The Pangkalpinang District Court Decision: An Analysis of the Criminal Offense of Collecting Personal Data Without Permission

Editho Berilphizaldi[1], Husni Thamrin[2]
[1,2]Universitas Pertiba, Pangkal Pinang, Indonesia
Email: edithoberilphizaldi@gmail.com

Abstract

This study aims to analyze the application of Article 67 of Law No. 27 of 2022 on Personal Data Protection in cases of unauthorized collection and use of personal data for activating prepaid cards, as outlined in the decision of the Pangkalpinang District Court. The research identifies how the panel of judges assessed the defendant's actions in collecting personal data without consent and whether such actions violated the constitutional rights of the data subjects. Additionally, this study examines the roles and responsibilities of corporations and individuas involved in this case, and the legal consequences, both material and immaterial, for the personal data subjects. The findings of the study indicate that the criminal act of collecting personal data without permission can cause harm to individuas, highlighting the need for strict law enforcement to protect privacy rights in the digital age.

Keywords: *Personal Data Protection, Unauthorized Data Collection, Prepaid Card Activation.*

A. INTRODUCTION

The rapid development of information and communication technology has fundamentally transformed social and economic activities, particularly in the administration and utilization of personal data in digital environments (Acquisti, Taylor, & Wagman, 2016). Personal data, including identifiers, financial information, and digital footprints, has increasingly become a valuable economic resource for both individuals and commercial entities operating in data-driven markets (Zuboff, 2019). The extensive collection and processing of personal data enable efficiency in digital transactions, yet simultaneously expose individuals to significant risks when such data is gathered without lawful authorization or valid consent (Solove, 2006). Unauthorized accumulation of personal data constitutes a critical legal issue because it facilitates privacy violations, identity misuse, and potential economic harm to data subjects (European Union, 2016). In response to these global challenges, Indonesia enacted Law Number 27 of 2022 on Personal Data Protection, which establishes explicit legal standards governing personal data collection, processing, and safeguarding within national jurisdiction (Republic of Indonesia, 2022). This legislation mandates that personal data processing must be based on lawful grounds and valid consent from data subjects, reflecting internationally recognized data protection principles (European Union, 2016). The collection or processing of personal data without authorization not only breaches statutory obligations but also infringes fundamental privacy rights recognized as part of human rights protections in democratic legal systems (Solove,

2006). Unauthorized data collection may generate material losses such as financial fraud risks, as well as immaterial harms including psychological insecurity and erosion of trust in digital governance systems (Acquisti et al., 2016). These conditions demonstrate that personal data protection laws serve a dual function of regulating digital economic activity while ensuring the preservation of individual dignity and informational self-determination in contemporary digital society (Zuboff, 2019).

Despite the existence of personal data protection regulations, the unauthorized accumulation and misuse of personal data continues to occur across various sectors, particularly in telecommunications industries where large-scale identity data processing is routinely conducted (Greenleaf, 2020). Empirical evidence demonstrates that SIM card registration mechanisms in multiple jurisdictions have been exploited to collect identity information without valid consent, thereby exposing individuals to identity misuse and illicit data trading practices (Donovan & Martin, 2014). In Indonesia, the unauthorized collection of Population Identification Numbers (NIK) and Family Card Numbers (KK) for prepaid card activation reflects systemic vulnerabilities in national personal data governance frameworks (Greenleaf, 2020). The registration and activation of telecommunication starter cards using unlawfully obtained personal data increases the risk of future misuse by unauthorized parties and heightens exposure to identity-based cybercrime (Donovan & Martin, 2014). Such practices involve corporate employees and third-party data suppliers, raising complex questions regarding individual criminal liability and corporate responsibility in personal data misuse cases (Greenleaf, 2020). The Pangkalpinang District Court's conviction of the defendant under Article 67 paragraph (1) and Article 65 paragraph (1) of Indonesia's Personal Data Protection Law illustrates the criminalization of unauthorized data collection that may cause harm to data subjects (Republic of Indonesia, 2022). Comparative legal scholarship confirms that criminal sanctions for unlawful data processing function as essential enforcement instruments to deter persistent non-compliance in emerging data protection regimes (Greenleaf, 2020). These developments raise critical inquiries regarding the effectiveness of Indonesia's PDP Law implementation and the capacity of law enforcement institutions to prosecute personal data violations in technologically mediated environments (Republic of Indonesia, 2022). Judicial enforcement in such cases serves as an important benchmark for evaluating national readiness in safeguarding privacy rights and regulating corporate conduct in digital markets (Donovan & Martin, 2014).

One of the central legal issues arising in this case concerns corporate responsibility in supervising and bearing liability for unlawful actions committed by employees or agents acting on behalf of the company. Even though Smartfren operates an official SIM card registration system, inadequate monitoring of registration procedures and personal data usage demonstrates potential negligence in corporate data governance obligations (Wachter, 2018). Corporations are legally required to ensure that personal data used for service activation is obtained from data subjects who have provided lawful and informed consent, in accordance with recognized data protection principles (European Union, 2016). In this case, personal data was unlawfully acquired from third parties and subsequently used to achieve corporate sales targets, raising questions regarding both

criminal and civil corporate liability for failure to safeguard personal data (Wachter, 2018). At the same time, the rights of data subjects whose identities were misused constitute an equally significant legal concern because unauthorized identity usage may generate material losses such as fraud or identity theft risks. In addition, immaterial losses arise through violations of privacy rights and diminished feelings of personal security, which are recognized as protected legal interests within modern data protection regimes (European Union, 2016). These circumstances illustrate that personal data misuse not only implicates individual offenders but also demands corporate accountability for insufficient supervision and protection mechanisms. Therefore, this research seeks to examine how Indonesian law regulates personal data protection and how the imposition of legal sanctions in this case may generate a deterrent effect to prevent the recurrence of similar violations (Republic of Indonesia, 2022).

The acquisition of personal data without valid consent in this context constitutes a criminal offense under Indonesia's Personal Data Protection Law and the Electronic Information and Transactions Law, both of which prohibit unlawful data collection and processing activities. Contemporary data protection doctrine establishes that lawful consent is a fundamental prerequisite for personal data processing and that violations of this principle directly infringe legally protected privacy rights (Kuner, Bygrave, & Docksey, 2020). Unauthorized acquisition of personal data therefore contravenes binding legal standards and exposes perpetrators to criminal liability under modern data protection regimes. A comprehensive examination of the application of Article 67 of Indonesia's Personal Data Protection Law is essential to assess how criminal provisions are enforced against unlawful data collection practices. This includes analyzing the legal reasoning adopted by judicial panels in interpreting statutory elements of personal data crimes and determining offender liability. Comparative studies confirm that criminal sanctions play a decisive role in strengthening compliance and deterrence in data protection enforcement frameworks (De Hert & Papakonstantinou, 2016). Evaluating judicial application of Article 67 provides a critical benchmark for measuring the effectiveness of Indonesia's emerging personal data protection enforcement system (Republic of Indonesia, 2022).

This research further investigates the roles of involved parties, including corporations and individuals, in the unauthorized collection of personal data, particularly in determining how responsibility is distributed between individual offenders and corporate entities within modern privacy governance systems (Bennett & Raab, 2020). A central legal question concerns whether corporations can be held accountable for illicit actions committed by employees or representatives in acquiring personal data, given that international privacy governance frameworks emphasize corporate obligations to implement effective internal oversight and compliance mechanisms (OECD, 2013). Another critical issue is how the Indonesian criminal justice system ensures protection of personal data subjects through enforcement of laws regulating lawful and accurate data usage, especially in emerging data protection regimes. The imposition of criminal sanctions on perpetrators of personal data offenses is widely recognized as an essential deterrent mechanism to prevent recurring violations

and to strengthen institutional trust in digital governance environments (UNCTAD, 2021). Examining judicial enforcement and sanctioning practices in this case provides an important assessment of Indonesia's readiness to uphold personal data protection and corporate accountability in the digital era.

This research is significant not only in an academic context but also in identifying existing legal gaps in personal data protection and in formulating recommendations to enhance law enforcement capacity in addressing privacy rights violations in digital environments. Contemporary legal scholarship recognizes that rapid technological advancement often outpaces regulatory adaptation, creating enforcement voids in criminal law related to digital privacy protection (Brownsword, 2008). In emerging data-driven societies, strengthening legal frameworks and enforcement mechanisms is essential to ensure that privacy rights remain effectively protected against evolving technological risks (Gellert, 2018). This research aims to address challenges arising from technological development and to contribute to the evolution of Indonesian criminal law in the specific context of personal data protection. By examining judicial practice and regulatory effectiveness, this study provides insight into how national legal systems can respond to privacy-related crimes in increasingly digitized social and economic structures (Hildebrandt, 2015). The findings of this research are expected to support the development of more adaptive legal policies and stronger institutional readiness in safeguarding personal data rights in Indonesia's digital transformation era.

B. METHOD

The author employs a normative research method in the writing, which includes a statute approach and a case approach. The objective of this research is to examine the applicability of the law in instances of personal data exploitation, with a particular emphasis on Article 67 of the Personal Data Protection Law. This research employs secondary data sources, such as legislation, court decisions, and legal literature, to investigate the offense of collecting personal data without permission and the preservation of personal data. The researcher conducted library research to acquire legal documents, including legislation and court rulings that were pertinent to the research topic, as part of the data collection method. To generate a comprehension of the application of law in the case and its legal implications, the analysis method employed is qualitative analysis with interpretative techniques on the content of legislation and court decisions, as well as comparing them with existing legal literature.

C. RESULTS AND DISCUSSION

1. The Application of Article 67 of the Personal Data Protection Law on the Crime of Collecting Personal Data Without Permission in the Case of SIM Card Activation Tried at the Pangkalpinang District Court

The rapid advancement of information and communication technology has intensified the urgency of enforcing laws that prohibit the collection of personal data without valid consent, as digital systems increasingly enable large-scale data processing across multiple sectors. This technological development creates significant opportunities for personal data misuse, thereby threatening individual privacy and legal certainty in data governance. In Indonesia, Law Number 27 of 2022 on Personal Data Protection represents a critical regulatory response to these challenges by explicitly prohibiting the collection, processing, and utilization of personal data without the consent of the data subject. Article 67 of this legislation specifically criminalizes unauthorized personal data collection, making its application central to cases involving privacy violations. The case examined in this research concerns an employee of the Smartfren Gallery who intentionally collected Population Identification Numbers (NIK) and Family Card Numbers (KK) without authorization to activate Smartfren starter cards. The personal data was used without the knowledge or consent of the rightful owners and was obtained through an electronic system-based application sourced from a third party. Such conduct demonstrates a deliberate misuse of identity information for both personal and business objectives under corporate sales targets. Consequently, this case is directly linked to the enforcement of Article 67 of the PDP Law, which mandates explicit consent as a fundamental requirement for lawful personal data collection. The judicial application of this provision reflects Indonesia's broader effort to strengthen legal protection of privacy rights in the digital era and to ensure the integrity of its emerging personal data protection system (Buttarelli, 2018).

Article 67 of Indonesia's Personal Data Protection Law explicitly stipulates that individuals who intentionally and unlawfully collect or process personal data belonging to others for personal or third-party benefit may be subjected to criminal liability. In the present case, this provision was clearly violated because the data used for SIM card registration belonged to another individual and was obtained without the data owner's consent. Beyond breaching statutory data protection obligations, such conduct also constitutes a direct violation of the fundamental right to privacy, which is legally safeguarded under modern constitutional and human rights frameworks. Individuals who acquire and process personal data without authorization are therefore subject to criminal sanctions, including imprisonment and fines, as judicially interpreted in the application of Article 67. The enforcement of Article 67 in this case carries significant legal implications for strengthening personal data protection in Indonesia's developing digital governance landscape. Unauthorized utilization of personal data, as demonstrated in this instance, exposes structural weaknesses in the national data protection system that require regulatory and institutional reinforcement. To prevent future misuse and to ensure a deterrent effect, stringent and consistent law enforcement against personal data violations is essential. The application of Article 67 to the defendant who intentionally collected and used another person's identity data to activate a Smartfren starter card marks an

important milestone in advancing judicial protection of individual privacy rights in Indonesia (Tzanou, 2013).

A proper application of Article 67 of the Personal Data Protection Law requires a clear understanding of the constituent elements of the offense, particularly intent (dolus) and illegality. Intent constitutes a primary element because criminal liability arises when the perpetrator knowingly and deliberately collects or uses personal data without lawful authorization. In this case, the defendant intentionally collected personal data without consent, despite claiming that the act was performed under instructions from a superior. The existence of an order from a superior does not eliminate criminal responsibility when the offender is aware that the act violates the rights of the data subject. The imposition of criminal sanctions under Article 67 of the PDP Law is therefore strongly predicated on the proven intention to use another individual's personal data without consent. Illegality forms the second essential element, as the acquisition and use of personal data without lawful grounds directly contradicts statutory data protection provisions. The defendant's actions infringe the privacy rights of the data owner, which must be safeguarded under fundamental personal data protection principles. Using Population Identification Numbers (NIK) and Family Card Numbers (KK) of another person without consent constitutes an illicit act because no legal justification exists for personal data utilization without valid authorization. These elements demonstrate that unauthorized personal data collection fulfills the requirements of a criminal offense under modern data protection doctrine, where intent and unlawfulness jointly establish individual criminal accountability (Fuster, 2014).

The application of Article 67 of the Personal Data Protection Law encompasses elements that may cause damage to personal data subjects, including both material losses and immaterial harms arising from privacy violations. Material losses may occur through unauthorized use of personal data, while immaterial losses emerge from infringements of the data owner's privacy, dignity, and sense of personal security. In this case, the data subject's identity was misappropriated without knowledge or consent, and even in the absence of proven direct financial loss, such unauthorized use still constitutes a legally recognizable immaterial harm. Misuse of personal data further carries the potential for long-term injury, including identity theft or fraudulent activities, thereby extending the risk exposure of victims beyond the initial violation. The application of Article 67 in this context also underscores the corporate obligation to supervise the handling of personal data by employees or affiliated representatives. Although the defendant acted under superior instructions, the company remains accountable for ensuring that customer personal data is lawfully obtained and processed in compliance with applicable regulations. As a telecommunications service provider, Smartfren bears a duty to implement effective oversight mechanisms to prevent abuse of personal data within its operational systems. Failure to establish stringent monitoring frameworks reflects deficiencies in corporate data governance that contribute to privacy infringements. These circumstances illustrate that personal data protection law not only addresses

individual wrongdoing but also demands corporate accountability in safeguarding informational integrity and contextual privacy in digital environments (Nissenbaum, 2010).

The significance of rigorous law enforcement in addressing privacy and personal data violations is clearly reflected in the application of Article 67 of Indonesia's Personal Data Protection Law in this case. The criminal sanctions imposed on the defendant serve not only to punish individual wrongdoing but also to establish a preventive mechanism against the recurrence of similar personal data violations. Consistent and effective enforcement of personal data protection law is essential to build public trust in Indonesia's data governance system and to ensure that individual privacy rights are adequately safeguarded within the existing legal framework. The implementation of Article 67 in this case further demonstrates Indonesia's commitment to strengthening personal data protection, particularly in sectors that intensively process consumer data, such as telecommunications services. In the context of rapid technological advancement and the increasing volume of electronic transactions, it is crucial that personal data protection mechanisms operate effectively and that privacy violations receive proportionate legal sanctions. This research not only clarifies how current legal provisions are applied in judicial practice but also identifies regulatory and institutional aspects requiring further development within Indonesia's personal data protection system. The application of Article 67 in cases of unauthorized personal data collection highlights the growing role of criminal law in safeguarding fundamental privacy rights in the digital era and in reinforcing the integrity of national data protection enforcement (Lynskey, 2015).

2. Legal Impact on Corporations and Individuas Involved in the Criminal Act of Collecting Personal Data Without Permission, and the Losses Suffered by Personal Data Subjects Based on the Decision of the Pangkalpinang District Court

An employee of the Smartfren Gallery is currently being prosecuted at the Pangkalpinang District Court for unlawfully acquiring personal data to activate prepaid starter cards. In this case, the defendant collected and used Population Identification Numbers (NIK) and Family Card Numbers (KK) belonging to other individuals to register and activate Smartfren SIM cards without authorization. This situation represents a critical focal point for assessing legal implications not only for the individual offender but also for the corporation benefiting from the commercial use of unlawfully obtained personal data. Indonesian criminal law recognizes that such conduct constitutes a violation of Article 67 paragraph (1) and Article 65 paragraph (1) of Law Number 27 of 2022 on Personal Data Protection, which prohibits the collection and processing of personal data without the data subject's consent. The unauthorized acquisition of personal data therefore forms the primary criminal offense in this case. The subsequent use of the data for commercial purposes, namely SIM card activation to meet corporate sales objectives, demonstrates how personal data misuse can generate mutual benefit for both individuals and corporate entities.

Under Article 67, those involved in unauthorized personal data collection are subject to criminal sanctions, including imprisonment and fines. This illicit act reveals that Indonesia's personal data protection system remains vulnerable to abuse by both individual actors and corporate representatives. Such vulnerabilities highlight the necessity of stronger compliance enforcement mechanisms and corporate accountability frameworks to prevent repeated exploitation of personal data in commercial environments (González Fuster & Gellert, 2012).

The legal implications for the corporation involved, Smartfren, must be considered alongside the liability of the individual offender, particularly regarding corporate oversight of customer personal data usage. Although the unlawful act was committed by employees influenced by corporate sales targets, the company remains accountable for ensuring that personal data collected through electronic systems is processed lawfully and protected from misuse. As a telecommunications service provider, Smartfren holds operational control over the SIM card registration and activation system, thereby imposing a legal duty to implement adequate supervision and data protection mechanisms. Under principles of vicarious liability, a corporation may be held responsible for wrongful acts committed by employees acting within the scope of their employment and for corporate benefit. This responsibility becomes especially relevant where insufficient monitoring systems enable unauthorized personal data collection to occur within corporate operations. Consequently, corporate negligence in supervising the collection and use of personal data may result in legal accountability in addition to the criminal liability borne by individual perpetrators. These conditions demonstrate that effective personal data protection requires not only individual compliance but also institutional governance structures capable of preventing internal misuse of personal data. Therefore, corporate accountability forms a crucial element in strengthening Indonesia's personal data protection enforcement system and in ensuring that commercial objectives do not override legal obligations to safeguard privacy rights (Polinsky & Shavell, 1993).

If a corporation is found to have failed in establishing an adequate monitoring system to safeguard customer personal data, the resulting legal consequences may include administrative or civil sanctions such as financial penalties or revocation of operational licenses. Corporate accountability in implementing personal data protection policies in compliance with statutory regulations is therefore essential to prevent employees or third parties from misusing personal data for personal or commercial purposes. The application of law in this case illustrates broader implications concerning the responsibility of companies to develop rigorous privacy governance frameworks and internal control mechanisms capable of preventing negligent handling of personal data. Corporations that fail to implement effective monitoring systems for personal data processing expose themselves not only to legal liability but also to reputational damage and loss of public trust among consumers and regulators. This case thus serves as a critical institutional lesson demonstrating that personal data protection is not merely a matter of individual compliance but also of corporate governance integrity. Strengthening internal oversight structures and

compliance cultures becomes indispensable in reducing organizational vulnerability to data misuse. This instance underscores that effective personal data protection enforcement requires corporations to prioritize privacy safeguards as a core element of responsible digital business operations (Ayres & Braithwaite, 1992).

This case not only produces legal consequences for individuals and corporations involved, but also generates tangible and intangible losses for personal data subjects whose identities were misused to activate prepaid starter cards. Material losses arise from the potential misuse of personal identity for subsequent criminal activities such as fraud or identity theft, even where no immediate financial harm can be proven. Unauthorized use of personal data therefore continues to pose long-term economic risks to data subjects, particularly when identity information remains beyond the control of its rightful owner. Immaterial losses are closely connected to violations of privacy rights, which include an individual's entitlement to control personal information as part of fundamental constitutional protection. The use of personal data without consent constitutes an infringement of legally protected rights under Indonesia's constitutional framework and statutory personal data protection law. Such violations may generate psychological insecurity and anxiety among data subjects, as their personal information is exploited for purposes unrelated to their intentions. Although immaterial in nature, these harms are significant because they weaken public trust in institutional systems designed to safeguard privacy and undermine individual confidence in participating in digital environments. This situation demonstrates that personal data misuse extends beyond economic harm and directly affects human dignity and autonomy in the information society. Recognition of both material and immaterial losses reinforces the necessity of robust legal protection for personal data subjects within modern data protection regimes (Floridi, 2016).

Losses suffered by personal data subjects also include the continuing risk of future misuse of their personal information after unauthorized data utilization has occurred. Once personal data is used without consent for prepaid card activation, such information may circulate beyond the control of the data owner and be exploited in subsequent crimes, including fraud or illegal account creation. Even where no direct evidence of further criminal activity is identified in the present case, the persistent risk of identity misuse remains a critical factor in assessing long-term harm arising from personal data violations. The legal consequences imposed on individuals and corporations in this case contribute to the development of stronger legal awareness and educational efforts regarding personal data protection obligations. Strict law enforcement is expected to serve as a societal lesson for both the public and business sectors concerning the importance of safeguarding personal data and respecting privacy rights. Beyond its deterrent effect on perpetrators, this case stimulates broader institutional discussion on improving personal data protection regulation and strengthening implementation mechanisms in Indonesia. This dynamic reflects the broader reality that personal data misuse generates extended societal risks, as

uncontrolled data dissemination increases exposure to secondary cyber-enabled crimes and undermines trust in digital systems (Mayer-Schönberger & Cukier, 2013).

The legal implications of the crime of collecting personal data without permission in this case are substantial for the individuals directly involved, the responsible company, and the affected personal data subjects, as indicated by this analysis. In the event of personal data misuse, corporations and individuals must be held accountable for their actions through the imposition of criminal and administrative sanctions. Individuals who are subjected to the misuse of their personal data incur both material and immaterial losses. This emphasizes the significance of stringent policies and rigorous law enforcement in Indonesia's protection of personal data.

D. CONCLUSION

Two significant conclusions can be drawn from the analysis presented above. Initially, the Pangkalpinang District Court's application of Article 67 of the Personal Data Protection Law in the context of unauthorized personal data collection demonstrates that this offense satisfies the criteria of intent, unlawfulness, and potential damage to the personal data subject. Individual privacy rights have been violated and the personal data protection provisions outlined in Law No. 27 of 2022 have been contravened by the offense of unauthorized personal data collection, which in this instance involves the use of another individual's NIK and KK data to activated a new SIM card. The court's decision to impose penal sanctions on the perpetrator also emphasizes the significance of rigorous law enforcement in Indonesia's efforts to safeguard personal data.

Secondly, the legal repercussions of this crime are substantial, both in terms of criminal and civil penalties, for both corporations and individuals. In this instance, Smartfren, a corporation, may be held accountable for negligence in the supervision of the use of personal data by its employees or third parties. This can lead to administrative or civil sanctions. Conversely, the losses suffered by the subjects of personal data are not only material but also immaterial. These losses include the potential for identity misuse that could cause damage to the victims in the future, as well as violations of privacy rights. Consequently, it is crucial for organizations to guarantee that their personal data management systems are in compliance with current regulations and have effective supervision mechanisms.

REFERENCES

1. Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54*(2), 442–492.
2. Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press.

3. Bennett, C. J., & Raab, C. D. (2020). *The governance of privacy: Policy instruments in global perspective*. MIT Press.
4. Brownsword, R. (2008). *Rights, regulation and the technological revolution*. Oxford University Press.
5. Buttarelli, G. (2018). The EU GDPR as a clarion call for a new global digital ethics. *International Data Privacy Law, 8*(2), 77–80. https://doi.org/10.1093/idpl/ipy004
6. De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals?. *Computer Law & Security Review, 32*(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006
7. Donovan, K., & Martin, A. K. (2014). The rise of African SIM registration: A legal and policy analysis. *Journal of Information Policy, 4*, 42–65.
8. European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj
9. Floridi, L. (2016). On human dignity as a foundation for the right to privacy. *Philosophy & Technology, 29*(4), 307–312.
10. Fuster, G. G. (2014). The emergence of personal data protection as a fundamental right of the EU. *International Data Privacy Law, 4*(4), 260–269. https://doi.org/10.1093/idpl/ipu018
11. Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review, 34*(2), 279–288. https://doi.org/10.1016/j.clsr.2017.12.003
12. González Fuster, G., & Gellert, R. (2012). The fundamental right of data protection in the European Union: In search of an uncharted right. *International Review of Law, Computers & Technology, 26*(1), 73–82.
13. Greenleaf, G. (2020). Global data privacy laws 2020: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report, 163*, 1–6.
14. Hildebrandt, M. (2015). *Smart technologies and the end(s) of law*. Edward Elgar Publishing.
15. Kuner, C., Bygrave, L. A., & Docksey, C. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.
16. Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.
17. Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.
18. Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.
19. OECD. (2013). *The OECD privacy framework*. OECD Publishing.
20. Polinsky, A. M., & Shavell, S. (1993). Should employees be subject to fines and imprisonment given the existence of corporate liability?. *International Review of Law and Economics, 13*(3), 239–257.

21. Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560.
22. Tzanou, M. (2013). Data protection as a fundamental right next to privacy? *International Data Privacy Law, 3*(2), 88–99. https://doi.org/10.1093/idpl/ipt002
23. UNCTAD. (2021). *Data protection and privacy legislation worldwide: Implications for digital trade and development*. United Nations Conference on Trade and Development.
24. Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (*Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection*).
25. Wachter, S. (2018). Corporate liability for data protection violations: A comparative analysis of GDPR enforcement mechanisms. *Computer Law & Security Review, 34*(4), 733–742. https://doi.org/10.1016/j.clsr.2018.02.002
26. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.