.

²⁵ Bram Freedrik Sangojoyo, Aurelius Kevin, and David Brilian Sunlaydi, "Urgensi Pembaharuan Hukum Mengenai Perlindungan Data Pribadi E-Commerce Di Indonesia," *Kosmik Hukum* 22, no. 1 (2022): 27–39, <https://doi.org/10.30595/kosmik hukum.v22i1.12154>.

personal data.²⁶ Data controllers who are proven to be negligent and cause data leaks must be subject to commensurate criminal sanctions, to ensure a deterrent effect and justice for the community. Corrective and administrative sanctions in Indonesia's personal data protection legal system have not been fully able to provide a deterrent effect and have made the prevention aspect of legal violations ineffective. This shows a fundamental weakness in the data protection law enforcement system, especially when violations are committed by data controllers who should bear significant legal responsibility.²⁷

In contrast, when compared to the legal approach in other countries such as Italy, there are significant differences in terms of commitment to the protection of the right to personal data. Regulations do not stop at the administrative realm, but have progressed to the realm of criminal law, especially for serious offenders who ignore data protection standards. This shows an awareness that personal data is part of human rights that require maximum protection, including through the threat of harsh penalties. As an illustration, Italy, through the Codice in materia di protezione dei dati personali (Code for the Protection of Personal Data), establishes strict criminal norms. In Section 33, it states that anyone who fails to fulfil the minimum obligations of personal data protection is liable to imprisonment of up to two years or a fine of between €10,000 and €50,000. This provision shows that the Italian legal system places data protection offences in a serious and strategic position in safeguarding the constitutional rights of its citizens.²⁸

Thus, the legal vacuum of criminal regulation against forms of negligence (*culpa*) in personal data control is a legal loophole that can weaken the data protection system in Indonesia. In the absence of clear criminal provisions related to negligence, data controllers can escape legal liability, even if proven negligent.²⁹ Therefore, it is necessary to formulate new criminal norms in the PDP Law that explicitly regulate criminal liability for negligent data controllers. This formulation should include a clear definition of negligence, minimum standards of data protection, as well as an effective enforcement mechanism.

In order to improve the legal protection of personal data in Indonesia, the formulation of Law No. 27 of 2022 on Personal Data Protection (UU PDP) needs to consider the addition of norms that explicitly regulate forms of negligence by data controllers that result in leakage or misuse of

²⁶ Dewi Sulistianingsih et al., "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)," *Masalah-Masalah Hukum* 52, no. 1 (2023): 97–106, <https://doi.org/10.14710/mmh.52.1.2023.97-106>.

²⁷ Nadiah Tsamara, "Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara," *Jurnal Suara Hukum* 3, no. 1 (2021): 53–85, <https://doi.org/10.26740/jsh.v3n1.p53-84>.

²⁸ Barda Nawawi, *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan* (Bandung: PT Citra Aditya Bakti, 2005).

²⁹ Arie Tri Hartantyo Fransiscus Xaverius Watkat, Muhammad Toha Ingratubun, Muhammad Hafiz Ingsaputro, "Pertanggungjawaban Pidana Pengendali Data Pribadi Terhadap Kebocoran Data Pribadi," *Jurnal Hukum Ius Publicum* 5, no. 2 (2024): 177–98, <https://doi.org/10.55551/jip.v5i2.175>.

personal data.³⁰ This is important given the rapid development of information technology, which increases the risk of personal data leakage, whether caused by intentional acts or negligence.

Table 1. Table of Legal Provisions Formulation Related to Negligence
of Personal Data Controllers

Aspect/Formulation	Substance of Provision
Formulation of General Provisions	<i>“Negligence is an act of carelessness, recklessness, or omission of a measure that should have been taken by a controller of personal data in the performance of his or her duties, which results in the unlawful access, retrieval, alteration, dissemination, or loss of personal data.”</i>
Formulation of Criminal Offenses	<i>“Any controller of personal data who, through his/her negligence, causes leakage, misuse, or unauthorized access to personal data, resulting in harm to the data subject, shall be punished with imprisonment of up to 5 (five) years and/or a maximum fine of Rp2,000,000,000.00.”</i>
Formulation of Criminal Liability	<i>“Criminal liability for criminal acts of negligence as referred to in Article ... may be imposed on: Criminal liability for criminal negligence, as referred to in Article ... may be imposed on: a. Individuals who act as data controllers b. A legal entity or corporation, in the event that the negligence is the result of an inadequate policy, omission, or internal system.”</i>
Formulation of Criminal Sanctions and Punishment	<i>a. In addition to the main punishment, the perpetrator may be sentenced to additional punishment in the form of: 1) Revocation of data management license 2) Announcement of the judge's decision 3) Compensation to the victim 4) etraining in the field of data security b. If the perpetrator is a corporation, the punishment may be imposed on the management and/or on the corporation itself in the form of a fine twice the maximum provision.”</i>

Through this formulation, data controllers are not only administratively responsible but can also be held criminally liable if there is negligence that has a broad impact on society. This responsibility is very important, especially in the digital era, where the personal data of each individual becomes very valuable. This arrangement can clearly provide legal certainty and protection and does not create impunity for perpetrators and weaken the protection of victims'

³⁰ Indra Indra, Trihoni Nalesti Dewi, and Daniel Budi Wibowo, “Perlindungan Kerahasiaan Data Pasien vs Kewajiban Membuka Akses Rekam Medis Elektronik,” *Soepra Jurnal Hukum Kesehatan* 10, no. 1 (2024): 97–117, <https://doi.org/10.24167/sjhk.v10i1.11542>.

rights. When there are clear legal consequences for negligent data controllers, this will encourage them to be more responsible in data management. This formulation reflects the government's commitment to provide a full and balanced guarantee of legal protection for all citizens, so it is hoped that every data controller will be more careful in managing the information they have. In a broader context, personal data protection is also closely related to human rights. Every individual has the right to privacy and protection of their personal data. When governments and data controllers take steps to protect these rights, they are not only fulfilling a legal obligation, but also demonstrating a commitment to human values.

4. CONCLUSION

The absence of norms regulating criminal liability for negligence (*culpa*) in Law Number 27 Year 2022 on Personal Data Protection has created a legal vacuum. This void not only creates legal uncertainty but also opens room for impunity for data controllers who are negligent in protecting personal data, and directly weakens the protection of the fundamental rights of data subjects. In the absence of explicit provisions that make negligence a form of criminal offense, law enforcement officials face serious obstacles in applying the principle of legality (*nullum crimen sine lege certa*). As a result, negligent acts of data controllers tend to only be subject to administrative sanctions that are corrective, light, and do not have a deterrent effect. This research offers a conceptual contribution in the form of a proposal for the formulation of criminal norms that specifically regulate negligence as a basis for legal liability in the PDP Law. The government needs to develop and implement regulations that set minimum standards for data security and objective indicators of negligence, which will serve as a strong foundation for law enforcement until a comprehensive revision of the PDP Law is formed. This effort is important to ensure justice for victims, strengthen the role of oversight, and prevent the state from neglecting its constitutional obligation to protect citizens' privacy rights.

REFERENCES

- Angnesia, Khetrina Maria, and Sidi Ahyar Wiraguna. "Analisis Pertanggungjawaban Hukum Pemerintah Dalam Menegakkan Pelindungan Data Pribadi Di Era Digital." *Perspektif Administrasi Publik Dan Hukum* 2, no. 2 (2025): 176–87. <https://doi.org/https://doi.org/10.62383/perspektif.v2i2.249>.
- Ariesta, Kadek, Dwi Anggara, I Made Minggu, Widyantara I Wayan, and Kartika Jaya. "Analisis Hukum Terhadap Pencurian Data Administrasi Kependudukan Dalam Perspektif Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Jurnal Analogi Hukum* 6, no. 3 (2024): 330–35. <https://doi.org/https://doi.org/10.22225/jah.6.3.2024.330-335>.
- Desti Fitri Anggranei, Ikama Dewi Setia Triana, M. Syamsudin. "Perlindungan Hukum Bagi Pengguna Akun Shopee Paylater Dari Tindak Pidana Peretasan Data." *Cakrawala Hukum* 27, no. 1 (2025): 1–9. <https://doi.org/https://doi.org/10.51921/chk.5ecj0j76>.
- Disemadi, Hari Sutra. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177–99. <https://doi.org/10.25072/jwy.v5i2.460>.

- Edbert, Felicia, and Moody Rizqy Syailendra Putra. "Pertanggungjawaban Hukum Terhadap Kebocoran Data Pribadi Pada Perusahaan Pengelola Jasa Keuangan Berbasis IT." *Unes Law Review* 6, no. 2 (2023): 5966–77. <https://doi.org/https://doi.org/10.31933/unesrev.v6i1>.
- Erlina Maria Christin Sinaga, Mery Christian Putri. "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0." *Jurnal RechtVinding* 9, no. 2 (2020): 237–56. <https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v9i2.428>.
- Fikriatul Nabila, Imran Bukhari Razief, Amiludin. "Evaluasi Terhadap Kebocoran Data Dalam Sistem Perbankan Di Indonesia (Studi Kasus Ransomware Pada Bank Syariah Indonesia)." *Al-Qisth Law Review* 7, no. 2 (2024): 295–310. <https://doi.org/https://doi.org/10.24853/al-qisth.7.2.295-310>.
- Fransiscus Xaverius Watkat, Muhammad Toha Ingratubun, Muhammad Hafiz Ingsaputro, Arie Tri Hartantyo. "Pertanggungjawaban Pidana Pengendali Data Pribadi Terhadap Kebocoran Data Pribadi." *Jurnal Hukum Ius Publicum* 5, no. 2 (2024): 177–98. <https://doi.org/10.55551/jip.v5i2.175>.
- Hadi, Abdul, and Bima Guntara. "Pembaharuan Hukum Nasional Dalam Upaya Perlindungan Data Pribadi Di Era Distrupsi Kecerdasan Buatan (Artificial Intelligence)." *Jurnal Hukum Mimbar Justitia* 8, no. 1 (2022): 233–53. <https://doi.org/10.35194/jhmv.v8i1.2426>.
- Hariwibowo, Fatnan Setyo. "Analisis Regulasi Telemedicine: Perlindungan Hukum Dan Implikasi Bagi Tenaga Kesehatan." In *Masyarakat Hukum Kesehatan Indonesia*, 149–58, 2024.
- Hisbulloh, Moh Hamzah. "Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi." *Jurnal Hukum* 37, no. 2 (2021): 119–33. <https://doi.org/10.26532/jh.v37i2.16272>.
- Indra, Indra, Trihoni Nalesti Dewi, and Daniel Budi Wibowo. "Perlindungan Kerahasiaan Data Pasien vs Kewajiban Membuka Akses Rekam Medis Elektronik." *Soepra Jurnal Hukum Kesehatan* 10, no. 1 (2024): 97–117. <https://doi.org/10.24167/sjhc.v10i1.11542>.
- Mahameru, Danil Erlangga, Aisyah Nurhalizah, Ahmad Wildan, Mochamad Haikal, and Mohamad Haikal Rahmadia. "Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas Di Indonesia." *Jurnal Esesnsi Hukum* 5, no. 2 (2023): 115–31. <https://doi.org/https://doi.org/10.35586/jsh.v5i2.240>.
- Maharani, Rista, and Andria Luhur Prakoso. "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital." *Jurnal USM Law Review* 7, no. 1 (2024): 333–47. <https://doi.org/10.26623/julr.v7i1.8705>.
- Marpaung, Leden. *Asas-Teori-Praktik Hukum Pidana*. Jakarta: Sinar Grafika, 2005.
- Matheus, Juan, and Ariawan Gunadi. "Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU." *Justisi* 10, no. 1 (2023): 20–35. <https://doi.org/10.33506/jurnaljustisi.v10i1.2757>.
- Nawawi, Barda. *Pembaharuan Hukum Pidana Dalam Perspektif Kajian Perbandingan*. Bandung: PT Citra Aditya Bakti, 2005.
- Ni Made Dwi Gayatri Putri, Ni Luh Made Mahendrawati, Ni Made Puspasutari Ujianti. "Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022." *Jurnal Preferensi Hukum* 5, no. 2 (2024): 240–45. <https://doi.org/https://doi.org/10.22225/jph.5.2.2024.240-245> Perlindungan.
- Niffari, Hanifan. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)." *Jurnal Yuridis* 7, no. 1 (2020): 105–19.

- <https://doi.org/10.35814/selisik.v6i1.1699>.
- Priiasari, Erna. "Legal Protection of Consumer Personal Data in E-Commerce According To Laws Dan Regulations in Indonesia." *Jurnal Rechts Vinding* 12, no. 2 (2023): 261–79. <https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v12i2.1285>.
- . "Pentingnya Perlindungan Data Pribadi Dalam Transaksi Pinjaman." *Majalah Hukum Nasional* 49, no. 2 (2019): 1–27.
- Purnama, Thiara Dewi, and Abdurrahman Alhakim. "Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia." *E-Journal Komunitas Yustisia* 4, no. 3 (2021): 273–83. <https://doi.org/https://doi.org/10.23887/jatayu.v4i3.44370>.
- Raharjo, Satjipto. *Ilmu Hukum*. Bandung: PT. Citra Aditya Bakti, 2000.
- Sakijo, Aruan. *Hukum Pidana Dasar Aturan Umum Hukum Pidana Kodifikasi*. Jakarta: Ghalia Indonesia, 1990.
- Sangojoyo, Bram Freedrik, Aurelius Kevin, and David Brilian Sunlaydi. "Urgensi Pembaharuan Hukum Mengenai Perlindungan Data Pribadi E-Commerce Di Indonesia." *Kosmik Hukum* 22, no. 1 (2022): 27–39. <https://doi.org/10.30595/kosmikhukum.v22i1.12154>.
- Setiawan, Hezkiel Bram, and Fatma Ulfatun Najjicha. "Perlindungan Data Pribadi Warga Negara Indonesia Terkait Dengan Kebocoran Data." *Jurnal Kewarganegaraan* 6, no. 1 (2022): 976–82. <https://doi.org/https://doi.org/10.31316/jk.v6i1.2657>.
- Shafa Salsabila, Sidi Ahyar Wiraguna. "Pertanggungjawaban Hukum Atas Pelanggaran Data Pribadi Dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia." *Konsensus : Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi* 2, no. 2 (2025): 145–57. <https://doi.org/https://doi.org/10.62383/konsensus.v2i2.736>.
- Siahaan, Albert Lodewyk Sentosa. "Urgency of Personal Data Protection on Marketplace Platforms Against Technological Advances." *Majalah Hukum Nasional* 52, no. 2 (2022): 209–23. <https://doi.org/10.33331/mhn.v52i2.169>.
- Sulistianingsih, Dewi, Miftakhul Ihwan, Andry Setiawan, and Muchammad Shidqon Prabowo. "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)." *Masalah-Masalah Hukum* 52, no. 1 (2023): 97–106. <https://doi.org/10.14710/mmh.52.1.2023.97-106>.
- Tsamara, Nadiyah. "Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara." *Jurnal Suara Hukum* 3, no. 1 (2021): 53–85. <https://doi.org/10.26740/jsh.v3n1.p53-84>.