PERSPEKTIF HUKUM

Volume 26 Issue 1 Mei 2026

THE URGENCY OF COMPLIANCE AUDIT 5.0 THROUGH AN APPROACH TO PERSONAL DATA PROTECTION LAW

Frendika Suda Utama [1]✉, **Irma Dwi Yulistyani** [2]

[1] Faculty of Law, Airlangga University, Surabaya, Indonesia, Email: frendika.suda.utama-2021@fh.unair.ac.id

[2] Faculty of Economics and Business, University of Indonesia, Depok, Indonesia, Email: irma.dwi31@ui.ac.id

✉ corresponding email: frendika.suda.utama-2021@fh.unair.ac.id

Article

Keywords:
Data Protection, Privacy, Legal Audit, Cybercrime

Article History
Received: Aug 18, 2025;
Reviewed: Oct 31, 2025;
Accepted: May 11, 2026;
Published: May 16, 2026;

Abstract

Datacrime is increasing massively and collectively in the era of Society 5.0. The era of data digitization has given rise to advances in information technology that affect all aspects of human life. The victims not only suffered material losses, but also immaterial. In Indonesia, there are not only cases of crimes against personal data in the financial sector (theft of customer data), but also in the public service sector, namely the leakage of voter data from the Indonesian Election Commission. This study aims to provide a comprehensive picture of personal data crimes, including descriptions of modus operandi and of how compliance audits are conducted from a personal data protection law perspective. The researcher used normative legal research, with a case approach, to explore the series of crimes and to unravel the ratio decidendi of the court's decision. This article also uses a conceptual approach, namely the perspective of Lex Specialist Data, and the regulation of digital data privacy. The technical regulation

of data privacy legal aspects in the legal compliance audit aligns with the strengthening of personal data protection laws. The idea of a legal compliance audit through a personal data protection approach helps prevent and even mitigate the risk of data privacy crimes.

https://doi.org/10.30649/ph.v26i1.433

Introduction

The Society 5.0 shows the condition of a society with high intellect in using information technology (super smart society) starting in 2025.[1] Various innovations in the Internet of Things (IoT), artificial intelligence (AI), and big data affect the pattern of community interaction. This wave shifts conventional patterns to be very digital, especially for essential sectors in life, such as the financial sector, banking, health, education, trade, and government. The challenge in the era of Society 5.0 is the national legal rules that must adapt to the speed of information technology innovation without eliminating the nation's identity in the framework of the constitution, namely, ethical, religious, and cultural values. The collaboration of Society 5.0 technology with national wisdom is ideal for responding to these dynamics. However, this must also be followed by a common will to harmonize the pattern of interaction of technological advances in the community with government policies in responding to incidents and proportionate mitigation of every incident of information technology-based crime. However, there is a well-known basic principle that prevention is much better than cure, so every effort to find gaps in information technology interaction is part of improving security

[1] Nabeel Mahdi Althabhawi, Zinatul Ashiqin Zainol, and Parviz Bagheri, "Society 5.0: A New Challenge to Legal Norms," *Sriwijaya Law Review 6*, no. 1 (2022): 41–54, https://doi.org/10.28946/slrev.Vol6.Iss1.1415.pp41-54.

patterns and preventing the misuse of data and information or cybercrime.

Digitization of personal data in the era of society 5.0 is an important tool across all applications in the financial sector and public services. In terms of personal data protection, the EU has had regulations and principles governing data processing since 1995. This was subsequently repealed and updated by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, in line with the dynamics of data freedom, and awareness of controls over the processing of personal data (GDPR).[2] In Indonesia, although the PDP Law addresses personal data protection, it is still necessary to implement the existing PDP Law to address and prevent data leakage cases.

The principle of administrative accountability underpins the obligations of each party involved in the processing of personal data. Most research on administrative accountability continues to focus on the legal subjects of people, corporations, or institutions.[3] Meanwhile, advances in information technology have changed the dynamics of physical data of legal subjects, making them digital and managed collectively through internet-free applications, so that the examination and supervision of administrative accountability need to adapt to the perspective of personal data protection.[4] The obligation of the personal data processor to refrain from disseminating personal data must be included in the adjustment to the compliance audit review to

---

[2] Daniar Supriyadi, "The Regulation of Personal and Non-Personal Data in the Context of Big Data," Journal of Human Rights, Culture and Legal System 3, no. 1 (2023): 33–69, https://doi.org/10.53955/jhcls.v3i1.71.

[3] Lei Tao, Jinhan Wan, and Bo Wen, "The Effects of Artificial Intelligence and Victims' Deservingness Information on Citizens' Blame Attribution towards Administrative Errors," Public Management Review 27, no. 12 (2025): 3104–24, https://doi.org/10.1080/14719037.2024.2411632.

[4] Tao, Wan, and Wen.

strengthen privacy protection while maintaining the principle of administrative accountability.

The processing of personal data is growing more and more massively, driven by an increase in the number of users of internet-based services, so there is the potential for negligence and abuse of privacy.[5] The privacy of every information intersects with the urgency of data protection, as this is due to the phenomenon of human relations in a community with corporations and public sector institutions that collect information and personal data both directly and indirectly.[6] Law Number 27 of 2022 on Personal Data Protection (PDP Law) is a response to the development of data digitization flows in the face of the increasing incidence of data leaks in Indonesia's private and public sectors. Data protection vulnerabilities have encouraged illegal access, data theft, and illegal data collection that harm internet users.

After the advent of the PDP Law, it should also be followed by more strategic and specific technical instructions in facing the challenges of mass data management. This is because the PDP Law has not regulated specific and independent institutions to conduct supervision related to data supervision. On the other hand, there are still many incidents of data leaks experienced by the private and public sectors, which are not only due to the internal negligence of data managers but also external threats from cybercriminals. The data leaks that the KPU RI has experienced on voter data and customer data collection modes in Indonesia have seriously threatened data privacy

---

[5] I Nyoman Putu Budiartha, I Made Pria Dharsana, and Indrasari Kresnadjaja, "Penguatan Konstruksi Hukum Perihal Perlindungan Data Pribadi," *Jurnal Magister Hukum Udayana 12*, no. 1 (2023): 56–65, https://doi.org/10.24843/JMHU.2023.v12.i0 1.p05.

[6] Radi P. Romansky and Irina S. Noninska, "Challenges of the Digital Age for Privacy and Personal Data Protection," *Mathematical Biosciences and Engineering* 17, no. 5 (August 10, 2020): 5288–5303, https://doi.org/10.3934/MBE.2020286.

sovereignty.[7] The presence of data protection officers as supervisors will support the security of any data processing carried out collectively.

Data collected collectively by corporations or governments needs to be constantly reviewed and mapped to get an overview of potential vulnerabilities and minimise the negative impact of cyber threats on the internet user data system.[8] Information data audits can be a means of data management in evaluating data management, reducing internal negligence, and preventing data leakage.[9] General and specific data collected by the government and corporations are targets for cybercrime to take advantage of the negligence of the principal data owners themselves, as well as collective data managers.

In terms of cybersecurity and privacy protection, almost every country already has a legal instrument in the form of rules related to data privacy, but it is still necessary to take preventive approaches to overcome and even mitigate data leakage risk in the era of information technology.[10] Not only are legal provisions needed to take action against any violation of data privacy, but an instrument is needed to periodically update every privacy data protection policy to prevent data leakage. The dynamics of progressive information technology must be

---

[7] Frendika Suda Utama, Didik Endro Purwoleksono, and Taufik Rachman, "Data Leakage of the Indonesian Elections Commission in Legal Aspects of Personal Data Protection," *Media Iuris* 7, no. 3 (2024): 479–98, https://doi.org/10.20473/mi.v7i3.55931.

[8] Mamoona Humayun et al., "Internet of Things and Ransomware: Evolution, Mitigation and Prevention," *Egyptian Informatics Journal* (Elsevier B.V., March 1, 2021), https://doi.org/10.1016/j.eij.2020.05.003.

[9] Petros Lois et al., "Internal Audits in the Digital Era: Opportunities Risks and Challenges," *EuroMed Journal of Business* 15, no. 2 (June 22, 2020): 205–17, https://doi.org/10.1108/EMJB-07-2019-0097.

[10] Yao Xu et al., "Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics," *World Electric Vehicle Journal* 16, no. 1 (2025): 1–27, https://doi.org/10.3390/wevj16010006.

addressed proportionately and systematically so as not to fall into increasingly rapid cybercrime.

Efforts to improve cybersecurity to gain public trust and increase institutional profits through increasingly progressive data protection arrangements have the potential to complicate data security management itself.[11] This is because digital-based business actors have been busy with internal targets and rules that sometimes overlap. The a need for more specific and proportionate technical implementation in harmonising the law as a technology-based national development instrument. In each data storage, it is collectively necessary to pay attention to supporting devices that comply with applicable rules to realize comprehensive privacy protection.[12]

In today's all-digital era, the weakest link in the crime against data privacy is the public as the owner of the data, who is not even aware that they have been a victim of data abuse.[13] The collection of large amounts of public data without being interfered with by serious efforts by data managers to implement data protection proportionally is the cause of the problem of data privacy law violations.[14] The era of data collection often encountered today is a cloud service platform that can collect a lot of data from its users. However, a potential for threats still

---

[11] In Lee, "Cybersecurity: Risk Management Framework and Investment Cost Analysis," *Business Horizons* 64, no. 5 (2021): 659–71, https://doi.org/10.1016/j.bushor.2021.02.022.

[12] Jian Lei, Quanwang Wu, and Jin Xu, "Privacy and Security-Aware Workflow Scheduling in a Hybrid Cloud," *Future Generation Computer Systems* 131 (2022): 269–78, https://doi.org/10.1016/j.future.2022.01.018.

[13] Jeeyun (Sophia) Baik, "Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)," *Telematics and Informatics* 52 (September 1, 2020), https://doi.org/10.1016/j.tele.2020.101431.

[14] Paul Atagamen Aidonojie et al., "Legal Issues Concerning of Data Security and Privacy in Automated Income Tax Systems in Nigeria," *Hang Tuah Law Journal* 8, no. 1 (2024): 14–41, https://doi.org/10.30649/htlj.v8i1.223.

exists if users are negligent in using it, so that a lot of privacy data is revealed.[15] An information system in every community's data management should be supported by a data and personal information security risk management system, aiming to quickly and appropriately mitigate data leaks.[16] Because of these things, this study needs to explore the modus operandi of data privacy abuse, to obtain cyber threat patterns for the phenomenon of collective data digital from the perspective of Data Lex Specialists in Indonesia, to strengthen the protection of data sovereignty of internet service users.

Method

This research adopts normative legal research methods through conceptual, case, and statute approaches.[17] Legal research is conducted to provide enlightenment on a legal issue.[18] This legal research is intended to obtain a comprehensive legal prescription, not only dissecting laws and regulations but also providing legal arguments regarding the phenomenon of personal data leakage. Authors use a case study to describe the modus operandi by comparing the legal considerations of several cases of personal data leakage in Indonesia. The author also uses a legal approach to obtain a description of

[15] Tom Bolton et al., "On the Security and Privacy Challenges of Virtual Assistants," *Sensors* 21, no. 7 (2021): 1–19, https://doi.org/10.3390/s21072312.

[16] Aggeliki Tsohou et al., "Privacy, Security, Legal and Technology Acceptance Elicited and Consolidated Requirements for a GDPR Compliance Platform," *Information and Computer Security* 28, no. 4 (October 1, 2020): 531–53, https://doi.org/10.1108/ICS-01-2020-0002.

[17] Marzuki Peter Mahmud, *Penelitian Hukum Edisi Revisi*, (Jakarta: Kencana Predana Media Group, 2021), p. 133.

[18] Ibid, p. 60

concrete juridical elements, which are reviewed in legal compliance audits and reviewed from the perspective of data law.[19]

Conceptual approach. The researcher considers it important to have an approach that also examines concepts and doctrines related to the uniqueness of data crime and privacy. From this, it helps identify and explain legal definitions and concepts related to personal data protection, datacrime, data privacy, and legal compliance audits.

Juridical analysis through a statute approach. The statute approach involves examining and studying legal materials, including laws and related regulations. The laws and regulations referred to here relate to privacy, data protection, and data crime. The laws and regulations used include: the Constitution of Indonesia (UUD 1945), Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2088 concerning Information and Electronic Transactions (ITE Law); Law Number 27 of 2022 concerning Personal Data Protection (PDP Law); Law Number 1 of 2023 concerning the Criminal Code (KUHP).

Furthermore, the author applies a case approach, focusing on legal cases involving the disclosure of personal data that have been examined and decided by judges. This is intended so that the author gets legal views and opinions from the panel of judges contained in his legal consideration of a case that has occurred. Legal considerations (ratio decidendi) in decisions that have legal force can still provide a conceptual overview at the level of analysis from the perspective of judges and law enforcers in carrying out law enforcement, thereby enabling the analysis in the research to obtain a comprehensive picture. The rulings used by the author include: Criminal cases of misuse of personal data in the financial sector, namely Decision Number 2575/Pid.Sus/2022/PN. Sby, dated February 17, 2023, Case

[19] Peter Machmudz Marzuki, "The Essence of Legal Research Is to Resolve Legal Problems," *Yuridika* 37, no. 1 (March 1, 2022): 37–58, https://doi.org/10.20473/ydk.v37i1.34597.

of negligence over personal data protection in the public sector, namely Decision Number 4-PKE-DKPP/I/2024 dated April 17, 2024.

Result and Discussion

A. Modus Operandi of Data Leakage in Indonesia & Juridical Review from the Perspective of Data Lex Specialist

The Society 5.0 era clearly illustrates that society has become increasingly dependent on information technology innovations to solve its problems.[20] The urgency of sustainable development, which includes the Society 5.0 in solving community dynamics, is the key to success in managing the issues that arise today. Technology-based ideas emerge as a synergy between humans, the environment, and technology. The dynamics in society will also affect the potential for crime, which will also use innovative means of information technology advancement. To handle this crime, we must also pay attention to the principles in the Society 5.0 era, namely the principle of sustainable development. This principle emphasises solving conventional problems and combining technological patterns, information dissemination, and electronic data.

In the digital era in Society 5.0, a person's collected data collectively becomes valuable, comparable to money.[21] Today's society is very dependent on instant service through the internet, not only in terms of e-commerce, but also in terms of public services provided by the government.[22] The public's dependence on information

---

[20] Rinat A. Zhanbayev et al., "Demoethical Model of Sustainable Development of Society: A Roadmap towards Digital Transformation," *Sustainability (Switzerland)* 15, no. 16 (2023): 1–25, https://doi.org/10.3390/su151612478.

[21] Tasya Safiranita Ramli et al., "Over-the-Top Media in Digital Economy and Society 5.0," *Journal of Telecommunications and the Digital Economy* 8, no. 3 (2020): 60–67, https://doi.org/10.18080/jtde.v8n3.241.

[22] Ramli et al.

technology is also followed by the rapid development of supporting infrastructure in the private and public sectors. In Society 5.0, information technology in artificial intelligence, blockchain, and IoT has become a solution in people's lives. The potential and creativity of millennials in Indonesia encourage the rise of the digital creative economy industry. This will also raise legal problems in the era of information disclosure, including cybercrime, one of which is related to the misuse of digital data and information.

Data protection and privacy are basic human rights, including the right to obtain information regarding personal data, how it is used, who uses it, and how mechanisms to protect the processing are implemented.[23] The dynamics of the big data phenomenon in this digital era have made individual data a commodity for profit-making. The rapid development of information technology must still maintain human dignity, including maintaining the privacy of every individual's data.

It is essential to realize that the PDP Law does not guarantee freedom from cybercrime attacks; therefore, internet users must understand the importance of data privacy and always take care of the security of personal data.[24] Every future job prospect will always be related to data collection, processing, and digital data sharing platforms.[25] Online data collection is a significant challenge in terms of privacy and security, as more and more applications require the

---

[23] Najd Alfawzan et al., "Privacy, Data Sharing, and Data Security Policies of Women's MHealth Apps: Scoping Review and Content Analysis," *JMIR MHealth and UHealth* 10, no. 5 (2022), https://doi.org/10.2196/33735.

[24] Dede Ibiere Peter and Ben Collin Emeka Ndinojuo, "Privacy Awareness and Social Media: Personal Data Protection among Facebook** and Instagram** Users," *Galactica Media: Journal of Media Studies* 6, no. 3 (2024): 168–98, https://doi.org/10.46539/gmd.v6i3.489.

[25] V. Balachandar and K. Venkatesh, "Privacy-Enhanced Secure Framework for Educational Data Protection and Analysis," *International Journal of Information Technology (Singapore)* 17, no. 5 (2025): 2887–2904, https://doi.org/10.1007/s41870-025-02458-4.

authentication of users' data.[26] Every digital service always offers a variety of conveniences and even integrity, but it also contains threats to data privacy. Criminals not only take advantage of weaknesses in the information security management system, but also of human negligence.

Data security vulnerability cases in Indonesia show a significant increase yearly. Personal data theft shows an increase from 7.96% in 2023 to 20.97% in 2024, in addition to online fraud, which increased from 10.30% in 2023 to 32.50% in 2024.[27] The need for digital security in the Society 5.0 era has become more critical than ever. Cybersecurity, including internet connectivity and information technology, has become essential daily. However, the fact is that Indonesia is still ranked 24th in the Global Cybersecurity Index (GCI) 2020 with a score of 94.88, compared with the GCI of ASEAN countries, namely Singapore, ranked 4th (score 98.52), and Malaysia, ranked 5th (score 98.06).[28] This survey shows that cybersecurity requires multi-stakeholder efforts and priorities in protecting individual, private, and public data. Four critical things in improving cybersecurity are infrastructure development, mutual awareness of cybersecurity responsibilities, growing a dynamic cybersecurity-based ecosystem, and strengthening collaboration between institutions or across countries.

The mode of collecting personal data for commercial or political purposes has made many people very worried about this incident. The

---

[26] Sajid Habib Gill et al., "Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study," *Intelligent Automation and Soft Computing* 31, no. 1 (2022): 117–28, https://doi.org/10.32604/IASC.2022.016597.

[27] Indonesian Internet Service Providers Association, "Indonesian Internet Penetration Survey 2024", Indonesian Internet Service Providers Association, http://survei.apjii.or.id (accessed March 21, 2025)

[28] International Telecomunication Union, "Global Cybersecurity Index 2020", ITU Publications, http:// www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed March 21, 2025)

potential for misuse of privacy data is increasing along with the emergence of increasingly digital applications that veil social media information and spread scam pages. That threatens their data privacy, but on the other hand, many Indonesian Gen Z teenagers still do not understand the urgency of data protection. There are several cases of data leaks that have become public concern, for example, the leak of 19.56 million BPJS Ketenagakerjaan data, the leak of 1.5 terabytes (TB) of BSI (Bank Syariah Indonesia) personal data, the leak of 35 million data records from MyIndiHome users, the leak of 34.5 million passport data of Indonesian people.[29] In 2022, Indonesia had special legal rules related to Data Protection. The dynamics of the Society 5.0 era have encouraged awareness of the importance of data and information principles. Therefore, the protection of individual data privacy must be realised in the legal and regulatory sectors.

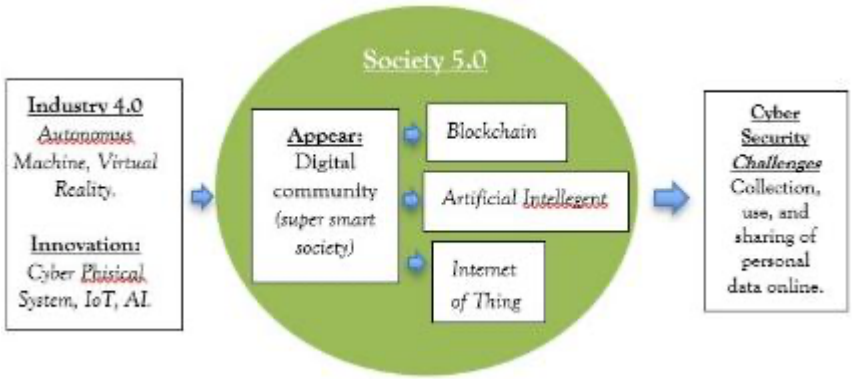

Figure 1. *Vulnerability Patterns for Cybersecurity in the Society 5.0, Source: Author Analysis*

One of the modus operandi that often occurs in this crime case is that criminals manipulate information to users to provide their data, which can then be used for identity theft indirectly. The threat of phishing crimes in the banking sector is increasing amid economic

[29] Kania Aisha Pasaman, et al, *Indonesia Gen Z Report 2024 Understanding and Uncovering the Behavior, Challenges, and Opportunities* (IDN Media, 2024) hlm. 34

growth and the digitalization of services worldwide.[30] The target of the perpetrators of the crime is the use of credit cards, debit cards, and e-money at random, and can be carried out across jurisdictions. The perpetrator provided information similar to that of related institutions to deceive the victim into sharing confidential personal data.

The current mode of crime that has developed rapidly is the Technical Support Scam (TSS) model, similar to the fraud method that is not only financially harmful, but also a viral infection on the device that causes disruption or damage.[31] This mode uses iframes and pop-up authentication displays to freeze the user's browser. When a Windows user visits the site and clicks on the link they created, it leads to a page on the site. Then, a warning appears as if the computer has been infected with a virus, and it warns users to call a specific number to get technical services immediately. When the victim is lured and calls the scammer's number, the scammer will impersonate it as if it were an official site service, and request remote access to the user's computer.

Furthermore, the perpetrator directs the user to show system errors and tricks the user into using the instructions, even though the repair service does not need to be carried out. Finally, the user sends the payment money to complete the transaction. And the scammer closes with the service verification information and disappears. They profit from payments from victims, and illegal access to data and documents on victims' computers.[32]

---

[30] Moruf Akin Adebowale, Khin T. Lwin, and M. A. Hossain, "Intelligent Phishing Detection Scheme Using Deep Learning Algorithms," *Journal of Enterprise Information Management* 36, no. 3 (April 24, 2023): 747–66, https://doi.org/10.1108/JEIM-01-2020-0036.

[31] Yu Chen Chen, Jiann Liang Chen, and Yi Wei Ma, "AI@TSS- Intelligent Technical Support Scam Detection System," *Journal of Information Security and Applications* 61 (September 1, 2021), https://doi.org/10.1016/j.jisa.2021.102921.

[32] Chen, Chen, and Ma.

Furthermore, the modus operandi that often occurs in the public sector is illegal access, which results in the leakage of public data to third parties. Legal and public policy practitioners discussed the case of data leakage that had gone viral, which was the leak of voter information belonging to KPU, which occurred repeatedly. The author describes one of the cases of voter data leakage experienced by the Indonesian Election Commission, which was sold and offered by the anonymous account "Jimbo" offering around more than 252k voter data on the hacker site "breachforump.is/user-jimbo" worth 24 thousand USD.[33] The data successfully hacked was 500 thousand records containing full names, NIK, place of birth, KK, Passport Number, gender, address, and TPS code. The KPU issued a press release dated November 29, 2023, and reported the data leak and voter data sales activities to the police. It also coordinated with the State Cyber & Cryptography Agency (BSSN) and the Indonesian Ministry of Information.[34]

Threats in the use of digital data in general can be grouped into three types: data security, cybersecurity, and transaction security.[35] A crime often encountered in the fintech company sector is the theft of personal data. Suppose it is known that there is a crime of data leakage and data theft. In that case, the effort that the victim can take is to make a complaint to BSSN, the Ministry of Digital of the Republic of Indonesia, and can also report it to the cyber police.

---

[33] Utama, Purwoleksono, and Rachman, "Data Leakage of the Indonesian Elections Commission in Legal Aspects of Personal Data Protection."

[34] Juniar Laraswanda Umagapi, "Leak of Voter Data 2024," Brief Info of the Parliamentary Analysis Center of the Expertise Body of the House of Representatives of the Republic of Indonesia, http: //berkas.dpr.go.id/pusaka/files/info_singkat/Info%20Singkat-XV-23-I-P3DI-Desember-2023-2044.pdf (accessed March 20, 2024).

[35] Amiliya Handayani, "Legal Protection of Personal Data Theft in Fintech Lending Services against Cyber Security Threats in Indonesia," *Jurist-diction*, vol. 6, 2023, https://e-journal.unair.ac.id/JD.

The modus operandi that often occurs in data misuse is the spread of scampages and selling data to other parties to gain profits in the form of money. This can be seen as Decision Number 2575/Pid.Sus/2022/PN. Sby, the perpetrator, has prepared several members and trained them to use an application to spread scampages to credit card service users. The victim was affected by the link sent by the perpetrator, as it had been made as similar as possible to his official account. Perpetrators collect victim-specific data automatically and collectively. After the data is collected, they sell it online using cryptocurrency, then they exchange the money into a specific country's currency.

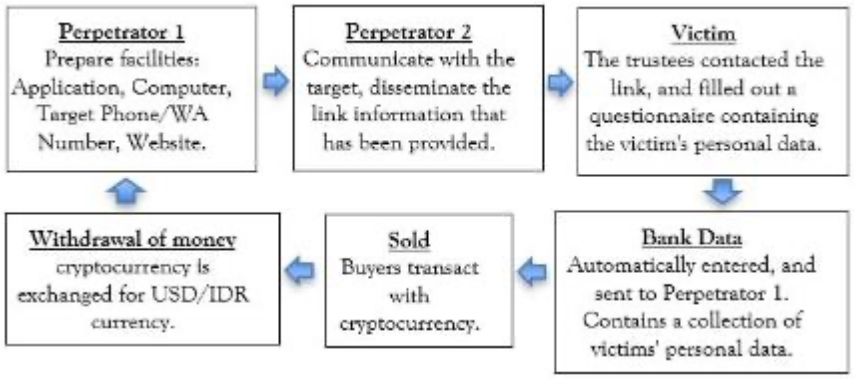

Figure 2. *Modus Operandi of Perpetrators of Personal Data Collection in the Private Sector, Source: Author Analysis* [36]

The juridical analysis in the provisions of Article 30 of the PDP Law has been regulated concerning the obligations attached to data controllers to prevent illegal access that leads to the leakage of personal data through the implementation of a data privacy security system. When connected to the incident of data leak cases experienced by the KPU RI as the controller of public data in the implementation of general elections in Indonesia, it has admitted that even though it has

[36] The results of the author's analysis are based on Decision Number 2575/Pid.Sus/2022/PN. Sby, dated February 17, 2023, explored legal considerations (ratio decidendi), witness statements, crown witnesses, and the defendant's confession that was revealed at trial.

used the Information Security Management System Standard in its data center as the IS Certificate 762126 as of February 10, 2022 to February 9, 2025, it turns out that the incident of voter data leakage still occurs.[37] This is because every system always has weaknesses with time and technological developments, so it needs to be updated and evaluated regularly.[38]

Furthermore, in the case of hackers who carry out illegal access and sale of data, in this case, it is necessary that, before the passage of the PDP Law, there is a legal rule of the ITE Law (Law Number 11 of 2008 concerning Information and Electronic Transactions). Article 30 paragraph (2) of the ITE Law regulates the prohibition for legal subjects (persons or corporations) who deliberately have illegal access to computers, electronic systems to obtain information and/or documents. More specifically, related to the data privacy law in Article 65 of the PDP Law, a prohibition associated with disclosing personal data that does not belong to the individual has been regulated.

In addition to the ITE Law, the derivative regulations are Government Regulation Number 71 of 2019 concerning implementing electronic systems and transactions. This is related to the state or government administrators providing information technology-based services and facilities to ensure security from all cybercrime threats. The philosophy of the regulation is to realize the protection of privacy, public freedom, and digital security while still upholding the democratic aspect in technological advances. However, the rules of the PDP Law have not yet been enacted.

Specifically, the provisions in the PDP Law related to the prohibition on the use of data are outlined in Chapter XIII and accompanied by criminal provisions in Chapter XIV.

---

[37] Decision Number 4-PKE-DKPP/I/2024 dated April 17, 2024.

[38] Utama, Purwoleksono, and Rachman, "Data Leakage of the Indonesian Elections Commission in Legal Aspects of Personal Data Protection."

TABLE 1. Criminal Prohibition & Sanctions Arrangements in the PDP Law

Prohibition Aspects	Criminal Sanctions
Unlawful	
Collecting other people's data for personal gain (Article 65 (1))	Imprisonment for a maximum of 5 years and/or a maximum fine of five billion rupiah (Article 67 (1))
Open someone else's data (Article 65 (2))	Imprisonment for a maximum of 4 years and/or a maximum fine of four billion rupiah (Article 67 (2))
Using data without permission (Article 65 (2))	Imprisonment for a maximum of 5 years and/or a maximum fine of five billion rupiah (Article 67 (3))
Creating false data that harms others (Article 66)	Imprisonment for a maximum of 5 years and/or a maximum fine of five billion rupiah (Article 68)

Sources: PDP Law

In reference to the PDP Law, criminal provisions provide criminal sanctions on individuals and corporations, and have even been regulated concerning additional criminal sanctions. In the provisions of the PDP Law, it is also known that there are additional criminal sanctions, namely in the form of confiscation of assets and/or assets obtained or the proceeds of criminal acts and payment of compensation (Article 69 of the PDP Law). The PDP Law is also equipped with corporate criminal instruments, as Article 70 of the PDP Law, with the provision that only a maximum fine of 10 (ten) times the maximum penalty can be imposed. Corporations can then

be subject to additional penalties by Article 70 (4) of the PDP Law, including:

a. Deprivation of profits from the proceeds of crime;
b. Freezing of its business (Wholly or partially);
c. Prohibition of carrying out activities (permanent);
d. Business closure (Partially or fully);
e. Performing negligent obligations;
f. Compensation;
g. Revocation of permits;
h. Dissolution.

There are types of administrative sanctions, namely: Written warning, temporary suspension of personal data processing activities, deletion/destruction of personal data, and administrative fines. The provision on administrative fines is a maximum of 2% of the annual income/revenue for the violation variable.

In connection with the existence of several legal rules that regulate the scope of misuse of information and/or electronic documents, as well as personal data, it is necessary to approach the principle of lex specialis derogat legi generalis in determining the legal rules that are most applicable to the subject matter. In general, this is used in situations where several legal rules have similar rules, so they can potentially cause a conflict of norms. The ITE and PDP laws have similar scopes and legal importance, namely in protecting electronic data against cybercrime. However, the PDP Law has specific regulations related to personal data protection, compared to the ITE Law, which regulates more generally. The categorization of a Lex specialist criminal act with Lex generalis in general can be seen from several indicators, including:[39]

[39] Adami Chazawi, Ardi Ferdian, *Tindak Pidana Informasi & Transaksi Elektronik Penyerangan terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik,* (Malang: Media Nusa Creative, Malang, 2015) p. 54.

a. The crime lex specialist not only has all the main elements in the criminal act, but also has one or several specific elements that are not found in the lex generalis;
b. Have a similar scope;
c. Equality of legal subjects;
d. Equality of the object of a crime;
e. There is a common legal interest;
f. The source of law between the lex specialist and the lex generalis must be equal (at the same level).

Specifically, the PDP Law has regulated systematically from the beginning of the collection to any use of personal data.[40]

B. Audit of Legal Compliance from the Perspective of Data Lex Spesialis

Data privacy can be classified as an economic item that must be protected. Efficiency and exchange of personal data information can provide added value for the interests of corporations and organizations, so they can be categorized as economic goods.[41] The datanomic phenomenon has had a significant influence globally due to the activities of digital application providers who collect data, conduct data analysis, and analyze data interaction actors from e-commerce platform users.[42] Even data is likened to new wealth that is more valuable than oil. That shows the importance of personal data protection during the development of digital dynamics in the Society 5.0 era.

---

[40] Romli, A.M., *Undang-Undang Perlindungan Data Pribadi dan Korporasi Pembahasan Isu -Isu Aktual Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi*, (Bandung: PT. Refika Aditama, 2023), p. 8.

[41] Smith, Jan, *Komputer: Suatu Tantangan Baru di Bidang Hukum*, (Surabaya: Airlangga University Press, 1991), p. 14.

[42] Budhijanto, Danrivanto, *Hukum Perlindugan Data Pribadi Di Indonesia Cyberlaw & Cybersecurity*, (Bandung: PT. Refika Aditama, 2023), p. 70.

Data security always involves a series of protection efforts to maintain data confidentiality, integrity, and access security, and protect against data theft crimes or illegal access to data in all data processing.[43] Each country has a legal instrument that guarantees explicitly the protection of data privacy sovereignty. However, there are still weaknesses in technical regulations and efforts to prevent data misuse. In addition, data protection is intended to guarantee the right to freedom of each individual to personal information, and to reduce the threat of misuse of information that can negatively impact the individual.[44]

The party that is the data controller must prevent illegal access or even unauthorised processing of personal data (Article 38 of the PDP Law). The controller of personal data is not limited to individuals but also includes public bodies and international organisations that control any processing of data. One form of privacy violation in e-commerce platforms is if a business actor, as the data controller, cannot maintain the confidentiality of the service user's data.[45] Personal data controllers must use a security system for personal data electronically with the principles of reliability, security, and responsibility (Article 39 (2) PDP Law).

Furthermore, as mandated by the provisions in Article (30) of the PDP Law, namely the obligation of data controllers to prevent the misuse of personal data through the use of security systems for data,

---

[43] Nur Adlin Hanisah Shahul Ikram, "Data Breaches Exit Strategy: A Comparative Analysis of Data Privacy Laws," *Malaysian Journal of Syariah and Law* 12, no. 1 (2024): 135–47, https://doi.org/10.33102/mjsl.vol12no1.458.

[44] Lyn E. Pleger, Katharina Guirguis, and Alexander Mertes, "Making Public Concerns Tangible: An Empirical Study of German and UK Citizens' Perception of Data Protection and Data Security," *Computers in Human Behavior* 122, no. February 2020 (2021): 106830, https://doi.org/10.1016/j.chb.2021.106830.

[45] Anita Sani, Joni Emirzon, and Annalisa Yahanan, "The Balance of Legal Protection Between Consumers and Business Actors," 2024, 302–18, https://doi.org/10.24843/JMHU.2024.v13.i0.

compliance audits must be carried out periodically. The purpose of the audit is to ensure the security of data and avoid sanctions for acts prohibited in the PDP Law. Please note that the things that are forbidden in the PDP Law include:

1. Unlawful collection and acquisition of data,
2. Unlawful disclosure,
3. Unlawful use of data,
4. Data falsification.

Preventing cyberattacks and obtaining a quality protection pattern through a robust legal compliance audit system prepared to add value and anticipate vulnerability risks is vital.[46] Continuous audits provide performance monitoring, especially regarding the suitability of target achievement strategies and juridical aspects. Collecting and processing collective data should be regularly evaluated and verified to update performance and systems, and prevent crimes against data privacy.

Good cybersecurity is built on collaboration between people, processes, and technology.[47] Concern for the importance of digital security must be carried out in conjunction with the technological infrastructure used. The active role of every element in the organisation is the best cyber defence. Risk compliance audits can provide a preventive and educational approach to improve cybersecurity.

Studies on the urgency of maintaining the confidentiality of personal information by internet users among households show that most of them are unaware of the potential threat of data leakage and the negative impact that will be experienced if criminals misuse the data.[48] People in general are aware that their data must be protected.

---

[46] Lois et al., "Internal Audits in the Digital Era: Opportunities Risks and Challenges."

[47] Akyuwen, Roberto, *Keamanan Siber Bank*, (Jakarta: Infobank Publishing, 2024), p. 294.

[48] Irina Maiorescu et al., "Intrusiveness And Data Protection In Iot Solutions For Smart Homes," *Amfiteatru Economic* 23, no. 57 (2021): 429–47, https://doi.org/10.24818/EA/2021/57/429.

Still, on the other hand, activities in cyberspace that are increasingly rapidly providing facilities and ease of life also pose a significant threat if they are not vigilant. Therefore, the role of the public and private sectors is always to provide the latest instruments to protect their private data.

The principle of transformation law is that the role of law is carried out in the context of order, certainty, and justice, and the function of law is as a transformation infrastructure.[49] The influence of information technology developments has encouraged cybercrime, which increasingly threatens data protection. Therefore, the approach pattern in legal compliance audits must also transform with the perspective of data lex specialis. Every internet-based service should pay attention to the urgency of data privacy as an interrelated relationship with the existence of human life as described by Phathetic Dot Theory, namely, four elements affect each other, including: law, market, social norms, and technological architecture.[50] Every digital service is not only influenced by telematics laws regulating activities in cyberspace but also by a market aspect, namely, every cost arising from its management to achieve the agreed completeness. In addition, social norms need to be considered in every service, such as the development of technology (architecture), which is related to using the latest and safest technology in these digital services.

[49] Ramli A.M., & Ramli T.S., *Hukum Sebagai Infrastruktur Transformasi Indonesia Regulasi dan Kebijakan Digital*, (Bandung: PT. Refika Aditama,2022), p. 86.

[50] Lessig, Lawrence., *Code and Other Laws of Cyberspace*, (New York: Basic Books, 1999), p. 87.

Figure 3. Challenges of Personal Data Protection in Digital Services, Source: Author[51]

Audits of legal compliance in data privacy must also pay attention to those related to data transfer activities. Personal data controllers must pay attention to the existence of elements of consent (Article 56 paragraph (4) of the PDP Law), contractual obligations (Article 56 paragraph (3) of the PDP Law), and equality (Article 56 paragraph 92 of the PDP Law). Before transferring or sharing data with third parties, it is necessary to ensure compliance audits to prevent data leakage and apply data privacy principles. In realizing proportional data transfer, it is essential to pay attention to, among others:

1. Data encryption and pseudonymization,
2. Certainty in the ability to maintain confidentiality, system resilience, and services,
3. Recovery in provision and access to data on time in the event of technical negligence,
4. The process of evaluating an organization for technical activities in data processing.

In an independent service test, a legal compliance audit can begin by digging up information related to the legal subject of personal data controllers required in the PDP Law. That is done to determine whether the subject of the law is a necessary party in the PDP Law. Testing materials that need to be considered in determining the correlation between data controller subjects and obligations under the PDP Law include:

1. Forms of entities (individuals, corporations),
2. Location of jurisdictional activities (jurisdictional aspect),
3. Data-related activities (collection, processing, storage, correction, deletion, dissemination),
4. Purposes in data processing (data control),

[51] The author's analysis uses the *Pathetic Dot Theory* analogy in the personal data protection perspective approach.

5. Form data in processing,
6. Categorization in data controllers.

Mitigation efforts for personal data leaks can be studied in the case of KPU RI data leaks as a form of corrective measures. After obtaining information on the voter data leakage incident, the KPU RI held a coordination meeting with the Cybersecurity Task Force Team.[52] Steps taken in efforts to mitigate data leaks include:[53]

1. The aspect of the application development, namely closing vulnerability gaps, consists of access logs, firewall logs, and all changes and feature additions;
2. The aspect of the network and infrastructure. Namely, by strengthening measures through the addition of security devices on all networks, consisting of data centers on-premise and cloud, as well as on the network of user devices;
3. The aspect of human resources (HR) management, namely, improvements in user management and the implementation of a strict information security management system. That is because almost all of these applications always involve many users.

The basis for processing personal data must be the main guideline for realizing digital security (as in Article 20, paragraph 2 of the PDP Law), including:

1. The existence of lawful (explicit) consent for any specific purpose of the personal data subject;
2. Fulfillment of contractual obligations in terms of the subject of personal data as a party to an agreement;
3. Fulfillment of legal obligations from personal data controllers by regulations;
4. Protection of the vital interests of personal data subjects;

[52] Decision Number 4-PKE-DKPP/I/2024 dated April 17, 2024.
[53] Ibid.

5. Implementation of duties in public services, public interest, or exercise of data controller authority by applicable legal rules;
6. The fulfillment of legitimate interests by paying attention to the aspects of the purpose, needs, and balance between the rights of the controller of personal data and the subject of personal data.

The urgency of data privacy audits in the supervision of responsible data collection systems has become a serious concern to ensure that the rule of law is used in databases and is not used unlawfully for the benefit of other parties.[54] A data privacy audit is a reasonable effort from personal data controllers to ensure cybersecurity in personal data protection. The biggest obstacle in personal data auditing is the lack of clarity regarding legal audit standards for personal data protection, so that each digital service provider can implement audit guidelines that vary according to the agency's needs. However, a reference is given by the Financial Services Authority (OJK) in the Cybersecurity Guidelines for Financial Sector Technology Innovation Providers as the Financial Services Authority (POJK) Regulation Number 3 of 2004.[55] The implementation of a cybersecurity framework can be a mechanism to minimize threats to the aspects of availability, integrity, and confidentiality of data and information processed electronically by operators. In carrying out operational activities, each organizer must pay attention to data protection aspects, namely:[56]

---

[54] Eglė Kavoliūnaitė-Ragauskienė, "Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union," *Journal of Human Rights Practice* 16, no. 2 (2024): 658–74, https://doi.org/10.1093/jhuman/huad065.

[55] Otoritas Jasa Keuangan, *Pedoman Keamanan Siber Bagi Penyelenggara ITSK*, (Jakarta: Kelompok Spesialis Layanan Digital dan Keamanan Siber (KSLK), 2021), p. 10.

[56] Ibid, p. 104.

1. Implementation of adequate data extraction protocols to protect sensitive financial information both in transit and in storage;
2. Implementation of strict access control and data preparation security to protect data from unauthorized access;
3. Drafting and enforcing comprehensive data retention and destruction policies following applicable legal and regulatory requirements.

Conclusion

The establishment of a legal compliance audit regime based on Article 29 of the PDP Law will ensure accountability in the perspective of personal data protection that can be enforced by privacy data supervisory officers. The era of data digitization in the development of society 5.0 has made data a key commodity across the public and private sectors. In implementing the PDP Law, it is necessary to support strategic and more specific technical supervision. The protection of user data privacy must keep pace with the growing needs of digital services. A PDP (Data Privacy Audit) compliance audit can be an effective way to oversee the use of personal data.

The preparation of new implementing regulations must set clear, specific legal requirements for institutional authority and compliance audit standards in the digital data era. Compliance Audit 5.0 is not only a manifestation of the obligation of personal data controllers to act in good faith in protecting data, but also a mitigation measure against the risk of data leakage. It is necessary to improve the PDP Law, namely, by implementing rules related to the obligations of personal data controllers, specifically, and regulations regarding PDP audits. This audit is necessary to increase oversight of all data controllers in the private and public sectors to ensure digital services are delivered safely and proportionately.

References

Books

Adami Chazawi, Ardi Ferdian, Tindak Pidana Informasi & Transaksi Elektronik Penyerangan terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik, (Malang: Media Nusa Creative, Malang, 2015)

Akyuwen, Roberto, Keamanan Siber Bank, (Jakarta: Infobank Publishing, 2024)

Budhijanto, Danrivanto, Hukum Perlindugan Data Pribadi Di Indonesia Cyberlaw & Cybersecurity, (Bandung: PT. Refika Aditama, 2023)

Kania, Aisha Pasaman, et al, Indonesia Gen Z Report 2024 Understanding and Uncovering the Behavior, Challenges, and Opportunities (IDN Media, 2024)

Lessig, Lawrence., Code and Other Laws of Cyberspace, (New York: Basic Books, 1999)

Marzuki, Peter Mahmud, Penelitian Hukum Edisi Revisi, (Jakarta: Kencana Predana Media Group, 2021)

Otoritas Jasa Keuangan, Pedoman Keamanan Siber Bagi Penyelenggara ITSK, (Jakarta: Kelompok Spesialis Layanan Digital dan Keamanan Siber (KSLK), 2021)

Ramli A.M., & Ramli T.S., Hukum Sebagai Infrastruktur Transformasi Indonesia Regulasi dan Kebijakan Digital, (Bandung: PT. Refika Aditama,2022)

Romli, A.M., Undang-Undang Perlindungan Data Pribadi dan Korporasi Pembahasan Isu -Isu Aktual Undang-Undang Nomor 27 tahun 2022 tentang Perlindungan Data Pribadi, (Bandung: PT. Refika Aditama, 2023)

Smith, Jan, Komputer: Suatu Tantangan Baru di Bidang Hukum, (Surabaya: Airlangga University Press, 1991)

Journals

Adebowale, Moruf Akin, Khin T. Lwin, and M. A. Hossain. “Intelligent Phishing Detection Scheme Using Deep Learning Algorithms.” Journal of Enterprise Information Management 36, no. 3 (April 24, 2023): 747–66. https://doi.org/10.1108/JEIM-01-2020-0036.

Aidonojie, Paul Atagamen, Toyin Afolabi Majekodunmi, Obieshi Eregbuonye, and Isaac Ottah Ogbemudia. “Legal Issues Concerning of Data Security and Privacy in Automated Income

Tax Systems in Nigeria." Hang Tuah Law Journal 8, no. 1 (2024): 14–41. https://doi.org/10.30649/htlj.v8i1.223.

Alfawzan, Najd, Markus Christen, Giovanni Spitale, and Nikola Biller-Andorno. "Privacy, Data Sharing, and Data Security Policies of Women's MHealth Apps: Scoping Review and Content Analysis." JMIR MHealth and UHealth 10, no. 5 (2022). https://doi.org/10.2196/33735.

Althabhawi, Nabeel Mahdi, Zinatul Ashiqin Zainol, and Parviz Bagheri. "Society 5.0: A New Challenge to Legal Norms." Sriwijaya Law Review 6, no. 1 (2022): 41–54. https://doi.org/10.28946/slrev.Vol6.Iss1.1415.pp41-54.

Baik, Jeeyun (Sophia). "Data Privacy against Innovation or against Discrimination?: The Case of the California Consumer Privacy Act (CCPA)." Telematics and Informatics 52 (September 1, 2020). https://doi.org/10.1016/j.tele.2020.101431.

Balachandar, V., and K. Venkatesh. "Privacy-Enhanced Secure Framework for Educational Data Protection and Analysis." International Journal of Information Technology (Singapore) 17, no. 5 (2025): 2887–2904. https://doi.org/10.1007/s41870-025-02458-4.

Bolton, Tom, Tooska Dargahi, Sana Belguith, Mabrook S. Al-Rakhami, and Ali Hassan Sodhro. "On the Security and Privacy Challenges of Virtual Assistants." Sensors 21, no. 7 (2021): 1–19. https://doi.org/10.3390/s21072312.

Budiartha, I Nyoman Putu, I Made Pria Dharsana, and Indrasari Kresnadjaja. "Penguatan Konstruksi Hukum Perihal Perlindungan Data Pribadi." Jurnal Magister Hukum Udayana 12, no. 1 (2023): 56–65. https://doi.org/10.24843/JMHU.2023.v12.i0 1.p05.

Chen, Yu Chen, Jiann Liang Chen, and Yi Wei Ma. "AI@TSS-Intelligent Technical Support Scam Detection System." Journal of Information Security and Applications 61 (September 1, 2021). https://doi.org/10.1016/j.jisa.2021.102921.

Gill, Sajid Habib, Mirza Abdur Razzaq, Muneer Ahmad, Fahad M. Almansour, Ikram Ul Haq, Nz Jhanjhi, Malik Zaib Alam, and Mehedi Masud. "Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study." Intelligent Automation and Soft Computing 31, no. 1 (2022): 117–28. https://doi.org/10.32604/IASC.2022.016597.

Handayani, Amiliya. "Perlindungan Hukum Terhadap Tindakan Pencurian Data Pribadi Pada Layanan Fintech Lending Atas Ancaman Cyber Security Di Indonesia." Jurist-Diction 6, no. 4 (October 1, 2023): 605–30. https://doi.org/10.20473/jd.v6i4.51212.

Humayun, Mamoona, N. Z. Jhanjhi, Ahmed Alsayat, and Vasaki Ponnusamy. "Internet of Things and Ransomware: Evolution, Mitigation and Prevention." Egyptian Informatics Journal. Elsevier B.V., March 1, 2021. https://doi.org/10.1016/j.eij.2020.05.003.

Kavoliūnaitė-Ragauskienė, Eglė. "Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union." Journal of Human Rights Practice 16, no. 2 (2024): 658–74. https://doi.org/10.1093/jhuman/huad065.

Lee, In. "Cybersecurity: Risk Management Framework and Investment Cost Analysis." Business Horizons 64, no. 5 (2021): 659–71. https://doi.org/10.1016/j.bushor.2021.02.022.

Lei, Jian, Quanwang Wu, and Jin Xu. "Privacy and Security-Aware Workflow Scheduling in a Hybrid Cloud." Future Generation Computer Systems 131 (2022): 269–78. https://doi.org/10.1016/j.future.2022.01.018.

Lois, Petros, George Drogalas, Alkiviadis Karagiorgos, and Kostantinos Tsikalakis. "Internal Audits in the Digital Era: Opportunities Risks and Challenges." EuroMed Journal of Business 15, no. 2 (June 22, 2020): 205–17. https://doi.org/10.1108/EMJB-07-2019-0097.

Maiorescu, Irina, Larisa Gabudeanu, Alexandru Lucian Vîlcea, Gabriel Cristian Sabou, and Marian Dârdală. "Intrusiveness And Data Protection In Iot Solutions For Smart Homes." Amfiteatru Economic 23, no. 57 (2021): 429–47. https://doi.org/10.24818/EA/2021/57/429.

Marzuki, Peter Machmudz. "The Essence of Legal Research Is to Resolve Legal Problems." Yuridika 37, no. 1 (March 1, 2022): 37–58. https://doi.org/10.20473/ydk.v37i1.34597.

Peter, Dede Ibiere, and Ben Collin Emeka Ndinojuo. "Privacy Awareness and Social Media: Personal Data Protection among Facebook** and Instagram** Users." Galactica Media: Journal of Media Studies 6, no. 3 (2024): 168–98. https://doi.org/10.46539/gmd.v6i3.489.

Pleger, Lyn E., Katharina Guirguis, and Alexander Mertes. "Making Public Concerns Tangible: An Empirical Study of German and UK Citizens' Perception of Data Protection and Data Security." Computers in Human Behavior 122, no. February 2020 (2021): 106830. https://doi.org/10.1016/j.chb.2021.106830.

Ramli, Tasya Safiranita, Ahmad M. Ramli, Huala Adolf, Eddy Damian, and Miranda Risang Ayu Palar. "Over-the-Top Media in Digital Economy and Society 5.0." Journal of Telecommunications and the Digital Economy 8, no. 3 (2020): 60–67. https://doi.org/10.18080/jtde.v8n3.241.

Romansky, Radi P., and Irina S. Noninska. "Challenges of the Digital Age for Privacy and Personal Data Protection." Mathematical Biosciences and Engineering 17, no. 5 (August 10, 2020): 5288–5303. https://doi.org/10.3934/MBE.2020286.

Sani, Anita, Joni Emirzon, and Annalisa Yahanan. "Keseimbangan Perlindungan Hukum Antara Konsumen Dan Pelaku Usaha." Jurnal Magister Hukum Udayana 13, no. 2 (2024): 302–18. https://doi.org/10.24843/JMHU.2024.v13.i0.

Shahul Ikram, Nur Adlin Hanisah. "Data Breaches Exit Strategy: A Comparative Analysis of Data Privacy Laws." Malaysian Journal of Syariah and Law 12, no. 1 (2024): 135–47. https://doi.org/10.33102/mjsl.vol12no1.458.

Supriyadi, Daniar. "The Regulation of Personal and Non-Personal Data in the Context of Big Data." Journal of Human Rights, Culture and Legal System 3, no. 1 (2023): 33–69. https://doi.org/10.53955/jhcls.v3i1.71.

Tao, Lei, Jinhan Wan, and Bo Wen. "The Effects of Artificial Intelligence and Victims' Deservingness Information on Citizens' Blame Attribution towards Administrative Errors." Public Management Review 27, no. 12 (2025): 3104–24. https://doi.org/10.1080/14719037.2024.2411632.

Tsohou, Aggeliki, Emmanouil Magkos, Haralambos Mouratidis, George Chrysoloras, Luca Piras, Michalis Pavlidis, Julien Debussche, Marco Rotoloni, and Beatriz Gallego-Nicasio Crespo. "Privacy, Security, Legal and Technology Acceptance Elicited and Consolidated Requirements for a GDPR Compliance Platform." Information and Computer Security 28, no. 4 (October 1, 2020): 531–53. https://doi.org/10.1108/ICS-01-2020-0002.

Utama, Frendika Suda, Didik Endro Purwoleksono, and Taufik Rachman. "Data Leakage of the Indonesian Elections Commission in Legal Aspects of Personal Data Protection." Media Iuris 7, no. 3 (2024): 479–98. https://doi.org/10.20473/mi.v7i3.55931.

Xu, Yao, Jixin Wei, Ting Mi, and Zhihua Chen. "Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics." World Electric Vehicle Journal 16, no. 1 (2025): 1–27. https://doi.org/10.3390/wevj16010006.

Zhanbayev, Rinat A., Muhammad Irfan, Anna V. Shutaleva, Daniil G. Maksimov, Rimma Abdykadyrkyzy, and Şahin Filiz. "Demoethical Model of Sustainable Development of Society: A Roadmap towards Digital Transformation." Sustainability (Switzerland) 15, no. 16 (2023): 1–25. https://doi.org/10.3390/su151612478.

Website

Indonesian Internet Service Providers Association, "Indonesian Internet Penetration Survey 2024", Indonesian Internet Service Providers Association, http://survei.apjii.or.id (accessed March 21, 2025)

International Telecomunication Union, "Global Cybersecurity Index 2020", ITU Publications, http:// www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (accessed March 21, 2025)

Juniar Laraswanda Umagapi, "Leak of Voter Data 2024," Brief Info of the Parliamentary Analysis Center of the Expertise Body of the House of Representatives of the Republic of Indonesia, http: //berkas.dpr.go.id/pusaka/files/info_singkat/Info%20Singkat-XV-23-I-P3DI-Desember-2023-2044.pdf (accessed March 20, 2025).

Regulation Legislation and Other Sources of Law

Law Number 11 of 2008 concerning Electronic Information and Transactions (Indonesian State Gazette Year 2008 Number 58, Additional of Indonesian State Gazette Number 4843)

Law Number 27 of 2022 concerning Personal Data Protection (Indonesian State Gazette Year 2022 Number 196, Additional of Indonesian State Gazette Number 6820)

Decision Number 2575/Pid.Sus/2022/PN. Sby, dated February 17,

2023
Decision Number 4-PKE-DKPP/I/2024 dated April 17, 2024.