Justicia Islamica: Jurnal Kajian Hukum dan Sosial
Vol 22 No 1, June 2025

The Legal Responsibility of the General Elections Commission in the 2024 Election Data Leak: Integration of Personal Data Protection Laws and the Principle of *Sadd al-Dharī'at*

Siti Nur Syifa,[1*] Muhammad Torieq Abdillah,[2] Fadil SJ[3]
[1,3] Postgraduate UIN Maulana Malik Ibrahim Malang, Indonesia
[2] Faculty of Sharia, UIN Antasari Banjarmasin, Indonesia
Email: [1]snrsyf17@gmail.com, [2]mtabdillah11@gmail.com, [3]fadilsj@syariah.uin-malang.ac.id

**Corresponding Author*

DOI: 10.21154/justicia.v22i1.10390

Received: April 10, 2025	*Revised: May 26, 2025*	*Approved: June 4, 2025*

Abstract: Indonesia's transition to digital governance has amplified the urgency of personal data protection, especially following the 2024 General Election data leaks, which exposed over 204 million voter records. This study investigates the legal responsibility of the General Election Commission (KPU), as the institution mandated to organize general elections, under Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) and Islamic legal doctrine, particularly the principle of *sadd al-dharī'at* (preventing harm). This study uses normative legal research methods with statutory, conceptual, and comparative approaches. The study analyzes primary legal materials and comparative frameworks such as the General Data Protection Regulation (GDPR). The findings reveal that despite UU PDP's existence, implementation remains weak due to inadequate digital infrastructure and limited institutional accountability. The research highlights a dual legal gap: insufficient positive law enforcement and underutilization of preventive Islamic principles. The novelty of this study lies in integrating *sadd al-dharī'at* with UU PDP to offer a preventive legal solution that strengthens institutional data security. The implication suggests the urgency of harmonizing regulatory frameworks and enhancing legal awareness within electoral institutions to ensure public trust and uphold digital democracy.

Keywords: personal data protection; KPU; *sadd al-dharī'at*.

Abstrak: Transisi Indonesia menuju tata kelola pemerintahan digital telah meningkatkan urgensi perlindungan data pribadi, terutama setelah kebocoran data Pemilu 2024 yang mengekspos lebih dari 204 juta data pemilih. Penelitian ini mengkaji tanggung jawab hukum Komisi Pemilihan Umum (KPU), sebagai lembaga yang diberi mandat untuk menyelenggarakan pemilihan umum, berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) serta doktrin hukum Islam, khususnya prinsip *sadd al-dharī'at* (pencegahan terhadap

kerusakan). Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif, serta menganalisis bahan hukum primer dan kerangka perbandingan seperti General Data Protection Regulation (GDPR). Temuan menunjukkan bahwa meskipun UU PDP telah berlaku, implementasinya masih lemah akibat infrastruktur digital yang belum memadai dan rendahnya akuntabilitas kelembagaan. Penelitian ini menyoroti adanya dualisme kekosongan hukum: lemahnya penegakan hukum positif dan kurang dimanfaatkannya prinsip-prinsip preventif dalam hukum Islam. Kebaruan dari penelitian ini terletak pada integrasi antara *sadd al-dharī'at* dan UU PDP untuk menawarkan solusi hukum preventif yang memperkuat keamanan data kelembagaan. Implikasinya menunjukkan perlunya harmonisasi kerangka regulasi serta peningkatan kesadaran hukum dalam tubuh lembaga pemilu untuk menjaga kepercayaan publik dan menegakkan demokrasi digital.

Kata Kunci: perlindungan data pribadi; KPU; *sadd al-dharī'at*.

Introduction

The era of disruption in the Industrial Revolution 4.0 is driving the shift to digital, with technology influencing all aspects of life. According to the Minister of Communication and Digital Republic of Indonesia, Meutya Hafid, Indonesia is among the most active countries in terms of internet usage. As of 2025, approximately 79.5% of the population, equivalent to over 221 million people, are reported to be internet users.[1] The Internet has positive impacts, such as advances in communication, business efficiency, and online education, but it also presents cyber threats. Personal data leaks can occur due to negligence of the owner or institution, opening up opportunities for crimes such as data leaks, account hacking, and information trading, which threaten the digital security of society.[2]

In the contemporary digital era, the importance of cybersecurity has increased sharply, and it has become an important aspect of organizational strategy and national security.[3] One of the factors that triggers this is the increase in misuse of

[1] Josua Sihombing, "Menkomdigi: Indonesia Pengguna Internet Terbesar Di Dunia," rri.co.id - Portal berita terpercaya, accessed May 20, 2025, https://www.rri.co.id/.

[2] Putri Hasian Silalahi and Fiorella Angella Dameria, "Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional," *Wajah Hukum* 7, no. 2 (2023): 2–7, http://dx.doi.org/10.33087/wjh.v7i2.1244.

[3] Temitayo Oluwaseun Abrahams et al., "A Review of Cybersecurity Strategies in Modern Organizations: Examining the Evolution and Effectiveness of Cybersecurity Measures for Data Protection," *Computer Science & IT Research Journal* 5, no. 1 (January 9, 2024): 1–25, https://doi.org/10.51594/csitrj.v5i1.699.

personal data, such as data trading, account embezzlement, and data leaks that lead to fraud. The urgency of protecting personal data is increasingly important, closely related to privacy, as an effort to maintain the integrity and dignity of individuals from the threat of digital crime.[4]

The concept of personal data protection has been stipulated in Article 28G of the 1945 Constitution (UUD 1945), "Every person shall have the right to protection of their self, family, honor, dignity, and property under their control, and shall have the right to feel secure and protected from threats of fear to do or not do something that constitutes a human right." Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) also requires every data user institution, including the General Elections Commission (KPU), to protect people's data. The KPU is required to ensure data confidentiality while applying the principle of transparency in the processing of election data so that the data remains securely accessible to the public.

In the 2024 Election, there was a voter data leak. There are around 204 million permanent voter lists (*daftar pemilih tetap*; DPT) that were leaked, including population registration numbers (NIK), identity card numbers (KTP), and so on.[5] Personal data leaks seriously impact public trust in the KPU and threaten digital security during elections. The KPU must improve personal data protection by complying with relevant regulations to prevent incidents such as data leaks or misuse that can harm the public and the democratic process. Reflecting on this problem, efforts are needed to protect personal data at the KPU, which are reviewed from two perspectives, namely the positive legal view regarding data protection at the KPU based on UU PDP and *sadd al-dharī'at* review of data leaks at the KPU.

Previous studies relevant to this topic include research by Miftahul Heldra Sandiza et al., entitled "Towards Personal Data Protection in Structural Leadership Training: An Analysis of Maqāshid al-Sharī'ah Perspective," which was published in December 2024. This article examines the application of the *maqāṣid al-sharī'at* approach to personal data protection in the context of structural leadership training. Islamic legal principles serve as a foundation for understanding and implementing data protection in this setting. The findings indicate that effective data protection requires strict policies, adequate security technology, staff training, and increased

---

4 Erlina Maria Christin Sinaga and Mery Christian Putri, "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (2020): 238–39, https://dx.doi.org/10.33331/rechtsvinding.v9i2.428.

5 Setjen DPR RI, "204 Juta DPT Pemilu Bocor, Sukamta Ingatkan KPU Tindaklanjuti Secara Serius," accessed April 30, 2024, http://www.dpr.go.id/berita/.

awareness. Additionally, the role of a data protection officer is essential to ensure the security of participants' data. This study contributes to strengthening data governance by integrating the values of *maqāṣid al-sharī'at*.[6]

Next, research by Sheila Kusuma Wardani Amnesti et al., entitled "Legal Protection of Personal Data Security in Indonesian Local Government Apps: Al Farabi's Perspective," was published in October 2024. This study aims to examine the implementation of the JAKI SuperApp by the DKI Jakarta Provincial Government, focusing on its role in public service delivery and data security. The findings show that JAKI complies with ISO 27001 standards, ensuring the confidentiality, integrity, and availability of data. The study also highlights the importance of shared responsibility between citizens and the government in managing personal data, reflecting Al-Farabi's concept of ethical information accountability.[7]

Then, research by Erwin Asmadi et al., which was published in November 2024, entitled "Data Theft and the Law on Protection of Personal Data: A Thematic Analysis." This article discusses the effectiveness of Law Number 27 of 2022 (UU PDP) in addressing data theft and leaks of personal information in Indonesia. Although the law stipulates criminal sanctions, its enforcement still faces various obstacles, such as limited institutional capacity, low public awareness, weak inter-agency coordination, and technological challenges. The study employs a qualitative approach with thematic analysis to assess the implementation and legal challenges of personal data protection in Indonesia.[8]

Finally, research by Lia Sautunnida et al. was published in 2025, entitled "Dispute Resolution Mechanisms in Personal Data Leakages: An Analysis of OJK's Role and Functions in Indonesia." This study examines the role and effectiveness of the Indonesian Financial Services Authority (OJK) in protecting the personal data of customers in the financial industry. Despite existing regulations and policies, data leaks continue to occur frequently. The findings indicate that the OJK has not been able to effectively address personal data violations. Therefore, it is recommended

---

6 Miftahul Heldra Sandiza, Sinta Dewi Rosadi, and Rahmat Suparman, "Towards Personal Data Protection in Structural Leadership Training: An Analysis of Maqāshid al-Sharī'ah Perspective," *Mazahib* 23, no. 2 (December 23, 2024): 631–68, https://doi.org/10.21093/mj.v23i2.8986.

7 Sheila Kusuma Wardani Amnesti, Siti Zulaichah, and Nurul Istiqomah, "Legal Protection of Personal Data Security in Indonesian Local Government Apps: Al Farabi's Perspective," *Legality: Jurnal Ilmiah Hukum* 33, no. 1 (2025): 1–19, https://doi.org/10.22219/ljih.v33i1.34623.

8 Erwin Asmadi et al., "Data Theft and the Law on Protection of Personal Data: A Thematic Analysis," *Jurnal Hukum Novelty* 15, no. 2 (November 2, 2024): 268–85, https://doi.org/10.26555/jhn.v15i2.27661.

that OJK Regulation No. 77/POJK.01/2016 be revised, as it is no longer compatible with current developments in financial technology.[9]

All of these studies discuss the topic of personal data leaks and have been published in reputable journals. Although they share a similar research focus, only one article specifically addresses personal data protection within government institutions.[10] The others primarily explore how personal data protection can be implemented through various approaches. Furthermore, this research is important considering that as many as 252 million voter registration data records for Indonesia's 2024 general election at the KPU were leaked and sold due to a cyberattack.[11] But after filtering to eliminate duplicates, approximately 204,807,203 unique data entries were identified, almost equivalent to the number of registered voters at the KPU's DPT, which comprises 204,807,222 voters from 514 regencies/municipalities across Indonesia, and 128 overseas representative offices were leaked.[12]

As of June 2024, the population of Indonesia is estimated to be 281 million, according to data from the Central Statistics Agency (Badan Pusat Statistik).[13] This means that 72.6% of Indonesia's population data has been widely exposed due to the data leaks. Other studies typically focus on a single approach, either positive law or Islamic law. This study contributes by focusing on the newly enacted UU PDP as a legal material of the research as positive law and Islamic law through the *sadd al-dharī'at* concept, which shares common ground as forms of preventive measures.

This research is a normative legal research that places law as a normative system.[14] Another term for normative legal research is doctrinal or theoretical legal research, which focuses on the question, "What is the applicable law?" In normative legal research, the researcher collects and analyzes relevant regulations or a body of

---

9 Lia Sautunnida, Izura Masdina Mohamed Zakri, and Faisal Ahmadi, "Dispute Resolution Mechanisms in Personal Data Leakages: An Analysis of OJK's Role and Functions in Indonesia," *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 9, no. 1 (January 15, 2025): 23–44, https://doi.org/10.22373/sjhk.v9i1.21102.

10 Umarwan Sutopo, Achmad Hasan Basri, and Hilman Rosyidi, "Presidential Threshold in the 2024 Presidential Elections: Implications for the Benefits of Democracy in Indonesia," *Justicia Islamica* 21, no. 1 (June 25, 2024): 155–78, https://doi.org/10.21154/justicia.v21i1.7577.

11 "252 Juta Data DPT Pemilu 2024 Bocor, Apa Tanggapan KPU dan Menkominfo? | tempo.co," Tempo, November 30, 2023, https://www.tempo.co/politik/.

12 Okezone, "Heboh Situs KPU Dibobol, 204 Juta Data DPT Bocor Dijual Peretas Miliaran Rupiah : Okezone Nasional," https://nasional.okezone.com/, November 28, 2023, https://nasional.okezone.com/read/2023/

13 Badan Pusat Statistik Indonesia, "Jumlah Penduduk Pertengahan Tahun - Tabel Statistik," accessed May 22, 2025, https://www.bps.go.id/id/statistics-table/.

14 Mukti Fajar and Yulianto Ahmad, *Dualisme Penelitian Hukum Normatif Dan Hukum Empiris* (Yogyakarta: Pustaka Pelajar, 2010), 34.

court decisions. The main objective of normative legal research is to explain and describe the content of the law and how it is applied.[15] The approach used in this research is the statutory approach, which examines laws and regulations related to the legal issues being discussed (researched),[16] the conceptual approach, which starts from the views and doctrines that develop in legal science, and the comparative approach. The research approach was chosen to find answers to legal issues in legal research.[17] The view used in this research is *sadd al-dharī'at* as part of Islamic law doctrine.

In this normative legal research, the legal materials that are the focus of the study are primary legal materials, namely Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), along with *sadd al-dharī'at*, plus other secondary legal materials in the form of scientific articles and books related to the discussion. The researcher conducted a comparative analysis using a content analysis approach. This method emphasizes an integrative and conceptual framework, with the primary aim of identifying, recognizing, processing, and evaluating legal sources to gain a deeper understanding of their meaning, significance, and relevance.[18]

Ius Constitutum in the Context of Personal Data Protection

Based on the time of its validity, the law is divided into two, namely *ius constitutum* and *ius constituendum*. *Ius constitutum* is a positive law that refers to the regulations that apply in a country during a certain period. For example, *ius constitutum* Indonesia covers the current Indonesian legal system, also known as the Indonesian legal system.[19] This means that *ius constitutum* is a regulation that is currently in force because it was previously *ius constituendum*. *Ius constituendum* is a law that aspires to be in the state's life but has not yet been formed into a law or other regulation.[20]

In Indonesia, *ius constitutum* is also called positive law, for example, the Civil Code (KUHPerdata), the Criminal Code (KUHPidana), and all laws currently in force based on the order of laws and regulations regulated in Law Number 12 of

---

15 Ian Dobinson and Francis Johns, "Qualitative Legal Research," in *Research Methods for Law* (Edinburgh: Edinburgh University Press, 2007), 19.

16 Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Press, 2020), 56.

17 Muhaimin, 57.

18 Burhan Bungin, *Metodologi Penelitian Kualitatif: Aktualisasi Metodologis Ke Arah Ragam Varian Kontemporer* (Jakarta: Rajawali Press, 2017), 203.

19 M. Ruhly Kesuma Dinata, *Ilmu Hukum* (Kotabumi: Sai Wawai Publishing, 2019), 18.

20 Bernadetha Aurelia Oktavira and Hukumonline, "Arti Ius Constitutum dan Ius Constituendum," July 7, 2018, https://www.hukumonline.com/klinik/

2011 concerning the Formation of Legislation (UU Pembentukan Peraturan Perundang-Undangan). Meanwhile, *ius constituendum* has not yet become a rule in formal form (law or other form), so in simple terms, it is a law that is still being aspired to, usually in the form of a concept or draft.[21]

The personal data protection policy in Indonesia is outlined in the Personal Data Protection Law (UU PDP), which was enacted during the 5th Plenary Session of the First Session of 2022–2023. This law consists of 16 chapters and 76 articles that regulate the rights of data subjects, the obligations of data controllers and processors, as well as provisions concerning regulatory institutions, including prohibitions and sanctions. A key provision of this law is the placement of the implementing agency under the President, in the form of a Non-Ministerial Government Institution. Further details regarding this institution are to be regulated by a Presidential Regulation. However, this placement has raised concerns regarding the effectiveness of its oversight. In both the public and private sectors, data protection efforts ideally require supervision by an independent authority to ensure objective transparency.[22]

From a technical perspective, the formulation of the UU PDP underwent a lengthy process. The initial draft of the law was introduced in 2016 with 72 articles. In 2019, harmonization and finalization were conducted among relevant ministries and institutions, resulting in the addition of four articles. In 2020, the President assigned the Ministry of Communication and Informatics, the Ministry of Home Affairs, and the Ministry of Law and Human Rights to engage in discussions with the House of Representatives. In 2021, further deliberations focused on key articles by considering global developments. Ultimately, the UU PDP was enacted and came into effect in Indonesia in 2022.[23]

Sadd al-Dharī'at in the Context of Personal Data Protection

Uṣul fiqh is a science that studies the global evidence of *shara'* and general rules used by *mujtahid* to derive shariah law related to human deeds, accompanied by detailed evidence. The objects of study in *uṣul fiqh* are divided into three, namely the sources and evidence of sharia law, sharia law contained in the evidence, and the rules of

---

21 Tami Rusli, *Pengantar Ilmu Hukum* (Lampung: Universitas Bandar Lampung (UBL) Press, 2017), 64–65.

22 Kiki Rezki Ramadhan and Chandra Wijaya, "The Challenges of Personal Data Protection Policy in Indonesia: Lesson Learned from the European Union, Singapore, and Malaysia," *Technium Social Sciences Journal* 36 (2022): 25.

23 Elfian Fauzy and Nabila Alif Radika Shandy, "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi," *Lex Renaissance* 7, no. 3 (2022): 458.

uṣūliyyat and the method of *istinbāṭ* of sharia law, including *qiyās, istiḥsān, istiṣḥāb, 'urf, maṣlaḥah mursalat,* and *sadd al-dharī'at.*

Sadd al-dharī'at linguistically means a path leading to something, good or bad, *ḥissī* or *maʿnawī*. To place it in a discussion that is by the purpose, the word *dharī'at* is preceded by *saddu,* which means to close, intended to close the path to damage. More broadly, the primary intended act is a prohibited act, so its *wasīlat* is called *dharī'at*. Because we must stay away from prohibited actions, including *wasīlat*, the discussion here is about efforts to stay away from *wasīlat* to avoid the main banned actions.[24] The urgency of *sadd al-dharī'at* is that all dangers are eliminated to achieve benefits and realize the goals of *syarī'at*.

According to al-Shāṭhibī, *sadd al-dharī'at* is divided into four parts. First, the effect of damage that will cause a definitive nature (*qaṭ'i*). Second, the effect of damage that will be caused is of a strong suspicion so that a strong assumption is the same as a certainty. Third, the effect of damage that will arise is of a small probability. Fourth, the effect of damage that will arise is a very rare probability.[25]

In the context of personal data protection, Islamic law recognizes the concept of *sadd al-dharī'at* as a legal method aimed at preserving public interest and preventing harm. This principle prohibits actions that are likely to lead to harm within society. While activities such as the collection of personal data are essentially permissible due to their potential benefits, they must be restricted when they carry the risk of misuse.[26] Therefore, efforts to protect personal data align with the principle of *sadd al-dharī'at*, which seeks to prevent any means that may result in harm or violation.[27]

Positive Legal Views Regarding Data Protection at the KPU according to Law Concerning Personal Data Protection

Before 2022, there were no specific regulations regarding personal data protection. Until the enactment of the UU PDP, what happened at the KPU with the leak of the permanent voter list (DPT) became a serious matter. The UU PDP serves as a clear legal foundation requiring maximum efforts in personal data protection.

---

24 Amir Syarifuddin, *Ushul Fiqh (2)* (Jakarta: Kencana, 2011), 242–45.

25 asy-Syathibi, *Al-Muwafaqat*, vol. 3 (Kairo: Mathba'ah al-Maktabah at-Tijariyah, n.d.), 358–61.

26 Eryna Syahadatina Badar, Ahmad Fauzi, and Ahya Jazuli, "Personal Data Protection Policy in Law Number 27 of 2022 in the Perspective of Positive Law and Islamic Law," *Hukum Islam* 23, no. 1 (July 12, 2023): 72, https://doi.org/10.24014/jhi.v23i1.20465.

27 Mohammad Farid Fad, "Perlindungan Data Pribadi Dalam Perspektif Sadd Dzari'ah," *Muamalatuna* 13, no. 1 (2021): 56, http://dx.doi.org/10.37035/mua.v13i1.4674.

The establishment of the UU PDP or Personal Data Protection Law in Indonesia is based on three fundamental aspects: philosophical, sociological, and juridical. Philosophically, the regulation of privacy rights over personal data reflects the recognition and protection of fundamental human rights. This is grounded in Pancasila, particularly its second principle, "Just and civilized humanity," which serves as the philosophical foundation for ensuring fairness and fostering a culture that respects personal data.[28]

Sociologically, the regulation addresses the need to protect individual rights in the digital age, especially regarding the collection, processing, and dissemination of personal data. Adequate data protection fosters public trust and ensures that data is used responsibly without violating individual rights. This legal framework aims to balance individual rights with the public interest represented by the state.[29]

Juridically, the values of Pancasila must be incorporated into national legislation, as it is enshrined in the Preamble of the 1945 Constitution of the Republic of Indonesia. The constitutional basis for personal data protection is found in Articles 28G and 28H of the Constitution, which affirm the right to personal security, dignity, and property, and prohibit arbitrary seizure.

The Constitutional Court Decision No. 006/PUU-I/2003 reinforces that any regulation concerning human rights must be enacted through legislation. Thus, the personal data protection must be legally established through a law.

Furthermore, although the value of privacy may not be deeply rooted in traditional Indonesian culture, there is growing public awareness and expectation for personal data protection. This is evidenced by surveys showing that the public recognizes privacy as essential and supports stronger safeguards for personal data in the digital era.[30]

Regarding the KPU, it is expressly stated in Article 1, numbers 4 and 9 of UU PDP, namely "A Personal Data Controller is any individual, public body, or international organization, acting independently or jointly, that determines the purposes of and exercises control over the processing of Personal Data."

The KPU, as an election organizing institution that organizes executive and legislative elections, is one of the parties entitled to obtain people's data as a form of personal data processing for DPT data collection. Looking at other articles, it can be

---

28 Sinta Dewi Rosadi, *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)* (Jakarta Timur: Sinar Grafika, 2024), 11–12.

29 Rosadi, 14.

30 Rosadi, 15–16.

explained that the obligations carried out by Personal Data Controllers, such as the KPU, namely. Article 39 number "(1) A Personal Data Controller shall be obligated to prevent unauthorized access to Personal Data. (2) The prevention referred to in paragraph (1) shall be carried out by implementing a reliable, secure, and accountable security system for the processing of Personal Data and/or the operation of electronic systems that process Personal Data."

As explained in the article above, the KPU, as the Personal Data Controller, must have a strong security system so that it cannot be hacked or leaked due to system errors. Thus, the security system must be reliable, safe, and responsible.

Looking at Article 58 number (4), the KPU must be responsible to the President in any case, including a data leak. If not, administrative sanctions will be imposed on institutions that violate the UU PDP, per the article below. Thus, the KPU must implement a strict security system because there will be 204 million more people whose data leaked if the security system is not improved. Referring to Article 60 letter c, the KPU must be given administrative sanctions for errors that exist, even if they accidentally leak people's data, because there is a privacy that must not be leaked. This firm stance is a form of evaluation of the KPU, which is responsible for organizing elections. With the existence of the UU PDP, it is clear that it has become a legal reference standard because it is the legal basis for personal data protection. In contrast, previously, there were no more specific regulations discussing personal data protection.

UU PDP, as *ius constitutum*, has an equal position with other laws. Hierarchically, the law is in 3rd place out of 7 laws and regulations mentioned in the Law on the Formation of Legislation (UU Pembentukan Peraturan Perundang-Undangan). The existence of legal regulations that have a structure and hierarchy is based on *Stufenbau* Theory by Hans Kelsen, which, in the context of Indonesia, is Pancasila as its legal ideal or *staatsfundamental norm*.[31]

With this hierarchy, there is a commitment to the implementation of the law. However, it still goes back to one of the internal functions of the existence of laws and regulations, namely the function of legal certainty.[32] So here, legal certainty goes hand in hand with legal awareness, which is part of the means of community

[31] Muhamad Bacharuddin Jusuf and Adara Khalfani Mazin, "Penerapan Teori Hans Kelsen Sebagai Bentuk Upaya Tertib Hukum Di Indonesia," *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat* 2, no. 01 (January 8, 2024): 5, https://journal.forikami.com/index.php/dassollen/article/view/519.

[32] Nurul Qamar and Farah Syah Rezah, *Ilmu Dan Teknik Pembentukan Peraturan Perundang-Undangan* (Makassar: Social Politic Genius, 2019), 13.

renewal, so that the values of order and tranquility are maintained[33] through the existence of UU PDP.

The form of order and tranquility that is the existence of legal awareness built into the UU PDP is the inclusion of criminal elements in Article 67. However, the criminal elements in the law are not absolute or mandatory.[34] So, if we look at the inclusion of criminal elements in UU PDP, then UU PDP, in the authors' opinion, is very important. The presence of UU PDP is the answer to the existence of legal awareness that must be built for every person, especially for related institutions/agencies, in this case, election organizers, so that they continue to pay attention to each point of the existing provisions, so that data leaks do not occur.

UU PDP and its criminal elements can strengthen the position of legal certainty, demanding that the law function as a rule that must be obeyed without exception. However, this is not only related to how the regulation is implemented but also to how the norms or substances in the regulation reflect the basic principles of law. As a written norm, laws and regulations in Indonesia function as a basis for implementing government policies and as a guideline in organizing the state.[35]

Sadd al-Dharī'at Views Regarding Data Protection at the KPU according to Law on Personal Data Protection

To determine the law of the path (means) that prohibits the goal, three things need to be considered: First, the goal: If the goal is prohibited, then the path is also prohibited, and vice versa. Second, Intention: If the intention is to achieve something *ḥalāl*, then the law of the means is *ḥalāl*, and if the intention is to achieve something *ḥarām*, then the means are also *ḥarām*. Third, Consequences: If the result of an act produces benefits, then its *wasīlat* may be carried out, and if the result is damage even though the goal is for good, then the law is not permissible.

The determination of the law through *sadd al-dharī'at* is by calculating the consequences of a treatment after it is carried out, not just by looking at the motive. That is why if an act is more directed towards loss and *mafsadat*, then it is prohibited because, according to Islamic law, namely rejecting loss is more important.[36]

---

[33] Soerjono Soekanto, "Kesadaran Hukum Dan Kepatuhan Hukum," *Jurnal Hukum & Pembangunan* 7, no. 6 (1977): 462.

[34] Maria Farida Indrati Soeprapto, *Ilmu Perundang-Undangan Proses Dan Teknik Pembentukannya* (Yogyakarta: Kanisius, 2007), 99.

[35] Siti Halilah and Mhd. Fakhrurrahman Arif, "Asas Kepastian Hukum Menurut Para Ahli," *Siyasah: Jurnal Hukum Tata Negara* 4, no. II (2021): 58.

[36] Syarmin Syukur, *Sumber-Sumber Hukum Islam* (Surabaya: Usana Ofset Printing, 1993), 112.

Implementation of *sadd al-dharī'at* and its relation to data leaks at the KPU that the original law of collecting personal data for the KPU is permissible because the initial purpose contains benefits, namely to become voters or participants in the implementation of elections. However, if there is potential for evil when achieving this goal, such as personal data leaks caused by the negligence of the KPU, then the law may change. Therefore, preventive measures are needed to prevent evil (*sadd al-dharī'at*) carried out by the KPU as an election organizing institution to prevent leaks of personal data of voters or election participants. Personal data protection must be carried out because personal data leaks will damage a person's life. Data leak cases, which often lead to the widespread dissemination of various types of data, carry the potential for misuse by parties with vested interests.[37]

Therefore, protecting personal data is a primary need (*ḍarūriyyat*) categorized as *ḥifẓ al-'irḍ*, namely maintaining honor. In other terms, Tāj ad-Dīn al-Subkī added, as referenced in Jasser Auda's book *Maqasid al-Shariah as Philosophy of Islamic Law: A Systems Approach,* that honor has long been a central concept in Arab culture since pre-Islamic times. However, Jasser Auda expands its interpretation to encompass the preservation of human dignity and even the protection of human rights, as fundamental objectives of Islamic law.[38]

In general, this theory divides *maqāṣid* into six parts, namely protecting religion (*ḥifẓ al-dīn*), protecting the soul (*ḥifẓ al-nafs*), protecting reason (*ḥifẓ al-'aql*), protecting descendants (*ḥifẓ al-nasb*), protecting property (*ḥifẓ al-māl*), and protecting honor (*ḥifẓ al-'irḍ*).[39]

To prevent damage in the form of personal data leaks, the KPU needs to make more systematic efforts to process people's data so that personal data leaks do not happen again. In addition, the processing of personal data has various implications for data subjects.[40] Therefore, special attention is needed in its implementation. Furthermore, this is also related to the dualistic nature of personal data processing at the KPU, namely the need to publish data for the sake of transparency in the

---

37 Naylawati Bahtiar, "Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah," *Development Policy and Management Review (DPMR)*, March 20, 2024, 86.

38 Jasser Auda, *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach* (International Institute of Islamic Thought (IIIT), 2008), 22–23.

39 Husamuddin MZ, "Hifzh Al-Irdh Dalam Transformasi Sosial Modern (Upaya Menjadikan Hifzhu Al-Ird Sebagai Maqashid Al-Dharuriy)," *At-Tasyri': Jurnal Ilmiah Prodi Muamalah* 11, no. 2 (2019): 128, https://doi.org/10.47498/tasyri.v11i2.298.

40 Valentin Rupp and Max von Grafenstein, "Clarifying 'Personal Data' and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection," *Computer Law & Security Review* 52 (April 1, 2024): 4, https://doi.org/10.1016/j.clsr.2023.105932.

implementation of elections and the need to protect data subjects from personal misuse.[41] Reflecting on this, the KPU has two main obligations in protecting personal data: maintaining data transparency and protecting data subjects, namely individuals.

The KPU can do several things to protect personal data and avoid *mafsadat* in the form of data leaks, namely, first, reviewing the rules contained in Law Number 7 of 2017 concerning General Elections (*UU Pemilu*) so that they do not conflict with UU PDP. Second, evaluating the personal data protection from two aspects, namely reviewing the information technology system used because data leaks indicate weaknesses in the system used, namely being unsafe, raising standards for human resources operating the system at a minimum, namely understanding the procedures and urgency of protecting personal data, then furthermore there must be openness between the KPU and the public to foster trust.

Furthermore, personal data protection should follow General Data Protection Regulation (GDPR)[42] data processing principles, which stipulate that anyone who owns and processes personal data is responsible for ensuring that it is (1) processed lawfully, fairly and transparently (lawfulness), (2) collected and used only for specific, explicit and legitimate purposes (purpose limitation), (3) limited only to what is necessary for the specific processing purposes (data minimization), (4) accurate, with inaccurate data corrected and deleted (data accuracy), (5) stored only as long as necessary (data retention), and (6) protected (integrity and confidentiality).[43]

Then, based on Article 16 of UU PDP, several principles must be applied, including personal data protection that covers data collectors in a limited and specific manner, is legally valid and transparent, processing is carried out according to purpose, processing is carried out by guaranteeing the rights of personal data subjects, is carried out accurately, and can be accounted for.

With several methods offered above, it is hoped that they can prevent personal data leaks, considering the consequences that arise are very detrimental. Efforts to protect personal data reviewed from *sadd al-dharī'at* prove that Islamic law is based

---

41 Faiz Rahman, "Pelindungan Data Pribadi dan Integritas Pemilu," kompas.id, December 19, 2023, https://www.kompas.id/baca/opini/2023/12/18/pelindungan-data-pribadi-dan-integritas-pemilu.

42 "General Data Protection Regulation (GDPR) – Legal Text," General Data Protection Regulation (GDPR), accessed January 23, 2025, https://gdpr-info.eu/.

43 Peter Chase, "Perspectives on the General Data Protection Regulation Of the European Union," 2024. 5

on the benefit. Therefore, sharia establishes a preventive legal method to support the benefit by eliminating all potential that gives rise to *mafsadat*.[44]

In addition, trust (*amanat*) is emphasized as an essential trait of a good Muslim and serves as a cornerstone of social relationships. Leaking this trust is considered a grave offense, as explained in various verses of the Qur'an and Hadith.[45] Thus, in a broader sense, the objective of the Qur'an and Hadith in advocating for the protection and respect of privacy (including preventing data leaks) is to close the doors to potential ***ḥarām***, following the Islamic legal principle of *sadd al-dharī'at*.

The Impact of Personal Data Leaks in Indonesia's Electoral System

The personal data leaks did not occur only at the KPU; as previously mentioned, 252 million records from the final voter list were leaked to the public in November 2023.[46] Although the official press release from the KPU did not specify the number of leaked data records.[47] In 2021, the Ministry of Health's health alert card (e-HAC) data leak also occurred. A year earlier, on April 17, 2020, around 15 million Tokopedia user data were hacked, and in May 2020, 1.2 million Bhineka.com e-commerce user data were also leaked.[48]

In brief, the chronology of the data leaks at the KPU is as follows: First, Disclosure by the Hacker: On November 27, 2023, a hacker using the alias "Jimbo" claimed to have leaked the website of the KPU and obtained approximately 252 million voter data records. After filtering out duplicate entries, he stated that he possessed 204,807,203 unique data records.[49] Second, Publication and Sale of Data: Jimbo shared 500,000 sample data records on the *BreachForums* website to demonstrate the authenticity of the data. He offered the entire dataset for sale at a price of approximately USD 74,000, or around IDR 1.2 billion.[50] Last, Detection by BSSN: The National Cyber and Crypto Agency (BSSN) detected the data publication

---

44 Fad, "Perlindungan Data Pribadi Dalam Perspektif Sadd Dzari'ah," 62.

45 Muharman Lubis and Mira Kartiwi, "Privacy and Trust in the Islamic Perspective: Implication of the Digital Age," in *2013 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)*, 2013, 1–6, https://doi.org/10.1109/ICT4M.2013.6518898.

46 "252 Juta Data DPT Pemilu 2024 Bocor, Apa Tanggapan KPU dan Menkominfo?"

47 KPU, "Siaran Pers Terkait Informasi Dugaan Kebocoran Data Milik KPU," accessed May 22, 2025, https://www.kpu.go.id/berita/.

48 Asa Pramudya Kristanto, "Perlindungan Terhadap Data Pribadi Dalam Aplikasi Digital Sebagai Bentuk Perlindungan Hak Asasi Manusia," *UNES Law Review* 5, no. 3 (2023): 953, https://doi.org/10.31933/unesrev.v5i3.367.

49 Juniar Laraswanda Umagapi, "Kebocoran Data Pemilih Pemilu 2024," *Pusaka*, Desember 2023, 1.

50 "Begini Kronologi Data 204 Juta DPT Pemilu 2024 Milik KPU Bocor Dibobol Hakcer | tempo.co," Tempo, November 29, 2023, https://www.tempo.co/

activity by Jimbo through a cyber patrol on the same day. BSSN promptly informed the KPU and coordinated efforts to mitigate the incident.[51]

What is described above can be understood through the following approach. One approach to categorizing data leak threats is based on their cause, namely, intentional or unintentional. Intentional data leaks occur due to external parties or irresponsible insiders, such as malware. These attacks usually target individuals and organizations that can cause device damage, personal data leaks, and significant financial losses.[52] Then there are break-ins and hacking. Second, there are unintentional data leaks, such as errors in the person operating, so that the data is accidentally shared with the public, or data is transmitted without proper encryption. The second approach is based on the party causing the leak, namely threats from insiders or outsiders.[53]

Apart from the various loopholes that cause personal data leaks, this case creates a sense of discomfort and insecurity for the public because the data can be used as material for crimes. This is considered very reasonable, considering that protecting personal data is a fundamental right, even considered as important as Human Rights.

Some of the impacts of personal data leaks are described below: Fraud, the first impact of personal data leaks, namely fraud in the sense of online fraud in the form of fraudulent crimes that refer to activities that use gadgets that use the internet.[54] Then, this is categorized into five types based on those that claim the most victims, namely prize scams (91.2%), illegal digital loans (74.8%), malicious link sharing (65.2%), scams disguised as family emergencies (59.8%), and illegal investments (56%).[55] The causes of fraud are generally divided into two categories: internet users who are not careful in using personal data in every application or transaction they make, and an institution's negligence in managing personal data. Fraud resulting

---

51 "BSSN Ungkap Kronologi Kebocoran Data Pemilih KPU di Sidang DKPP," nasional, accessed May 22, 2025, https://www.cnnindonesia.com/nasional/

52 Dhani Kristianto and Azis Budianto, "Guaranteed Legal Protection for Malware Victims in Indonesia," in *Proceedings of the 4th International Conference on Law, Social Sciences, Economics, and Education, ICLSSEE 2024, 25 May 2024, Jakarta, Indonesia* (Proceedings of the 4th International Conference on Law, Social Sciences, Economics, and Education, ICLSSEE 2024, 25 May 2024, Jakarta, Indonesia, Jakarta, Indonesia: EAI, 2024), 1,

53 Long Cheng, Fang Liu, and Danfeng Yao, "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 7, no. 5 (2017): 2, https://doi.org/10.1002/widm.1211.

54 I Gusti Made Jaya Kesuma, Ida Ayu Putu Widiati, and I Nyoman Gede Sugiartha, "Penegakan Hukum Terhadap Penipuan Melalui Media Elektronik," *Jurnal Preferensi Hukum* 1, no. 2 (2020): 74, https://doi.org/10.22225/jph.1.2.2345.72-77.

55 "Maraknya Penipuan Digital Di Indonesia," *Indonesia Baik*, accessed May 1, 2024, https://indonesiabaik.id/infografis/

from personal data leaks presents its challenges in law enforcement. A specific understanding is required to take effective action against such crimes, so that they can be minimized or even eliminated.

Doxing is an online practice that aims to expose someone's personal information without permission. It is an unethical practice because it is carried out by the perpetrator with malicious intent, causing harm to the target.[56] Personal information leaked to the public allows for crimes such as blackmail, coercion, and even harassment. In general, the information that is spread is the victim's real identity in the form of a telephone number, information to find the victim physically, namely home address and workplace, and information that has the potential to embarrass the victim. Meanwhile, based on the purpose of the perpetrator. Doxing is divided into three categories: the pure intention of committing a crime, political purposes, and internal regulations between members of an online community.[57]

The issue of doxing frequently occurs in Indonesia, with victims ranging from the living to the deceased, from public figures to ordinary citizens. Doxing can also affect journalists. According to *Aliansi Jurnalis Independen* (AJI) Indonesia, during the 2020--2021 period, there were 8 cases of doxing out of a total of 14 cases of digital attacks.[58] Nevertheless, it is still very possible for the general public to be highly vulnerable to doxing.

In simple terms, doxing can be interpreted as misusing someone's data, where the data is obtained from leaks and used for crime. This can be included in the category of violation of someone's right to privacy. The personal data protection as a guarantee of someone's right to privacy must start from the existence of legal certainty because the guarantee of data protection must be placed on a legal instrument with the highest power in a country, namely the constitution.[59]

This doxing crime has been regulated in the latest regulation on personal data protection, namely Article 65 of UU PDP: "Any person is prohibited from obtaining or collecting personal data that does not belong to them with the intent to benefit themselves or others, resulting in harm to the data subject."

---

[56] Yao-Tai Li and Katherine and Whitworth, "Coordinating and Doxing Data: Hong Kong Protesters' and Government Supporters' Data Strategies in the Age of Datafication," *Social Movement Studies* 23, no. 3 (May 3, 2024): 369, https://doi.org/10.1080/14742837.2023.2178404.

[57] Batuhan Kukul, "Personal Data and Personal Safety: Re-Examining the Limits of Public Data in the Context of Doxing," *International Data Privacy Law* 13, no. 3 (2023): 183–84, https://doi.org/10.1093/idpl/ipad011.

[58] "AJI Indonesia: 14 Kasus Serangan Digital Kepada Jurnalis dan Media, 8 Diantaranya Kasus Doxing," KOMPAS.tv, accessed May 1, 2024, https://www.kompas.tv/

[59] Halif Halif, Ainul Azizah, and Prisma Diyah Ratrini, "Regulating Doxing and Personal Data Dissemination in Indonesia," *Jurnal Kajian Pembaruan Hukum* 3, no. 1 (2023): 69, https://doi.org/10.19184/jkph.v3i1.33938.

Here, it can be seen that this doxing behavior violates the law, and perpetrators who do it will be subject to criminal penalties in the form of imprisonment and fines. The existence of this regulation strengthens the role of the state in protecting someone's data as a guarantee of citizens' basic rights.

The next impact is digital blackmail, which refers to the exploitation of technology and social media platforms to blackmail victims by threatening to reveal their personal information in the form of sensitive images and other materials.[60] One common method used is threatening to spread private photos, some of which have been edited to appear nude. The victim is then contacted and asked to pay a ransom to prevent the photos from being leaked. Another method involves the leakage of personal data, such as phone numbers, where scammers contact the victim with various pretexts, such as claiming to have kidnapped a loved one or threatening to hack a bank account, all of which ultimately lead to coercing the victim into making a payment.

Blackmail can be prevented by being aware of maintaining personal information used in the digital world, avoiding suspicious links, updating information and terms of service in each application, and paying attention to ethics in social media.[61]

Phishing is a form of online identity theft carried out by phishers to gain monetary gain. This crime is a social engineering trick that tricks people into obtaining personal information. The targeted data, namely personal data consisting of name, age, and home address, then account data in the form of username and password, and financial data including credit card information and accounts.[62]

Deceptive phishing is the most common type of phishing attack in which the attacker uses social engineering techniques to deceive victims. By believing these scenarios, the user will fall prey and follow the given link, which will disclose their personal information to the phisher. Deceptive phishing is performed through phishing emails, fake websites, phone phishing (Scam Call and IM), social media,

---

60 Hawraa Taher Hussein, "Exploring the Social Impact of Cyber Extortion : A Sociolinguistic Study" *The Islamic University College Journal* 2, no. 79 (2024): 86.

61 Sinta Nuriyah and Wiwik Afifah, "Analisis Kasus Pemerasan Akibat Penyalahgunaan Pada Sosial Media," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 2, no. 3 (December 7, 2022): 11, https://doi.org/10.53363/bureau.v2i3.116.

62 Ananta Fadli Sutarli and Shelly Kurniawan, "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia," *Innovative: Journal of Social Science Research* 3, no. 2 (2023): 3.

and via many other mediums. The most common social phishing types are discussed below;

1) A phishing email, a phishing email or Spoofed email, is a forged email sent from an untrusted source to thousands of victims randomly. These fake emails are claiming to be from a person or financial institution that the recipient trusts in order to convince recipients to take actions that lead them to disclose their sensitive information.
2) Spoofed website, also called phishing websites, in which phishers forge a website that appears to be genuine and looks similar to the legitimate website.
3) Phone Phishing (Vishing and Smishing). This type of phishing is conducted through phone calls or text messages, in which the attacker pretends to be someone the victim knows or any other trusted source the victim deals with.
4) Social Media Attack (Soshing, Social Media Phishing). Social media is the new favorite medium for cybercriminals to conduct their phishing attacks. The threats of social media can be account hijacking, impersonation attacks, scams, and malware distribution. However, detecting and mitigating these threats requires a longer time than detecting traditional threats, as social media exists outside of the network perimeter.[63]

Several ways to avoid phishing crimes include enabling Two-Factor Authentication (2FA), which involves a two-step verification process to ensure that account data remains secure. It is also important to verify the safety of websites visited and emails received, use the latest version of your browser, since browsers are generally updated to enhance user security while browsing, making newer versions more secure, conduct regular malware scans, and install anti-phishing protection applications.[64]

Fraud, doxing, extortion, and even phishing are certainly very detrimental, and there should be stricter protection to mitigate the risk of recurrence. One of the efforts is by enacting regulations concerning personal data protection, which was later realized in UU PDP. This regulation has accommodated measures to tackle various crimes in the digital world, including imposing strict sanctions on

---

[63] Zainab Alkhalil et al., "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," *Frontiers in Computer Science* 3 (March 9, 2021): 12–14, https://doi.org/10.3389/fcomp.2021.563060.

[64] Purnama Sari and Tata Sutabri, "Analisis Kejahatan Online Phising Pada Institusi Pemerintah/Pendidik Sehari-Hari," *Jurnal Digital Teknologi Informasi* 6, no. 1 (2023): 33–34, https://doi.org/10.32502/digital.v6i1.5620.

cybercrime perpetrators. However, in practice, there are still various obstacles to its enforcement.

Several factors that may illustrate the challenges faced by law enforcement in handling digital crimes include: (a) Limitations Capacity and Resources: Investigating digital crimes requires technical expertise and sufficient resources; however, many law enforcement agencies do not yet have sufficient capacity to handle the volume and level of complexity of existing cases, (b) Inability to Follow Development Technology: Cyber technology continues to evolve, and the latest attacks are often more sophisticated than law enforcement agencies can overcome. Education and insufficient training in technical aspects often become obstacles. (c) Limitations: Cooperation Interagency: Lack of coordination and cooperation between government agencies involved in law enforcement can hinder the exchange of information and coordination in investigating data leak cases.[65]

The effort to protect personal data is the responsibility of all parties, including both the government and the public themselves. The government is responsible for ensuring that the provisions of UU PDP are properly implemented and followed to safeguard individuals' data. As part of the prevention and prosecution of phishing perpetrators, the government also plays a role in enforcing the UU PDP by strengthening cooperation among government institutions responsible for cybersecurity, including the Police, the National Cyber and Crypto Agency (BSSN), and the Indonesian Child Protection Commission (KPAI).

In addition, the government is also responsible for imposing sanctions on phishing perpetrators. Referring to Article 58 of UU PDP, the institution responsible for the implementation of the law is the Personal Data Protection Authority (LOPDP), which is established by the government, and the agency in charge is appointed by the President and further regulated by Presidential Regulation. LOPDP holds significant duties and authority in the effort to protect individuals' data. In carrying out its responsibilities, the institution must maintain independence, possess adequate expertise, and operate with transparency.[66]

Various efforts can be undertaken by the public to protect their data. These include being aware of the importance of safeguarding personal data and having a

---

[65] Fenny Bintarawati, "The Influence of the Personal Data Protection Law (UU PDP) on Law Enforcement in the Digital Era," *ANAYASA: Journal of Legal Studies* 1, no. 2 (January 22, 2024): 6, https://doi.org/10.61397/ays.v1i2.92.

[66] Sutarli and Kurniawan, 9-10. Bintarawati, "The Influence of the Personal Data Protection Law (UU PDP) on Law Enforcement in the Digital Era," 6.

[66] Sutarli and Kurniawan, 9-10.

clear understanding of what constitutes personal data; being cautious with information found on the internet by not blindly trusting it without verifying its accuracy; avoiding clicking on links or documents from unknown sources; and using secure internet connections, for example, by not using public Wi-Fi when accessing sensitive information such as mobile banking. Furthermore, it is important to use secure and verified original applications; thus, refrain from using pirated apps, and always read the privacy policy before giving consent. Lastly, it is advisable to use antivirus and anti-malware programs.

Conclusion

This study concludes that the General Election Commission (KPU), as the designated personal data controller, holds full responsibility for ensuring the security and confidentiality of people's data, as mandated by Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). The data breach incident during the 2024 General Election, which involved the exposure of more than 204 million voter records, reflects the institutional weaknesses and the ineffective enforcement of data protection regulations in the digital electoral process. Through the integration of a positive legal approach (*ius constitutum*) and the Islamic legal doctrine of *sadd al-dharī'at*, this study reveals that personal data protection must be grounded not only in normative legal frameworks but also in ethical-preventive principles embedded in Islamic law. The principle of *sadd al-dharī'at* serves to close all potential pathways that may lead to harm (*mafsadat*), with data breaches being one of the modern manifestations of such harm. As such, this principle is highly relevant as a conceptual and practical framework for anticipating and preventing violations in digital governance.

This research contributes to contemporary Islamic legal discourse by demonstrating that the values of *sharī'at* can be constructively integrated into the state's modern regulatory systems. This fusion offers a holistic approach to addressing the challenges of data protection in the digital age. The implication of this study is the need for harmonization between the General Election Law and the UU PDP, the strengthening of the KPU's institutional capacity in cybersecurity management, and the establishment of an independent supervisory authority for data protection. In addition, relevant principles from the General Data Protection Regulation (GDPR) may be selectively adopted to reinforce Indonesia's data protection system, provided they are contextualized within local legal culture and Islamic ethical values.

References

Abrahams, Temitayo Oluwaseun, Sarah Kuzankah Ewuga, Samuel Onimisi Dawodu, Abimbola Oluwatoyin Adegbite, and Azeez Olanipekun Hassan. "A Review of Cybersecurity Strategies in Modern Organizations: Examining the Evolution and Effectiveness of Cybersecurity Measures for Data Protection." *Computer Science & IT Research Journal* 5, no. 1 (January 9, 2024): 1–25. https://doi.org/10.51594/csitrj.v5i1.699.

Alkhalil, Zainab, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy." *Frontiers in Computer Science* 3 (March 9, 2021). https://doi.org/10.3389/fcomp.2021.563060.

Amnesti, Sheila Kusuma Wardani, Siti Zulaichah, and Nurul Istiqomah. "Legal Protection of Personal Data Security in Indonesian Local Government Apps: Al Farabi's Perspective." *Legality: Jurnal Ilmiah Hukum* 33, no. 1 (2025): 1–19. https://doi.org/10.22219/ljih.v33i1.34623.

Asmadi, Erwin, Adi Mansar, Triono Eddy, Mukti Fajar Nur Dewata, Farid Wajdi, and Norhasliza binti Ghapa. "Data Theft and the Law on Protection of Personal Data: A Thematic Analysis." *Jurnal Hukum Novelty* 15, no. 2 (November 2, 2024): 268–85. https://doi.org/10.26555/jhn.v15i2.27661.

asy-Syathibi. *Al-Muwafaqat*. Vol. 3. Kairo: Mathba'ah al-Maktabah at-Tijariyah, n.d.

Auda, Jasser. *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach*. International Institute of Islamic Thought (IIIT), 2008.

Badar, Eryna Syahadatina, Ahmad Fauzi, and Ahya Jazuli. "Personal Data Protection Policy in Law Number 27 of 2022 in the Perspective of Positive Law and Islamic Law." *Hukum Islam* 23, no. 1 (July 12, 2023): 61–74. https://doi.org/10.24014/jhi.v23i1.20465.

Bahtiar, Naylawati. "Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah." *Development Policy and Management Review (DPMR)*, March 20, 2024, 85–100.

Bakare, Seun Solomon, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, and Nkechi Emmanuella Eneh. "Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations." *Computer Science & IT Research Journal* 5, no. 3 (March 9, 2024): 528–43. https://doi.org/10.51594/csitrj.v5i3.859.

Bintarawati, Fenny. "The Influence of the Personal Data Protection Law (UU PDP) on Law Enforcement in the Digital Era." *Anayasa: Journal of Legal Studies* 1, no. 2 (January 22, 2024): 135–43. https://doi.org/10.61397/ays.v1i2.92.

Bofa, Maya, Arifin Sudirman, and Darmawan Wawan Budi. "Data Rights Di Era Surveillance Capitalism: Skandal Data Cambridge Analytica & Facebook

Dalam Pemilihan Presiden Amerika Serikat 2016." *Hasanuddin Journal of International Affairs* 2, no. 2 (2022). https://doi.org/10.31947/hjirs.v2i2.22686.

Bungin, Burhan. *Metodologi Penelitian Kualitatif: Aktualisasi Metodologis Ke Arah Ragam Varian Kontemporer*. Jakarta: Rajawali Press, 2017.

Chase, Peter. "Perspectives on the General Data Protection Regulation Of the European Union," 2024.

Cheng, Long, Fang Liu, and Danfeng Yao. "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions." *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 7, no. 5 (2017): e1211. https://doi.org/10.1002/widm.1211.

Dinata, M. Ruhly Kesuma. *Ilmu Hukum*. Kotabumi: Sai Wawai Publishing, 2019.

Dobinson, Ian, and Francis Johns. "Qualitative Legal Research." In *Research Methods for Law*. Edinburgh: Edinburgh University Press, 2007.

Fad, Mohammad Farid. "Perlindungan Data Pribadi Dalam Perspektif Sadd Dzari'ah." *Muamalatuna* 13, no. 1 (2021): 33–69. http://dx.doi.org/10.37035/mua.v13i1.4674.

Fajar, Mukti, and Yulianto Ahmad. *Dualisme Penelitian Hukum Normatif Dan Hukum Empiris*. Yogyakarta: Pustaka Pelajar, 2010.

Farayola, Oluwatoyin Ajoke, Oluwabukunmi Latifat Olorunfemi, and Philip Olaseni Shoetan. "Data Privacy and Security in IT: A Review of Techniques and Challenges." *Computer Science & IT Research Journal* 5, no. 3 (March 27, 2024): 606–15. https://doi.org/10.51594/csitrj.v5i3.909.

Fauzy, Elfian, and Nabila Alif Radika Shandy. "Hak Atas Privasi Dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Lex Renaissance* 7, no. 3 (2022): 445–61.

General Data Protection Regulation (GDPR). "General Data Protection Regulation (GDPR) – Legal Text." Accessed January 23, 2025. https://gdpr-info.eu/.

Halif, Halif, Ainul Azizah, and Prisma Diyah Ratrini. "Regulating Doxing and Personal Data Dissemination in Indonesia." *Jurnal Kajian Pembaruan Hukum* 3, no. 1 (2023): 61–90. https://doi.org/10.19184/jkph.v3i1.33938.

Halilah, Siti, and Mhd. Fakhrurrahman Arif. "Asas Kepastian Hukum Menurut Para Ahli." *Siyasah: Jurnal Hukum Tata Negara* 4, no. II (2021).

Hoofnagle, Chris Jay, Bart van der Sloot, and Frederik Zuiderveen Borgesius. "The European Union General Data Protection Regulation: What It Is and What It Means." *Information & Communications Technology Law* 28, no. 1 (January 2, 2019): 65–98. https://doi.org/10.1080/13600834.2019.1573501.

Husamuddin MZ. "Hifzh Al-Irdh Dalam Transformasi Sosial Modern (Upaya Menjadikan Hifzhu Al-Ird Sebagai Maqashid Al-Dharuriy)." *At-Tasyri': Jurnal Ilmiah Prodi Muamalah* 11, no. 2 (2019): 119–32. https://doi.org/10.47498/tasyri.v11i2.298.

Hussein, Hawraa Taher. "Exploring the Social Impact of Cyber Extortion : A Sociolinguistic Study" 2, no. 79 (2024): 86.

Indonesia, Badan Pusat Statistik. "Jumlah Penduduk Pertengahan Tahun - Tabel Statistik." Accessed May 22, 2025. https://www.bps.go.id/id/statistics-t.

Jusuf, Muhamad Bacharuddin, and Adara Khalfani Mazin. "Penerapan Teori Hans Kelsen Sebagai Bentuk Upaya Tertib Hukum Di Indonesia." *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat* 2, no. 01 (January 8, 2024). https://journal.forikami.com/index.php/dassollen/article/view/519.

Kesuma, I Gusti Made Jaya, Ida Ayu Putu Widiati, and I Nyoman Gede Sugiartha. "Penegakan Hukum Terhadap Penipuan Melalui Media Elektronik." *Jurnal Preferensi Hukum* 1, no. 2 (2020): 72–77. https://doi.org/10.22225/jph.1.2.2345.72-77.

KOMPAS.tv. "AJI Indonesia: 14 Kasus Serangan Digital Kepada Jurnalis dan Media, 8 Diantaranya Kasus Doxing." Accessed May 1, 2024. https://www.kompas.tv/.

KPU. "DPT Pemilu 2024 Dalam Negeri Dan Luar Negeri, 204,8 Juta Pemilih." Accessed April 30, 2024. https://www.kpu.go.id/berita/

———. "Siaran Pers Terkait Informasi Dugaan Kebocoran Data Milik KPU." Accessed May 22, 2025. https://www.kpu.go.id/berita/

Kristanto, Asa Pramudya. "Perlindungan Terhadap Data Pribadi Dalam Aplikasi Digital Sebagai Bentuk Perlindungan Hak Asasi Manusia." *UNES Law Review* 5, no. 3 (2023): 952–60. https://doi.org/10.31933/unesrev.v5i3.367.

Kristianto, Dhani, and Azis Budianto. "Guaranteed Legal Protection for Malware Victims in Indonesia." In *Proceedings of the 4th International Conference on Law, Social Sciences, Economics, and Education, ICLSSEE 2024, 25 May 2024, Jakarta, Indonesia*, 1. Jakarta, Indonesia: EAI, 2024. https://doi.org/10.4108/eai.25-5-2024.2349181.

Kukul, Batuhan. "Personal Data and Personal Safety: Re-Examining the Limits of Public Data in the Context of Doxing." *International Data Privacy Law* 13, no. 3 (2023): 182–93. https://doi.org/10.1093/idpl/ipad011.

Lee, Hema Nadarajah, Alberto Iskandar, Sasha Lee, Sasha. "Indonesian Government Under Fire for String of Cyber Breaches." Asia Pacific Foundation of Canada. Accessed April 11, 2025. https://www.asiapacific.ca/publication/

Li, Yao-Tai, Katherine, and Whitworth. "Coordinating and Doxing Data: Hong Kong Protesters' and Government Supporters' Data Strategies in the Age of Datafication." *Social Movement Studies* 23, no. 3 (May 3, 2024): 355–72. https://doi.org/10.1080/14742837.2023.2178404.

Lubis, Muharman, and Mira Kartiwi. "Privacy and Trust in the Islamic Perspective: Implications of the Digital Age." In *2013 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M)*, 1–6, 2013. https://doi.org/10.1109/ICT4M.2013.6518898.

"Maraknya Penipuan Digital Di Indonesia | Indonesia Baik." Accessed May 1, 2024. https://indonesiabaik.id/.

Muhaimin. *Metode Penelitian Hukum*. Mataram: Mataram University Press, 2020.

nasional. "BSSN Ungkap Kronologi Kebocoran Data Pemilih KPU di Sidang DKPP." Accessed May 22, 2025. https://www.cnnindonesia.com/nasional/

Nuriyah, Sinta, and Wiwik Afifah. "Analisis Kasus Pemerasan Akibat Penyalahgunaan Pada Sosial Media." *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 2, no. 3 (December 7, 2022): 1241–51. https://doi.org/10.53363/bureau.v2i3.116.

Okezone. "Heboh Situs KPU Dibobol, 204 Juta Data DPT Bocor Dijual Peretas Miliaran Rupiah : Okezone Nasional." https://nasional.okezone.com/, accessed November 28, 2023. https://nasional.okezone.com/

Qamar, Nurul, and Farah Syah Rezah. *Ilmu Dan Teknik Pembentukan Peraturan Perundang-Undangan*. Makassar: Social Politic Genius, 2019.

Rahman, Faiz. "Pelindungan Data Pribadi dan Integritas Pemilu." kompas.id, December 19, 2023. https://www.kompas.id/baca/opini/.

Ramadhan, Kiki Rezki, and Chandra Wijaya. "The Challenges of Personal Data Protection Policy in Indonesia: Lesson Learned from the European Union, Singapore, and Malaysia." *Technium Social Sciences Journal* 36 (2022).

RI, Setjen DPR. "204 Juta DPT Pemilu Bocor, Sukamta Ingatkan KPU Tindaklanjuti Secara Serius." Accessed April 30, 2024. http://www.dpr.go.id/berita/detail/id/47962.

Rosadi, Sinta Dewi. *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Jakarta Timur: Sinar Grafika, 2024.

Rupp, Valentin, and Max von Grafenstein. "Clarifying 'Personal Data' and the Role of Anonymisation in Data Protection Law: Including and Excluding Data from the Scope of the GDPR (More Clearly) through Refining the Concept of Data Protection." *Computer Law & Security Review* 52 (April 1, 2024): 105932. https://doi.org/10.1016/j.clsr.2023.105932.

Rusli, Tami. *Pengantar Ilmu Hukum*. Lampung: Universitas Bandar Lampung (UBL) Press, 2017.

Sandiza, Miftahul Heldra, Sinta Dewi Rosadi, and Rahmat Suparman. "Towards Personal Data Protection in Structural Leadership Training: An Analysis of Maqāshid al-Sharī'ah Perspective." *Mazahib* 23, no. 2 (December 23, 2024): 631–68. https://doi.org/10.21093/mj.v23i2.8986.

Sari, Purnama, and Tata Sutabri. "Analisis Kejahatan Online Phising Pada Institusi Pemerintah/Pendidik Sehari-Hari." *Jurnal Digital Teknologi Informasi* 6, no. 1 (2023). https://doi.org/10.32502/digital.v6i1.5620.

Sautunnida, Lia, Izura Masdina Mohamed Zakri, and Faisal Ahmadi. "Dispute Resolution Mechanisms in Personal Data Leakages: An Analysis of OJK's Role

and Functions in Indonesia." *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 9, no. 1 (January 15, 2025): 23–44. https://doi.org/10.22373/sjhk.v9i1.21102.

Oktavira, Bernadetha Aurelia, and Hukumonline. "Arti Ius Constitutum dan Ius Constituendum," July 7, 2018. https://www.hukumonline.com/klinik/.

Sihombing, Josua. "Menkomdigi: Indonesia Pengguna Internet Terbesar Di Dunia." rri.co.id - Portal berita terpercaya. Accessed May 20, 2025. https://www.rri.co.id/.

Silalahi, Putri Hasian, and Fiorella Angella Dameria. "Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional." *Wajah Hukum* 7, no. 2 (2023): 614–27. http://dx.doi.org/10.33087/wjh.v7i2.1244.

Sinaga, Erlina Maria Christin, and Mery Christian Putri. "Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (2020): 237. https://dx.doi.org/10.33331/rechtsvinding.v9i2.428.

Soekanto, Soerjono. "Kesadaran Hukum Dan Kepatuhan Hukum." *Jurnal Hukum & Pembangunan* 7, no. 6 (1977).

Soeprapto, Maria Farida Indrati. *Ilmu Perundang-Undangan Proses Dan Teknik Pembentukannya*. Yogyakarta: Kanisius, 2007.

Sulaiman, Abdullah. *Pengantar Ilmu Hukum*. Jakarta: UIN Jakarta bersama Yayasan Pendidikan dan Pengembangan Sumber Daya Manusia, 2019.

Sutarli, Ananta Fadli, and Shelly Kurniawan. "Peranan Pemerintah Melalui Undang-Undang Perlindungan Data Pribadi Dalam Menanggulangi Phising Di Indonesia." *Innovative: Journal of Social Science Research* 3, no. 2 (2023): 4208–21.

Sutopo, Umarwan, Achmad Hasan Basri, and Hilman Rosyidi. "Presidential Threshold in the 2024 Presidential Elections: Implications for the Benefits of Democracy in Indonesia." *Justicia Islamica* 21, no. 1 (June 25, 2024): 155–78. https://doi.org/10.21154/justicia.v21i1.7577.

Syarifuddin, Amir. *Ushul Fiqh (2)*. Jakarta: Kencana, 2011.

Syukur, Syarmin. *Sumber-Sumber Hukum Islam*. Surabaya: Usana Ofset Printing, 1993.

Tempo. "252 Juta Data DPT Pemilu 2024 Bocor, Apa Tanggapan KPU dan Menkominfo? | tempo.co," November 30, 2023. https://www.tempo.co/politik/

Tempo. "Begini Kronologi Data 204 Juta DPT Pemilu 2024 Milik KPU Bocor Dibobol Hakcer | tempo.co," November 29, 2023. https://www.tempo.co/.

Umagapi, Juniar Laraswanda. "Kebocoran Data Pemilih Pemilu 2024." *Pusaka*, Desember 2023.