PERSPEKTIF
Kajian Masalah Hukum dan Pembangunan
P-ISSN 1410-3648 E-ISSN 2406-7385
Volume 31 Nomor 3 (2026): Edisi September
**Sekretariat:**
Fakultas Hukum Universitas Wijaya Kusuma Surabaya
Jl. Dukuh Kupang XXV No. 54 Surabaya
*e-mail*: perspektif_hukum@yahoo.com
**Diterbitkan oleh:**
Lembaga Penelitian dan Pengabdian Masyarakat (LPPM)
Universitas Wijaya Kusuma Surabaya

# Legal Protection of Personal Data in The Use of Cyber Security and Artificial Intelligence Against Banking Systems

**Reynaldo**
Faculty of Information Technology, Pradita University, Tangerang, Banten, Indonesia
*corresponding author e-mail*: aldotjung@gmail.com

*Submitted: February 10th, 2026* | *Accepted: September 2nd, 2026* | *Published: September 9th, 2026*

***ABSTRACT***
*Indonesia has brought convenience to financial transactions, but it has also increased the risk of customer personal data leaks, particularly because banks now rely on cyber security systems and artificial intelligence in Know Your Customer procedures, biometric authentication, and credit scoring. This phenomenon raises concerns about the weak protection of privacy rights and the security of customers' financial data. This study aims to analyse the forms of legal protection provided to customers against personal data leaks and the criminal law policy governing cybercrime committed through artificial intelligence. This research is normative legal research employing statutory, conceptual, and comparative approaches, with legal materials collected through a literature study of legislation, legal doctrine, and reported cases of data breaches in the national banking sector. The results show that although a national legal framework has been established through Law Number 27 of 2022 concerning Personal Data Protection, the Banking Law, and the regulations of the Financial Services Authority and Bank Indonesia, its implementation is still obstructed by weak law enforcement, the absence of technical benchmarks for data protection by design and for explainable artificial intelligence, unprepared digital banking infrastructure, and low customer awareness. Criminal law policy has likewise not accommodated artificial intelligence as a means of committing crime, which creates a legal vacuum. This study therefore recommends a rebuttable presumption of negligence for banks, explainable artificial intelligence compliance benchmarks, and a lex specialis governing artificial intelligence-based cybercrime.*
***Keywords:*** *artificial intelligence; personal data; digital banking; cyber security; bank liability.*

## INTRODUCTION

The development of science and technology has penetrated all areas of human life, such as education, health, and the economy, particularly the banking sector. The banking world, will continue to face challenges in providing good and beneficial services to all consumers. This is to ensure easy, fast, and efficient service, which can be used as a benchmark for a country's progress. A country can be measured by its level of economic growth. Likewise, banking services are crucial as a benchmark for economic development and progress within a country.[1]

Banks are financial institutions that play a role in providing payment services and enforcing monetary policy. They are also organizations that the public can trust due to their reliance on their performance. Banks have objectives as stipulated in Law No. 7 of 1992 concerning Banking (abbreviated to as the Banking Law). The development of science and technology, coupled with the need for adjustments to banking itself, is crucial given the crucial role of banks as financial service institutions, collecting funds and ultimately distributing them to the public.[2]

[1] Nur Kholis, "Perbankan Dalam Era Baru Digital," *Jurnal Economicus* 12, no. 1 (2018): 80–88.

[2] Rizki Akbar Maulana and Rani Apriani, "Perlindungan Yuridis Terhadap Data Pribadi Nasabah Dalam Penggunaan Elektronik Banking (e-Banking)," *Jurnal Hukum De'rechtsstaat* 7, no. 2 (2021): 163–72.

According to the explanation above, a technology is needed that can assist in carrying out an activity, especially those that occur in the banking sector. This technology is Cyber Security and artificial intelligence. Artificial Intelligence (hereinafter referred to as AI) is an example of intelligence created by humans which is built in the form of a programming machine in such a way that AI can think like humans, AI supporting components require data to form a knowledge base and so on.

Artificial intelligence (AI) technology is becoming a legal topic today, as it can become a legal subject and produce objects protected by law. Artificial intelligence, an example of a product of the development of the Fourth Industrial Revolution, should be considered a specific protected object under national regulations. However, in fact, the existing laws and regulations have not yet included any mention of Artificial Intelligence innovation in the applicable laws of the Banking Law, Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number I1 of 2008 concerning Electronic Information and Transactions, Regulation of the Financial Services Authority of the Republic of Indonesia Number 9 of 2025 concerning Dematerialization of Equity Securities (hereinafter referred to as Law 9/2025) and Management of Unclaimed Assets in the Capital Market (hereinafter referred to as OJK Regulation 9/2025) and Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as Law 27/2022).

Indonesia itself only has legal regulations regarding the protection of personal data which still have a special nature towards a situation or event which in other words only provides regulations for certain fields spread across various laws and regulations, such as Law Number 36 of 2009 concerning Health which in certain articles regulates the confidentiality of patient medical records, Law Number 10 of 1998 concerning Banking which in its regulations contains regulations for the protection of customer personal data related to storage and deposits, Law 36 of 1999 concerning Telecommunications which contains regulations related to the protection of personal data, namely the obligation for telecommunications providers to provide confidentiality of information belonging to violators of telecommunications services. In general, as stated in Law Number 39 of 1999 concerning Human Rights in Article 29 paragraph (1) which provides recognition of the right of every person to protect themselves, their families, honor, dignity and property rights. The protection in question also relates to the context of personal data information, family, honor, dignity and property rights, the protection in question also relates to the context of information or personal data. Law 23 of 2006 concerning Population Administration, Law 11 of 2009 concerning Information and Electronic Transactions as amended by Law 19 of 2016, and Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions.

In short, it can be seen that the role of Cyber Security and AI can provide very rapid and specific assistance in all aspects. In banking itself, the use of cyber security and AI can be implemented in several aspects such as saving banking capital and making it easier for consumers to access data, thus increasing activity. In addition, AI itself can be applied to Chatbots for bank customer service departments, where the use of chatbots also simplifies services within the bank and provides faster time savings compared to direct service. In short, Chatbot is one form of AI creation that is applied in the form of a human-computer interaction model. The development of AI allows a Chatbot to have the ability to communicate not much different from humans. Chatbots can be personal assistants that can provide various information services according to technological developments, especially information related to the customer themselves, which can be kept confidential with the help of Cyber Security.

The development of technology, while having positive impacts, is also inextricably linked to negative impacts. Examples include the potential misuse or leakage of personal data from banking customers. It is undeniable that cybersecurity and AI have engaged in unethical actions, which will undoubtedly harm all parties, including bank customers and the banks themselves. Although cybersecurity and AI are fundamentally regulated and incorporate several formulas and data that can eventually mimic human intelligence, this does not make AI a legal entity. This is especially true

if personal data leaks are caused by cybersecurity and AI through e-banking and other features that are inextricably linked to customer personal data. For example, in one case of data leak, documents captured in the screenshot included photos of an electronic ID card (KTP), account number, tax identification number (NPWP), birth certificate, and medical record of a BRI Life customer.[3]

Violations of the use of personal data often occur in Indonesia, the exchange of personal data is carried out through a sharing system, namely the exchange of information about customer personal data among fellow card centers, disclosure of information including transactions related to credit card holders to third parties or sold between banks themselves or through third parties, namely individuals or legal entities collecting data and selling customer personal data. In Indonesia, violations of personal data usage are common. In banking practices, personal data is exchanged through a sharing system, which involves exchanging customer personal data among card centers, disclosing information, including transactions related to credit card holders, to third parties, or trading it within banks or through third parties, including individuals and data collection companies, as well as the sale of customer personal data.

A data-trading syndicate for online gambling was uncovered when police raided a hotel in the Juanda area of Sidoarjo Regency. The raid was prompted by reports from members of the public who observed suspicious activity. The perpetrators' modus operandi involved seeking clients by inviting them to open bank accounts, complete with mobile banking services. These accounts were then transferred to Cambodia and Vietnam for online gambling transactions. In exchange, those who opened accounts were rewarded with millions of rupiah. The turnover in one account reached Rp 5 billion.[4]

Cases of data theft and even personal data misuse often occur in Indonesia, such as the case of misuse by falsifying personal data that occurred in the TunaiCPT case as reported by BBC Indonesia on May 9, 2021, a source named Arief complained that he was suddenly transferred Rp. 800,000 to his account, then received a threat sent via email to immediately return the money and interest within seven days for a total of Rp. 1,200,000, even though he had never applied for a loan to the company. Then Arief contacted the email address listed on the TunaiCPT Application page on the Play Store to clarify, but the TunaiCPT service provider insisted that he had to pay off the debt which was his obligation. In the end, Arief paid the debt and interest totaling Rp. 1,200,000 million, but the problems he faced did not stop there. In March 2021, the same thing happened again, Arief received a bill from the same email address, but the company had changed its name to Tunai Gesit. The company is not registered with the Financial Services Authority (OJK) aka illegal. Furthermore, on the Tunai Gesit application web display that can be accessed through the Play Store, many people complained about having experienced the same thing as Arief. However, currently the Tunai Gesit online loan service is no longer found on the Play Store.[5]

Essentially, the most important factor, data security, is equally important for business owners and consumers. Whether in personal or business settings, data privacy and security are paramount. High risks can arise if information system data security plays a crucial role in ensuring data authenticity cannot be easily compromised by unauthorized parties. Despite extensive protection, hackers can still obtain the original data, which is now the root cause.

This aligns with the principle of consumer protection, which is a key aspect of regulations and policies in the financial services sector. Data breaches or cyberattacks can result in significant costs to address personal data protection failures. A 2020 report published by IBM Security found that losses caused by data breaches reached US$3.86 million globally, while the cost of these breaches

[3] Mediana and Benediktus Krisna Yogatama, "Data 2 Juta Nasabah Bocor, BRI Life Telusuri Jejak Digital," kompas.id, 2021, https://www.kompas.id/artikel/data-2-juta-nasabah-bocor-bri-life-telusuri-jejak-digital.

[4] Anggie Meidyana, "Sindikat Jual Beli Data Pribadi Untuk Judol Terungkap, Korban Diiming-Imingi Jutaan Rupiah," metrotvnews.com, 2025, https://www.metrotvnews.com/play/kBVC9Qdn-sindikat-jual-beli-data-pribadi-untuk-judol-terungkap-korban-diiming-imingi-jutaan-rupiah.

[5] Pijar Anugerah, "Pinjaman Online: 'Bagaimana Saya Menjadi Korban Penyalahgunaan Data Pribadi,'" BBC News Indonesia, 2021, https://www.bbc.com/indonesia/majalah-57046585.

reached US$291,870. The financial services sector is among the top three sectors, along with healthcare and energy, experiencing losses due to data breaches, amounting to US$5.85 million.[6] Referring to Article 2 of Financial Services Authority Regulation Number 11/POJK.03/2022, the implementation of risk management in the use of information technology includes: active supervision; adequacy of policies, standards, and procedures for the use of information technology; adequacy of processes for identifying, measuring, monitoring, and controlling risks in the use of information technology; and an internal control system for the use of information technology. Based on the scope of risk management in the use of information technology, Digital Banks are required to have policies, standards, and procedures to ensure the effective implementation of information security with the aim of maintaining the confidentiality, integrity, and availability of managed information. An information system integrated with carefully managed technology can function as an effort to protect data, cybersecurity, and consumer protection.

Absence of Specific AI Governance Standards for the Financial Sector: Current banking cyber resilience regulations typically prescribe routine Vulnerability Assessment and Penetration Testing (VAPT) alongside conventional IT risk management frameworks. However, they fail to account for specialized AI-driven cyberattacks.

Research Gap: There is a lack of technical regulatory benchmarks mandating "Data Protection by Design and by Default" specifically tailored to the integration of AI models in banking Know Your Customer (KYC) and biometric systems. The absence of a clear compliance standard creates legal uncertainty when distinguishing between actionable civil torts (unlawful acts) and ordinary operational or business risks.

Leaks of consumer personal data cause significant losses for consumers, and the leaked data is vulnerable to misuse by irresponsible individuals to commit crimes. Therefore, the government is required to play a role in protecting the public's personal data so that personal data used in e-commerce services does not cause harm to the public. It is important to note that there must be specific regulations governing the protection of personal data so that the data is used according to its intended purpose and is not misused. As a country based on the rule of law, Indonesia guarantees the protection of human rights in the country's constitution. Referring to the increasing use of information and communication technology in various individual activities, the potential for personal data breaches increases. This is the background to the potential for personal data breaches in Indonesia.

This study offers novelty by reconstructing the doctrine of banking liability through a rebuttable presumption of negligence, while formulating legal compliance benchmarks for Explainable AI (XAI) integration to overcome the evidentiary barriers posed by 'Black Box' algorithms in protecting customer biometric data against AI-driven cyber threats.

Based on the description above, this article formulates two legal problems, namely: first, how are bank efforts towards customers and the strengthening of digital banking regulations carried out through cyber security and artificial intelligence; and second, how is the legal policy in combating crime committed by using artificial intelligence and cyber security. This study is aimed at analysing both problems in order to formulate a model of legal protection for customers' personal data that is preventive, technically measurable, and capable of allocating liability when a data breach occurs.

## RESEARCH METHOD

This research is normative legal research. Peter Mahmud Marzuki stated, "Legal research is a process of discovering legal rules, legal principles, and legal doctrines to address the legal issues faced." Research using normative law does not utilize data obtained from fieldwork. Instead, analysis is conducted using a specific approach. The type of approach in this research uses a normative juridical approach, namely research based on existing legal rules by observing the reality that occurs. Legal research with a normative doctrinal approach is essentially an activity that will examine the internal aspects (to solve problems within) of positive law. This research

[6] IBM Security, *Cost of a Data Breach Report 2020* (New York, 2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost of a Data Breach Report 2020.pdf.

method uses a method of studying legislation, a conceptual approach, and a comparative approach related to the problem being studied.[7]

## DISCUSSION

### Bank Efforts Towards Customers and Strengthening Banking Regulations Digitally Using Cyber Security and Artificial Intelligence

The legal challenges facing the banking industry in the digital era have a significant impact on business activities and customer trust. To address these challenges, banking regulations must keep pace with technological developments and provide adequate protection for all parties involved in the banking industry. One key challenge is customer data security and privacy. In an increasingly connected digital era, cybersecurity risks are increasing. Data breaches and hacking attacks can cause significant financial losses for both customers and financial institutions. Therefore, banking regulations need to ensure that financial institutions implement adequate security measures, including data encryption, strong authentication, and protection against cyberattacks.[8]

Legal protection efforts for customers against personal data leaks are carried out through two main approaches: preventive and repressive. The preventive approach includes establishing regulations, supervision, and increasing legal awareness among financial industry players. The repressive approach, on the other hand, involves imposing administrative, civil, and criminal sanctions on parties who violate personal data protection provisions. As part of the preventive approach, the Financial Services Authority (OJK) and Bank Indonesia have issued various regulations related to data security and information technology. For example, OJK Circular Letter Number 29/SEOJK.03/2022 regulates the implementation of risk management in the use of information technology by commercial banks. This regulation requires every bank to have a cybersecurity framework that can detect and handle data leak incidents quickly and accurately.[9]

Legal protection for customers in digital banking transactions is a legal consequence of the growing use of information technology in the financial services sector, which is accompanied by increased potential legal risks. In digital-based transactions, customers are vulnerable to misuse of personal data, electronic system failures, and unclear legal liability in the event of losses. Adnyani emphasized that consumer protection in digital transactions must be directed at ensuring system security, information transparency, and the availability of effective complaint mechanisms as a form of preventative protection for financial services consumers. This protection is crucial considering that digital transactions are conducted without physical meetings, so customer trust depends entirely on the reliability of the systems provided by the bank.[10]

In addition to regulations, strengthening legal protection is also carried out through digital literacy for customers. Many data breaches occur due to customers' lack of understanding of digital transaction security. The digital literacy program implemented by the Financial Services Authority (hereinafter referred to as OJK) and Bank Indonesia (hereinafter referred to as BI) is part of the National Financial Inclusion Blueprint 2024 strategy, which emphasizes the importance of data security in the digital financial ecosystem. On the repressive side, Law 27/2022 provides a strong legal basis for prosecuting violations of personal data protection. Articles 57 to 61 of Law 27/2022 regulate administrative sanctions ranging from warnings, administrative fines, to temporary suspension of data processing activities. Furthermore, Articles 67 to 69 also regulate criminal sanctions for parties who intentionally or negligently cause data breaches. However, the implementation of these sanctions still faces various obstacles. The lack of capacity of supervisory agencies to trace digital footprints and the limitations of digital forensic technology mean that many data breach cases remain unresolved.

[7] IBM Security.

[8] Camila Amalia et al., "Legal Issues of Personal Data Protection and Consumer Protection in Open API Payments," *Journal of Central Banking Law and Institutions* 1, no. 2 (2022): 323–52, https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost of a Data Breach Report 2020.pdf.

[9] Bank Indonesia, *Blueprint Sistem Pembayaran Indonesia 2025 BI: Menavigasi Sistem Pembayaran Nasional di Era Digital* (Jakarta: Bank Indonesia, 2019), p. 39.

[10] Eric Goosen, "The Influence of Law & Regulations on The Process of Digital Transformation at Banks in The Netherlands" (Leiden University, 2020).

Therefore, strengthening institutional capacity and collaboration between agencies such as the Financial Services Authority (OJK), the Ministry of Communication and Information Technology (Kominfo), and the National Cyber and Cyber Security Agency (BSSN) is urgent. Legal protection efforts must also consider the principle of restorative justice, which prioritizes restoring the rights of injured customers over mere punishment. Banks can be required to provide financial compensation, data recovery services, or additional security guarantees to affected customers. This approach aligns with the principles of consumer protection law, which focuses on restoring public trust. Furthermore, legal certainty in digital banking transactions plays a crucial role in maintaining public trust in banking institutions.

In the long term, legal protection for digital banking customers will be effective if accompanied by an improved compliance culture within banking institutions. Banks must view personal data protection as part of their strategic value and competitive advantage, not simply a legal obligation. Thus, data protection becomes the foundation for building a sustainable and equitable digital financial ecosystem. From the above description, it can be concluded that legal protection for customers against personal data leaks in digital banking services must be implemented comprehensively through strong regulations, consistent law enforcement, and increased legal awareness at both customer and industry levels. This combination will maintain public trust in the digital banking system and allow the digital financial transformation in Indonesia to develop safely and sustainably.[11]

The Financial Services Authority (OJK) is pushing for digital acceleration in the financial sector, driven by the spirit and goal of making Indonesian banking more competitive, efficient, adaptive, and contributive to the national economy, as well as providing broad benefits to the Indonesian people.[12] The Financial Services Authority (OJK) has issued Regulation No. 12/POJK.03/2021 concerning Commercial Banks (POJK on Commercial Banks), which strengthens the presence of Digital Banks in an effort to respond to technological developments in the digital era. The shift from traditional banking to future banking is driving the digitalization of banking, including the establishment of digital banks through the establishment of new banks or the transformation of existing ones. Therefore, Indonesian Legal Entity Banks (BHI) that claim to be Digital Banks are not only guided by the provisions in the POJK on Commercial Banks that regulate Digital Bank requirements, but are also required to comply with other provisions closely related to the business and operational models of Digital Banks and not simply use the Digital Bank label as a business gimmick. This, in addition to creating innovation risks, is the cost of innovation that outweighs the benefits gained.[13] Digital banking operations face challenges in the form of other potential risks, such as the protection and exchange of personal data that are not guaranteed by law; cyberattacks, data leaks, technology misuse, or third-party risks (outsourcing).[14]

Innovative and secure technology is a prerequisite for digital banks. Innovative technology includes reliable technology that supports digital bank business activities, while secure technology ensures the protection of the interests of digital banks, customers, and other stakeholders. Furthermore, rapid technological developments require digital banks to have a robust Information Technology (IT) framework and governance integrated with corporate governance. This IT governance will influence IT selection decisions that align with the needs and circumstances of all stakeholders. A good IT Governance framework and implementation will guide the bank to achieve the bank's business goals and objectives for the long term. The Financial Services Authority Regulation (POJK) for Commercial Banks does not regulate governance, but refers to applicable provisions. Previously, the OJK issued POJK

[11] Muhamad Amirulloh et al., "Legal Basis and Readiness of the Banking Sector in Implementing Privacy Reliability Certification," *Jurnal IUS Kajian Hukum dan Keadilan* 13, no. 3 (2025): 545–58, https://doi.org/10.29303/ius.v13i3.1777.

[12] Otoritas Jasa Keuangan, "Ringkasan Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 Tentang Bank Umum," ojk.go.id, 2022, https://www.ojk.go.id/id/regulasi/Documents/Pages/Bank-Umum/Summary - POJK 12 - 03 - 2021.pdf.

[13] Elisa Tjondro et al., "Do Digital Innovation and Risk Disclosure Control Performance? Evidence from Banking in ASEAN-6," *JIA (Jurnal Ilmiah Akuntansi* 6, no. December (2021): 200–220, https://doi.org/10.23887/jia.v6i2.33321.

[14] Tjondro et al.

No. 55/POJK.03/2016 concerning Governance for Commercial Banks (POJK Governance for Commercial Banks) which was then followed up by issuing OJK Circular Letter No. 13/SEOJK.03/2017 concerning the Implementation of Governance for Commercial Banks and its attachments. Similar to the general obligations of banks, in order to improve bank performance, digital banks are required to implement governance based on 5 principles of good governance, namely: Transparency, namely openness in disclosing material and relevant information and openness in the decision-making process, Accountability, namely clarity of function and implementation of the accountability of bank organs so that management runs effectively, Responsibility, namely the conformity of bank management with laws and regulations, Independence, namely the professional management of the bank without influence or pressure from any party, and fairness, namely justice and equality in fulfilling the rights of stakeholders that arise based on agreements and statutory regulations.

Information technology is a valuable asset for banks, so its management is not only the responsibility of the bank itself but also of all parties using it. The use of technology by digital banks can improve efficiency and service quality, but on the other hand, it can also increase risks. The most potential risk in digital banking activities is data leaks or cyberattacks. These data leaks or cyberattacks impact consumer trust in the security of shared data. As a result, banks will face several types of risks, including strategic risk, operational risk, legal risk, and reputational risk. One factor that consumers consider when sharing personal data is trust in the company. Therefore, in the context of data protection and cybersecurity, the implementation of information technology risk management in digital banking activities is very urgent.[15]

The provision of information technology can be carried out by the Bank itself and/or an information technology service provider. In the case of information technology provision carried out by a service provider, the Bank is obliged to be responsible for the implementation of risk management. Information technology service providers are obliged to have reliable experts supported by academic and/or professional expertise certificates and maintain the security of all information including Bank secrets and customer personal data. Regarding information security and Bank secrets, service providers can only transfer some activities (subcontracts) based on the bank's approval as evidenced by written documents. The legal relationship between the Bank and the service provider is based on a written agreement whose clauses at least refer to Article 20 Paragraph (3) of the POJK MRTI. In principle, service providers are obliged to provide services that can maintain and protect data security. Therefore, a written agreement containing the rights and obligations of the Bank and the service provider is one way to strengthen risk management.[16]

AI Innovation and Data Access: In 2025, Bank BDN deployed a Generative and Predictive Machine Learning-based AI technology named "SmartVerify" to expedite Know Your Customer (KYC) procedures, credit scoring, and fraud detection systems. The AI framework was granted full access to the bank's historical customer databases, including National Identification (KTP) records, biometric facial scans, transaction histories, and behavioral data.

Cyberattack and AI Exploitation: A threat actor group launched a combined Data Poisoning and Adversarial Attack targeting the SmartVerify AI algorithm. By manipulating data inputs to deceive the AI model, the perpetrators exploited vulnerabilities within the banking system's cybersecurity Application Programming Interfaces (APIs).

Breach and Fraudulent Exploitation: The breach compromised the biometric facial data and financial records of 1.2 million customers, which were subsequently leaked onto the Dark Web. Utilizing this stolen biometric information, the attackers generated synthetic biometric deepfakes to execute Deepfake Biometric Spoofing, illicitly accessing third-party bank accounts and causing massive financial losses to account holders.

[15] Bruno Zeller and Andrew Dahdal, "Open Banking and Open Data in Australia: Global Context, Innovation and Consumer Protection" (Doha, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3766076.

[16] Amalia et al., "Legal Issues of Personal Data Protection and Consumer Protection in Open API Payments."

**Legal Policy in Combating Crime Using Artificial Intelligence and Cyber Security**

The rise in cybercrime, which is increasingly diverse and sophisticated, demands systematic efforts to develop policies that address the need for personal data protection. Crimes such as credit card fraud (carding), system hacking, and malware distribution have detrimental impacts on individuals, organizations, and even countries. Therefore, legislation governing personal data protection is highly relevant and urgently needed to mitigate the risks posed.

The integration of artificial intelligence (AI) models into core banking functions—specifically Know Your Customer (KYC) and biometric authentication—fundamentally alters the legal duties imposed on financial institutions. Under modern data protection legal frameworks, such as the Indonesian Personal Data Protection Act (UU No. 27/2022) and the EU General Data Protection Regulation (GDPR), PT Bank Digital Nusantara (BDN) operates in the capacity of a Data Controller.

Biometric facial templates constitute Specific (Sensitive) Personal Data due to their unique, immutable relationship to individual identity. Consequently, the standard of care required in processing such data elevates from ordinary prudence to a heightened duty of care (extraordinary diligence).

However, the lack of clear regulations regarding personal data protection has led to an increase in cases of misuse of information systems and personal data. Therefore, it is crucial to develop a system that can address this issue. Currently, Indonesia still lacks a law specifically governing personal data protection. Existing regulations are scattered across various laws, necessitating the creation of more comprehensive, detailed, and robust legislation to regulate the protection of personal data.[17]

The importance of personal data protection is increasingly recognized with the increasing use of information technology in everyday life. Without clear and adequate regulations, the potential for misuse of personal data increases, both for commercial purposes and cybercrime. This demands that the government immediately take concrete steps to draft legislation that not only regulates individuals' rights to their personal data but also provides strict sanctions for perpetrators of misuse. The existence of this comprehensive law is expected to strengthen public trust in digital systems and prevent data exploitation that is detrimental to irresponsible parties.[18]

Instead, prevention needs to be carried out with a more systematic and integrated approach. Fundamentally, criminal law policy aims to formulate criminal law in an appropriate manner, provide guidance for lawmakers, and ensure the effective implementation of criminal law. Legislative policy plays a crucial role in determining the direction of criminal law regulations, as the desired objectives must be established from the outset. For example, in Article 26 paragraph (2) of the ITE Law, the provision does not impose criminal sanctions on perpetrators, where victims can only file civil lawsuits. Furthermore, Article 26 of the ITE Law only covers basic protection for personal data. Information technology experts have criticized Article 26 for its shortcomings, namely that it does not provide adequate protection for users of personal data used for specific purposes by companies. Data security aims to improve data protection by: 1) Protecting data from being accessed by unauthorized parties; and 2) Preventing unauthorized parties from entering or deleting data. Indonesia requires a more specific legal instrument to address this crime. Currently, existing Indonesian law, specifically Law Number 1 of 2023 concerning the Criminal Code, is ineffective (KUHP).[19]

Criminal law policy within Indonesian positive law is currently in its early stages in responding to the development of Artificial Intelligence (AI)-based cybercrime. The primary instruments used to address cybercrime are the Criminal Code (KUHP) and the ITE Law. In general, these regulations address several forms of cybercrime, such as illegal access, hacking, the dissemination of false information, and

[17] Moody Rizqy Syailendra, Gunardi Lie, and Ahmad Sudiro, "Personal Data Protection Law in Indonesia: Challenges and Opportunities," *Indonesia Law Review* 14, no. 2 (2024): 56–72, https://doi.org/10.15742/ilrev.v14n2.1.

[18] Syailendra, Lie, and Sudiro.

[19] Supeno Supeno et al., "Personal Data Protection in Review of Legal Theories and Principles," *Journal of Law & Legal Reform* 6, no. 3 (2025): 1349–76, https://doi.org/10.15294/jllr.v6i3.10252.

personal data breaches. However, in the context of AI-based cybercrime, existing positive law does not explicitly regulate the role, legal responsibilities, or limitations of the use of artificial intelligence in cybercrime. For example, crimes involving deepfakes, automated phishing, or AI-driven malware are still difficult to clearly classify within the categories of offenses regulated by the Criminal Code or the ITE Law.[20]

In this regard, Indonesia still faces a legal vacuum, as Artificial Intelligence (AI) is a digital entity with no clear legal status, making it difficult to determine who is criminally responsible for its actions. This creates legal uncertainty and can hamper law enforcement efforts. From the author's perspective, this indicates that existing criminal law policies are still inadequate, both substantively and technically, to address the complexities of AI-based cybercrime. This legal vacuum arises because the Indonesian legal system has not yet anticipated the rapid development of digital technology, particularly in terms of legal subjects, criminal liability, and digital crime prevention models that use AI as a tool or actor.[21] A comparable gap has been identified in the handling of digital invitation fraud carried out through modified applications, in which the general provisions of the Criminal Code and the ITE Law were unable to accommodate the specific modus operandi used by the perpetrators.[22]

The development of artificial intelligence has now penetrated various devices and is used in almost all sectors of life, from finance and business, engineering, gadgets, aviation, transportation, and so on. The increasingly easy and common access to artificial intelligence is now starting to be used for criminal purposes. Some forms of AI-based cybercrime that are currently rampant include Deepfake Fraud (the use of AI algorithms to create fake videos that resemble a person), AI-Generated Phishing Emails (creating phishing via email with a very high level of personalization), and Identify Theft (the theft of personal data from social media to create a fake identity using AI). The main challenges in eradicating AI-based cybercrime are due to the lack of specific regulations, limited capabilities and knowledge of law enforcement officials, and the lack of technological infrastructure in detecting and preventing cyber attacks.[23]

Criminal law regulations regarding combating AI-based cybercrime, particularly the Electronic Information and Transactions Law (UU ITE), are a crucial primary instrument. However, despite the law's existence, its implementation has not been able to address the existing problems. Some limitations in positive law regarding combating AI-based cybercrime include:[24]

1) Lack of regulations specifically regarding AI Cybercrime
2) The definition and scope of cybercrime in the ITE Law tend to be general, thus failing to encompass AI-based crimes.
3) Lack of capacity among law enforcement officials, particularly regarding the identification and handling of AI-based cybercrimes.

Legal policy reforms regarding combating AI-based cybercrime are urgently needed. This is undoubtedly due to the legal vacuum in Indonesia, where there are no regulations that specifically address AI-based cybercrime issues. This legal vacuum specifically concerns the legal status and responsibilities of AI within the Indonesian legal industry. This legal vacuum in the AI field has led many legal practitioners to utilize existing regulations related to technology to address AI-related issues, one of which is the Electronic Information and Transactions Law (UU ITE).[25]

Given the legal vacuum in the AI field, it is necessary to anticipate all potential issues arising from the lack of regulations in the field of artificial

[20] Danrivanto Budhijanto, *Hukum Pelindungan Data Pribadi di Indonesia: Cyberlaw & Cybersecurity* (Bandung: PT. Refika Aditama, 2023), p. 112.

[21] Budhijanto.

[22] Septiana Prameswari and Titik Suharti, "Perlindungan Hukum Terhadap Korban Penipuan Berkedok Undangan Digital Menggunakan Aplikasi Whatsapp [1],[2]," *PERSPEKTIF: Kajian Masalah Hukum Dan Pembangunan* 31, no. 1 (2026): 35–42, https://doi.org/10.30742/perspektif.v31i1.915.

[23] Aloysius Wisnubroto and Hilaire Tegnan, "Preventing AI Crime Towards A New Legal Paradigm: Lessons From United States," *Journal of Human Rights, Culture and Legal System* 5, no. 2 (2025): 630–58, https://doi.org/10.53955/jhcls.v5i2.606.

[24] Lytio Enggar Erlangga, Muhammad Syaroni Rofii, and Eko Daryanto, "The Potential Threat of Artificial Intelligence Use in Cybercrime Activities: A Case Study of 2024 Regional Head Elections," *International Journal of Science and Society* 6, no. 4 (2024): 56–67, https://doi.org/10.54783/ijsoc.v6i4.1297.

[25] Erlangga, Rofii, and Daryanto.

intelligence. This new regulation is expected to provide detailed and clear considerations regarding the position of artificial intelligence in legal accountability. Explicitly, artificial intelligence can indeed perform legal acts like existing legal subjects. However, in practice, artificial intelligence is a human-built system and cannot act as a legal subject. Therefore, a detailed interpretation is needed in the new legal regulation that clearly regulates artificial intelligence, particularly in the context of combating artificial intelligence-based cybercrime under Indonesian law.

The urgency of updating regulations related to AI in cybercrime lies in this technology's ability to accelerate, expand, and conceal the traces of crimes. AI can be used to create adaptive malware, deepfakes, and even manipulate data that is extremely difficult to detect. Existing positive laws, such as the ITE Law or the National Criminal Code, do not yet provide explicit provisions regarding the use of AI for criminal purposes. This creates a legal vacuum that criminals can exploit. Therefore, revisions to existing regulations must include specific elements regarding AI in cybercrime. Necessary updates include adding provisions regarding crimes involving the development, use, or distribution of AI technology for illegal purposes. For example, regulations need to specifically address the creation of deepfakes for fraud, the use of AI for attacks on critical infrastructure, and market manipulation through intelligent algorithms. Furthermore, it is crucial to define legal responsibilities for irresponsible AI developers and users, including algorithm audit mechanisms and appropriate criminal sanctions.[26]

The legal reform landscape should also encompass international collaboration, given the cross-border nature of AI-based cybercrime. Indonesia can learn from other countries that have begun to regulate this technology, such as the European Union's Artificial Intelligence Act or the United States' approach through legislation governing AI-based data security. Legal reform in Indonesia should emphasize the integration of global standards, algorithm monitoring, and capacity building for law enforcement to handle AI cybercrime cases. With these reforms, the Indonesian legal system will not only be responsive to the challenges of modern technology but also create a fair and relevant legal framework. This aligns with the goal of Law Number 1 of 2024, which is to provide stronger legal protection for citizens in the digital age. This step also reflects a progressive legal vision that not only reacts to threats but also proactively creates a safe and just digital space.[27]

## CLOSING

### Conclusion

First, regarding legal protection for customers against personal data leaks in digital banking services in Indonesia, it can be concluded that the legal protection provided to customers is not yet fully effective and comprehensive. Although Indonesia has a fairly strong legal basis through Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), Law Number 10 of 1998 concerning Banking, and various derivative regulations from the Financial Services Authority (OJK) and Bank Indonesia (BI), its implementation in the field still faces several obstacles. The main problems lie in weak policy implementation, low compliance by financial institutions with data security standards, and suboptimal supervision and law enforcement by the relevant authorities. Leakage of customer personal data is a multidimensional phenomenon that involves not only legal aspects but also technology and business ethics. Dominant causal factors such as weak cybersecurity systems, the absence of adequate data governance, and low legal awareness at both the banking institution and customer levels demonstrate that the existing regulations remain normative and have not been implemented in a preventive and comprehensive manner.

Second, customer protection within the digital banking ecosystem cannot rely on a single entity. The successful mitigation of cybercrime risks—ranging from social engineering and phishing to data breaches and the exploitation of artificial intelligence models through data poisoning and adversarial attacks—requires robust synergy between the technical and educational readiness

[26] Herke Csongor and David Toth, "Artificial Intelligence in Cybersecurity: Examining Liability, Crime Dynamics, and Preventive Strategies," *EU and Comparative Law Issues and Challenges Series (ECLIC)* 8, no. 1 (2024), https://doi.org/10.25234/eclic/32299.

[27] Csongor and Toth.

of commercial banks and a dynamic, responsive regulatory framework established by the governing authorities. The integration of AI into Know Your Customer (KYC) procedures and biometric authentication elevates the standard of care owed by banks, because biometric facial templates constitute specific (sensitive) personal data whose compromise is permanent and irreversible.

Third, current criminal law policies in Indonesian positive law are not yet fully able to accommodate the complexity and development of cybercrimes involving Artificial Intelligence (AI) technology. Although several provisions in the Criminal Code and the ITE Law regulate types of cybercrime in general, there are no specific and comprehensive regulations governing the role and impact of AI use in digital crimes. The absence of explicit regulations regarding AI as a means or as a subject contributing to cybercrime creates a legal vacuum that weakens law enforcement efforts and the protection of the public, and this condition is aggravated by the limited capacity of law enforcement officials in identifying and handling AI-based cybercrime.

**Recommendation**

Based on the findings above, the authors put forward the following recommendations, addressed to the legislature, the financial services authorities, banking institutions, and law enforcement agencies.

1) To the Government and the House of Representatives (regulatory reform). A lex specialis governing AI-based cybercrime needs to be formulated, either through a targeted amendment of the ITE Law or through a dedicated Artificial Intelligence Act. At a minimum, such regulation should: (a) define artificial intelligence as a means, an object, and a potential source of criminal risk; (b) allocate criminal, civil, and administrative responsibility along the AI value chain—the developer, the provider, and the user or controller of the model—so that the unsettled legal status of AI does not become a ground for impunity; and (c) adopt a risk-based classification approach, as applied in the European Union Artificial Intelligence Act, under which the use of AI for biometric identification and credit scoring in the banking sector is categorised as high-risk and subjected to stricter obligations.
2) To the Financial Services Authority (OJK) and Bank Indonesia (technical standards). A technical regulation should be issued that mandates Data Protection by Design and by Default together with Explainable AI (XAI) compliance benchmarks for every AI model used in KYC procedures, biometric authentication, and credit scoring. Supervision must go beyond routine Vulnerability Assessment and Penetration Testing (VAPT) to include periodic algorithmic audits, adversarial robustness testing (simulation of data poisoning and adversarial attacks or AI red-teaming), documentation of models and the provenance of training data, and an obligation to retain meaningful human oversight (human-in-the-loop) over decisions that produce significant legal effects for customers.
3) To banking institutions (internal compliance). Banks should conduct a Data Protection Impact Assessment before deploying any AI system, treat biometric templates as specific personal data through encryption, tokenisation, segregated storage, and strict retention limits, and tighten the governance of third-party information technology service providers by including audit rights and clear liability clauses in outsourcing contracts. Banks must also maintain an incident response mechanism with notification to the supervisory authority and affected data subjects within the time limit prescribed by the PDP Law, provide continuous digital literacy programmes for customers, and shift from a formalistic approach to a genuine compliance culture in which personal data protection is treated as part of risk management and customer trust rather than an administrative burden.
4) To the courts and legal doctrine (reconstruction of liability). The doctrine of banking liability should be reconstructed through a rebuttable presumption of negligence, whereby the burden of proof is shifted to the bank to demonstrate that it has applied the prevailing security and data governance standards once a leak of customer data has occurred. This reconstruction needs to be accompanied by strengthening the customer's right to restitution and compensation,

an effective complaint channel through the Alternative Dispute Resolution Institution of the Financial Services Sector (LAPS SJK), and the opening of a class action mechanism for mass data breaches. The reinforcement of restitution as a legal remedy for consumers has likewise been emphasised in studies concerning victims of illegal digital investment.[28]

5) To the supervisory and law enforcement institutions (institutional capacity). The establishment and operationalisation of an independent Personal Data Protection Supervisory Authority endowed with genuine administrative sanctioning powers should be accelerated, since supervision that is spread across sectors has proven ineffective. In parallel, the capacity of law enforcement officials must be improved through certified digital forensics training oriented towards AI-based evidence, the formation of specialised units within the Police and the Attorney General's Office, and certification for judges handling cybercrime cases.

6) To policymakers and future researchers (international cooperation and further study). Given the cross-border character of AI-based cybercrime, Indonesia needs to harmonise its national rules with international instruments such as the Budapest Convention on Cybercrime and to strengthen mutual legal assistance as well as cross-border data transfer arrangements. Further research is recommended in the form of empirical studies on the effectiveness of AI-based fraud detection systems in national banking and quantitative testing of the proposed Explainable AI compliance benchmarks, so that the normative findings of this study can be validated in practice.

## REFERENCES

**Regulations:**

Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan. (Lembaran Negara Tahun 1998 Nomor 182, Tambahan Lembaran Negara Nomor 3790).

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 dan Undang-Undang Nomor 1 Tahun 2024. (Lembaran Negara Tahun 2008 Nomor 58, Tambahan Lembaran Negara Nomor 4843).

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (Lembaran Negara Tahun 2022 Nomor 198, Tambahan Lembaran Negara Nomor 6820).

Peraturan Otoritas Jasa Keuangan Nomor 12/ POJK.03/2021 tentang Bank Umum.

Peraturan Otoritas Jasa Keuangan Nomor 11/ POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum.

**Books:**

Bank Indonesia. *Blueprint Sistem Pembayaran Indonesia 2025 BI: Menavigasi Sistem Pembayaran Nasional di Era Digital*. Jakarta: Bank Indonesia, 2019.

Budhijanto, Danrivanto. *Hukum Pelindungan Data Pribadi di Indonesia: Cyberlaw & Cybersecurity*. Bandung: PT. Refika Aditama, 2023.

Goosen, Eric. "The Influence of Law & Regulations on The Process of Digital Transformation at Banks in The Netherlands." Leiden University, 2020.

**Journal Articles:**

Amalia, Camila, Esha Gianne Poetry, Mochamad Kemal Kono, Dadang Arief K., and Alex Kurniawan. "Legal Issues of Personal Data Protection and Consumer Protection in Open API Payments." *Journal of Central Banking Law and Institutions* 1, no. 2 (2022): 323–52. https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost of a Data Breach Report 2020.pdf.

Amirulloh, Muhamad, Eman Suparman, Helitha Novianty Muchtar, and Hetty Hassanah. "Legal Basis and Readiness of the Banking Sector in Implementing Privacy Reliability Certification." *Jurnal IUS Kajian Hukum dan Keadilan* 13, no.

[28] Natalia Ramma, "Restitution of Victims: Funds as Legal Remedy for Consumer in Illegal Digital Investments," *PERSPEKTIF: Kajian Masalah Hukum dan Pembangunan* 31, no. 1 (2026): 43–51, https://doi.org/10.30742/perspektif.v31i1.999.

3 (2025): 545–58. https://doi.org/10.29303/ius.v13i3.1777.

Csongor, Herke, and David Toth. "Artificial Intelligence in Cybersecurity: Examining Liability, Crime Dynamics, and Preventive Strategies." *EU and Comparative Law Issues and Challenges Series (ECLIC)* 8, no. 1 (2024). https://doi.org/10.25234/eclic/32299.

Erlangga, Lytio Enggar, Muhammad Syaroni Rofii, and Eko Daryanto. "The Potential Threat of Artificial Intelligence Use in Cybercrime Activities: A Case Study of 2024 Regional Head Elections." *International Journal of Science and Society* 6, no. 4 (2024): 56–67. https://doi.org/10.54783/ijsoc.v6i4.1297.

Kholis, Nur. "Perbankan Dalam Era Baru Digital." *Jurnal Economicus* 12, no. 1 (2018): 80–88.

Maulana, Rizki Akbar, and Rani Apriani. "Perlindungan Yuridis Terhadap Data Pribadi Nasabah Dalam Penggunaan Elektronik Banking (e-Banking)." *Jurnal Hukum De'rechtsstaat* 7, no. 2 (2021): 163–72.

Prameswari, Septiana, and Titik Suharti. "Perlindungan Hukum Terhadap Korban Penipuan Berkedok Undangan Digital Menggunakan Aplikasi Whatsapp [1],[2]." *PERSPEKTIF: Kajian Masalah Hukum dan Pembangunan* 31, no. 1 (2026): 35–42. https://doi.org/10.30742/perspektif.v31i1.915.

Ramma, Natalia. "Restitution of Victims: Funds as Legal Remedy for Consumer in Illegal Digital Investments." *PERSPEKTIF: Kajian Masalah Hukum dan Pembangunan* 31, no. 1 (2026): 43–51. https://doi.org/10.30742/perspektif.v31i1.999.

Supeno, Supeno, Rosmidah Rosmidah, Syed Mohd, and Uzair Iqbal. "Personal Data Protection in Review of Legal Theories and Principles." *Journal of Law & Legal Reform* 6, no. 3 (2025): 1349–76. https://doi.org/10.15294/jllr.v6i3.10252.

Syailendra, Moody Rizqy, Gunardi Lie, and Ahmad Sudiro. "Personal Data Protection Law in Indonesia: Challenges and Opportunities." *Indonesia Law Review* 14, no. 2 (2024): 56–72. https://doi.org/10.15742/ilrev.v14n2.1.

Tjondro, Elisa, Margaretha Oerip Cintya, Silvia Seto, and Yemima Gracia Suherman. "Do Digital Innovation and Risk Disclosure Control Performance? Evidence from Banking in ASEAN-6." *JIA (Jurnal Ilmiah Akuntansi* 6, no. December (2021): 200–220. https://doi.org/10.23887/jia.v6i2.33321.

Wisnubroto, Aloysius, and Hilaire Tegnan. "Preventing AI Crime Towards A New Legal Paradigm: Lessons From United States." *Journal of Human Rights, Culture and Legal System* 5, no. 2 (2025): 630–58. https://doi.org/10.53955/jhcls.v5i2.606.

**Thesis, Reports, and Internet Sources:**

Anugerah, Pijar. "Pinjaman Online: 'Bagaimana Saya Menjadi Korban Penyalahgunaan Data Pribadi.'" BBC News Indonesia, 2021. https://www.bbc.com/indonesia/majalah-57046585.

IBM Security. *Cost of a Data Breach Report 2020*. New York, 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost of a Data Breach Report 2020.pdf.

Mediana, and Benediktus Krisna Yogatama. "Data 2 Juta Nasabah Bocor, BRI Life Telusuri Jejak Digital." kompas.id, 2021. https://www.kompas.id/artikel/data-2-juta-nasabah-bocor-bri-life-telusuri-jejak-digital.

Meidyana, Anggie. "Sindikat Jual Beli Data Pribadi Untuk Judol Terungkap, Korban Diiming-Imingi Jutaan Rupiah." metrotvnews.com, 2025. https://www.metrotvnews.com/play/kBVC9Qdn-sindikat-jual-beli-data-pribadi-untuk-judol-terungkap-korban-diiming-imingi-jutaan-rupiah.

Otoritas Jasa Keuangan. "Ringkasan Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 Tentang Bank Umum." ojk.go.id, 2022. https://www.ojk.go.id/id/regulasi/Documents/Pages/Bank-Umum/Summary - POJK 12 - 03 - 2021.pdf.

Zeller, Bruno, and Andrew Dahdal. "Open Banking and Open Data in Australia: Global Context, Innovation and Consumer Protection." Doha, 2021. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3766076.