YURIDIKA
FAKULTAS HUKUM UNIVERSITAS AIRLANGGA
Volume 40 No 3, September 2025
DOI: https://doi.org/10.20473/ydk.v40i3.74179
Fakultas Hukum Universitas Airlangga, Jalan Dharmawangsa Dalam Selatan Surabaya, 60286 Indonesia, +6231-5023151/5023252
Fax +6231-5020454, E-mail: yuridika@fh.unair.ac.id
Yuridika (ISSN: 0215-840X | e-ISSN: 2528-3103)

Article history: Submitted 12 June 2025; Accepted 14 August 2025; Available Online 30 September 2025.

Harmonization of Personal Data Protection Principles With Electronic Justice Systems in Indonesia

Dody Novizar Mardyansyah[1], Sukarmi[2], Adi Kusumaningrum[3] and Yenny Eta Widyanti[4]
dodynovizar@student.ub.ac.id
[1 2 3 4] Brawijaya University, Indonesia

Abstract
Modern digital-based justice is the answer to the challenges of the development of the times. Although modern justice reflects an adaptive judicial body, it must still be equipped with established regulations. This study aims to examine the harmonization of personal data protection principles between the Supreme Court Regulation No. 7/2022 concerning electronic case administration and trials and Law No. 27/2022 concerning Personal Data Protection (PDP Law). In this case, the researcher uses a normative juridical method, with a statutory regulatory and comparative combined approach. This study highlights the norms gap in the Supreme Court Regulation No. 7/2022, particularly in the aspect of protecting the personal data of the parties input into the electronic justice administration system. The main findings exhibited are that the Supreme Court Regulation No. 7/2022 does not regulate the basic principles of data protection as mandated by the PDP Law, which has the potential to cause legal uncertainty and privacy right violations. The fact that the principle of personal data protection in the Supreme Court regulation has not been absorbed is due to the PDP Law, which only came into effect in 2024, even though both were enacted in the same year in 2022. This is seen as weakening the legitimacy of electronic justice in Indonesia. This study is expected to provide a positive contribution in the form of regulatory reform through the revision of the Supreme Court regulations, the establishment of data protection units in the judicial environment, and strengthening institutional coordination. The results of the comparative analysis of common law systems such as England show the importance of integrating data protection principles into the legal infrastructure and institutions of electronic justice to be aware of the protection of privacy rights that intersect with the guarantee of the human rights of justice seekers.
Keywords: Regulatory Reform; Electronic Justice; Personal Data Protection; PDP Law.

Introduction

Notably, the digital transformation in the Indonesian judicial system along with the demands of increasingly rapid globalization of information and communication technology are inevitable. The Supreme Court of the Republic of Indonesia (MARI), as the highest in rank for the judicial institution, has formulated the goal of judicial reform in the MARI blueprint with the main vision of bringing about a modern and adaptive judicial system in response to changes.[1] In this framework, the digitalization of justice is not only interpreted as an adaptation of technology but also as a systemic effort to create accessibility, efficiency, transparency, and accountability in law enforcement. Modern technology-based justice has been successfully applied in the form of the Electronic Justice System (hereinafter referred to as EJS) which changes the offline judicial mechanism to an online judicial system. This is a concrete manifestation of the new paradigm of digital technology-based justice.[2]

Electronic justice in Indonesia is regulated by internal regulations, Supreme Court Regulation No. 7/2022 and KMA Decree No. 363/KMA/SK/XII/2022, which officially regulate the procedures for organizing electronic judicial services. However, the complexity of the transition from a manual system to a digital system cannot be separated from various crucial issues, one of which is the absence of explicit norms regarding the protection of personal data. In this context, digital transformation, which is not equipped with an adequate legal protection foundation regarding the sensitive data of the parties to the case, has the potential to give rise to legal issues that are counterproductive to the principles of certainty and justice themselves.

When an electronic-based justice system is implemented, various sensitive data including identity information, case documents, electronic evidence, and legal statements are processed, stored, and transmitted through the digital platforms. This condition escalates serious issues regarding the security, confidentiality, and integrity

[1] Amran Suadi, *Sistem Pengawasan Badan Peradilan Indonesia* (Rajawali Press 2014).

[2] Teuku Rahmi, 'Transformasi Digital Dan Pengaruhnya Terhadap Budaya Organiasasi: Tinjauan Literatur Sistematis' (2024) 1 Jurnal Manajemen AKuntansi dan Ilmu Ekonomi.[103].

of information, especially in the context of the threat of cyberattacks and the misuse of private information by irresponsible individuals. This problem becomes even more significant considering that personal data is vulnerable to being misused when it is not based on clear protection rules. This is caused by the undeveloped electronic justice system in Indonesia, which is still in a transition phase from a traditional legal protection model to a comprehensive digital technology-based model.[3]

Furthermore, the absence of sensitive data protection norms in the Supreme Court Regulation of the Republic of Indonesia Number 7 of 2022 (hereinafter referred to as Supreme Court Regulation 7/2022) is present in the context of a broader legal paradigm shift from judicial administrative law to digital judicial law. In the traditional paradigm, legal protection is only focused on formal and procedural aspects, without considering the new risks arising from digitalization. However, in the digital era, the complexity of personal data vulnerabilities requires a legal framework that is to be able to anticipate and respond to non-physical threats that are systemic, such as data leaks, electronic data manipulation, and digital disinformation. The issuing of Law No. 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law) is an important milestone in response to this challenge. However, ironically, the enactment of the PDP Law, which was only enacted in 2024, is not included in the substance of Supreme Court Regulation 7/2022. This indicates a temporal gap in the formation of legislation that causes a normative disintegration between electronic justice policies and data protection policies, which in turn hinders the creation of a cohesive and resilient legal system.[4]

From a legal perspective, the absence of data protection norms in MA Regulation 7/2022 reflects the limitations of borough legislation in responding to socio-technological changes quickly and precisely. This emphasizes the need for

[3] Henny Saida Flora and others, *Perkembangan Ilmu Hukum Di Era Globalisasi* (Cedikia Mulia Mandiri 2025).

[4] Jumadi and Sarah, 'Transformasi Digital Sistem E-Court Dalam Modernisasi Persidangan Kasus Hukum Pidana, Perdata, Dan Hukum Islam Di Indonesia' (2025) 5 Jurnal Ilmu Hukum, Humaniora dan Politik.[1998].

a more progressive and responsive legal approach, not only fixated on regulatory aspects but also on the adequacy of the legal content that is to be able to anticipate the digital risks. In doctrinal studies, the absence of the essential principles of personal data protection such as the principle of data minimization, limitations on the purpose of use, and individual access rights to their own data opens up legal loopholes that not only have the potential to harm individuals but also weaken the credibility of judicial institutions in implementing digital systems. In addition, systematically, this void of norms can hamper the level of the public trust in the digitalization of justice as the public perception concerning the protection of privacy rights greatly determines the legitimacy of technology-based legal reform.[5] Therefore, a systemic and multidisciplinary approach ought to be put forward in formulating electronic justice policies that are not only efficient but also fair and inclusive.

From the existing legal phenomena, there is an urgent need for harmonization between the MA Regulation 7/2022 and the PDP Law, which is not only legally important but also serves as a strategic step in building a rule of law that is adaptive to the dynamics of digital transformation. In practice, these harmonization efforts can be carried out through regulatory revisions, strengthening legal protection instruments in the EJS system, and increasing the capacity of judicial human resources to understand the principles of data privacy. At the international level, common law countries such as the United Kingdom have previously designed the integration between the electronic justice system and personal data protection through comprehensive regulations that bind judicial institutions as data controllers. Lessons learned from the United Kingdom showed that a strong and legitimate EJS system can only be built on a legal framework that respects citizens' digital rights.[6]

---

[5] Rasji and Muhammad Yogi Septian Priyono, 'Tantangan Terhadap Privasi Dan Kebebasan Berpendapat Di Indonesia Pada Era Digital: Analisis Pandangan Filsafat Hukum' (2024) 5 Jurnal Hukum Lex Generalis.[4-7].

[6] Yufan Luo, 'The Development of Online Courts in The Digital Age and The Prospect of Future Justice: Based on The Innovation of Judicial Methods in China and The United Kingdom' (2024) 42 Journal of Education Humanities and Social Sciences.[437-438].

Based on this, it is necessary to conduct an in-depth analysis of the background of why this study was conducted according to a normative legal research method, using a statutory regulatory and comparative approach, by comparing the aspects of data protection in Indonesian electronic courts with the data protection system applied to electronic courts in the United Kingdom. The results of this study are expected to provide a contribution of thought related to regulatory reform through the revision of the Supreme Court regulations by including the principle of data protection in the legal infrastructure of digital courts within the judicial body and in parallel. The Supreme Court can form a data protection unit within the judicial body and strengthen cross-institutional coordination to be more aware of the comprehensive protection necessary of privacy rights.

The Urgency of the Personal Data Protection Concept in the Electronic Justice System

Personal data in the concept of the PDP Law is a set of data about an identified or identifiable person, either directly or indirectly, in any form. In the electronic justice system, the scope of this data includes more than just basic information such as name or address; it also includes the lawsuit documents, case data, witness statements, electronic evidence, and the verdicts uploaded to the court's electronic system.[7] Thus, personal data becomes an integral part of the entire electronic legal process cycle. The transition of the justice system from a conventional to a digital model has resulted in significant changes to the way judicial institutions process and store data. During this transformation, it is important to realize that personal data is not just an administrative entity but part of the constitutional rights inherent in every individual, and that is why the protection should be provided by the state through its state institutions as a form of respect for human dignity and guarantee of procedural justice.[8]

[7] Muhktar and Tanto Lailam, 'Implementasi Peradilan Elektronik Pada Pengadilan Negeri Dan Agama Di Daerah Istimewa Yogyakarta' (2024) 53 Jurnal Masalah-Masalah Hukum.[46].

[8] Asri Agung P. and Ludfie Jatmiko, 'Jaminan Kesehatan Dalam Hak Konstitusional Bagi Pekerja Migran Dalam Konstruksi Negara Kesejahteraan' 1 The Presecutor Law Review.[5].

The IT-based trial mechanism offers various conveniences, such as online case submission, real-time access to files, and transparency of the litigation process. However, behind all of this, there are security risks that cannot be ignored. Threats to personal data come in the form of cyberattacks, the manipulation of internal systems, data leaks due to human negligence, and the misuse of the data carried out by internal or external actors. Not only from a technical perspective, the blind spot in the legal regulations surrounding this system also opens up opportunities for violations of confidentiality and information security if the system's security mechanism does not yet follow the principles of modern security architecture such as double authentication, end-to-end encryption, or network segmentation.[9] In the midst of the lack of explicit provisions requiring judicial institutions to apply the principle of protecting sensitive data, the potential risk of data leaks and misuse becomes even greater and uncontrolled. This is what places personal data protection as a central issue in the reform of the electronic justice system.

The right to privacy is an inseparable part of human rights as regulated by the Indonesian constitution and international legal instruments. In this context, the state is obliged to create a legal system and institutions able to protect the personal information of its citizens from all forms of violation. As a matter of fact, when someone is involved in a legal process and must submit their personal data to the judicial system, there is a relationship of trust that should be maintained according to the highest standards of protection. The failure of the judicial institution to protect this data not only causes personal losses but also damages the legitimacy of the judicial institution itself. From the perspective of justice, everyone has the right to a legal process that is not only fast and cheap but also safe and respects their privacy. Therefore, personal data protection is no longer an option but rather a constitutional obligation inherent in every digital justice system.[10]

---

[9] Prado Dian Firmansyah and others, 'Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Perlindungan Data Dengan Teknologi Lanjutan' (2024) 2 Jurnal Kewirausahaan dan Multi Talenta.[116].

[10] Heru Setiawan and others, 'Digitalization of Legal Transformation on Judicial Review in the Constitutional Court' (2024) 4 Journal of Human Rights, Culture and Legal System.[286-287].

The evidence in Indonesia points out that the EJS system still focuses on administrative and efficiency aspects, while the data protection aspects have not been a priority in policy or technology infrastructure.

The absence of standard data management, the lack of clarity on the role of data controllers in the judicial environment, and the weak complaint mechanism and restoration of rights for victims of data leaks indicate the need for corrective steps. A comprehensive reformulation of the design of the electronic justice system is needed, from both regulatory and technical perspectives, including a revision of MA Regulation 7/2022 to accommodate the principles contained in the PDP Law. This will strengthen the institutional capacity in terms of cybersecurity, and increase stakeholder awareness of the importance of maintaining the confidentiality of case data. Thus, the digital justice system will not only be able to answer the demands of institutional modernization but it will also be able to uphold the principles of inclusive and dignified justice.

The Importance of Personal Data Protection Regulations in Supreme Court Regulation Number 7 of 2022

The Supreme Court Regulation 7/2022 is a form of institutional response to the demand for the modernization of the national justice system. This regulation is a normative framework for the implementation of a digital-based justice system that includes case registration, summons, document exchange, payment of court fees, and electronic trials.[11] However, when examined systematically, this internal regulation focuses more on technical and procedural arrangements for the implementation of online justice without guaranteeing the principle of protecting human rights, especially regarding the personal data of the parties involved in the judicial process. The articles listed explain more about the stages of case administration, the user account structure, and the technical procedures for uploading documents through

[11] Indra Budi Jaya and others, 'Inovasi Teknologi Peradilan Modern (E-Court) Mahkamah Agung Republik Indonesia Dalam Menjawab Tantangan Global' (2024) 2 Faedah Jurnal Hasil Kegiatan Pengabdian Masyarakat Indonesia.[3-8].

the EJS platform but barely regulate the basic principles of data protection based on the rights of data subjects as regulated in the PDP Law, the existence of which is an urgent need.[12] This situation creates a vacuum in the rules governing the principles of data protection in the reality of existing regulations.

Explicitly, MA Regulation 7/2022 does not include the terms "personal data" or "personal data protection" in its normative provisions. In the practice of implementing an electronic justice system, all stages of the case process, from registration through to the verdict, involve the input, storage, and transmission of highly sensitive data. For example, when registering a case electronically, the system will collect the complete identities of the parties as digital evidence that may contain personal or confidential information. The absence of a clause on the protection of this information indicates a serious weakness in data security.[13] This negligence shows that the MA Regulation 7/2022 has not adopted the privacy-by-design approach that is the standard in modern judicial regulations. The absence of norms governing the limitations of data use, the obligation to delete obsolete data, access and correction mechanisms by data subjects, and the obligation to notify in the event of a leak incident are the evidence that data protection has not been a primary concern in the design of this regulation.

Notably, Perma 7/2022 also does not provide space for supervision or a complaint mechanism in the event of a violation of the confidentiality of personal data. In a legal system that respects the right to data protection, a complaint mechanism is an important element to ensure that the data subjects have the legal tools to fight for their rights when a violation occurs. In the context of guaranteeing human rights, the PDP Law has regulated the existence of an independent supervisory authority but at the time MA Regulation 7/2022 was issued, this institution had not yet been established. This lack of norms in terms of supervision creates a legal vacuum effect

[12] Ida Bagus Rahmadi Supancana, *Berbagai Perspektif Harmonisasi Hukum Nasional Dan Hukum Internasional* (Penerbit Universitas Atma Jaya 2012).[142-143].

[13] Fenny Bintarawati, 'The Influence Of The Personal Data Protection Law (UU PDP) On Law Enforcement In The Digital Era' (2024) 1 Anayas: Journal of Legal Studies.[138-139].

that endangers the rights of data subjects, while also weakening the principle of a state based on law which demands a checks and balances mechanism in every technology-based public service system.[14]

Absorption of Personal Data Protection Principles in Law Number 27 of 2022

The PDP Law is a response to the urgent need for national legal protection that is expected to be able to comprehensively regulate the governance of personal information in the digital era. This law stipulates that personal data is the information that is attached and can be identified directly or indirectly with a particular individual, containing the main principles that have established the foundation for protecting privacy rights. These principles include, among others, the legality of the basis for data processing (lawfulness), limitation of the purpose of use (purpose limitation), data minimization (data minimization), information accuracy (accuracy), storage limitation (storage limitation), integrity and confidentiality (integrity and confidentiality), and accountability from the data controller (accountability). The establishment of these principles represents the harmonization of Indonesian law with international standards, especially the European Union's GDPR, which has become a global reference model for personal data protection.[15] With these principles in mind, data protection is not just a technical issue of storing information but has become a basic human right that must be guaranteed by the state and complied with by every entity that manages personal data, including judicial institutions.

One of the most essential elements in the PDP Law is the principle of explicit consent from the data subject as the primary basis for information processing. This means that no institution is permitted to process personal data without a valid legal basis or without the clear consent of the individual whose data is collected. In

[14] Uu Nurul Huda, Dian Rahmar Gumelar and Alwi Al Hadad, 'Forifying Democracy: Deploying Electoral Justice For Robust Personal Data Protection in The Indonesian Election' (2024) 6 Khazanah Hukum.[27].

[15] Syafira Agata Ramadhani, 'Komparasi Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa' (2022) 3 Jurnal Hukum Lex Generalis.[79-81].

the context of the courts, even though individuals de facto provide their personal information to resolve legal disputes, the courts still have a legal obligation to provide transparent information regarding the use, storage, and distribution of the data. The data subjects also have the right to revoke consent, have access to the stored data, can correct inaccurate data, and can eliminate irrelevant or unnecessary data. This is a crucial issue in the context of electronic justice (EJS), where various case documents are uploaded to a digital system and can become archives that are stored for the long term. Without the regulations being in line with this principle, the EJS system has the potential to ignore the fundamental rights of the parties involved in the legal process.[16]

The PDP Law also emphasizes the principle of transparency, which requires the judiciary as the data controller to openly explain the reasons, methods, and purposes for processing the personal data. As a matter of fact, the judiciary as part of the state authority cannot exempt itself from this principle. Since it acts as a place for the final resolution of legal disputes, the court has a higher moral and legal burden to maintain public trust through strict transparency and data protection mechanisms. This includes the obligation to provide information to the parties involved regarding which third parties have access to their data, how long the data will be stored for, and how technical protection is applied. In the context of EJS, which is highly dependent on the integration of information systems between agencies (courts, prosecutors, advocates, police, and ministries), this principle is very important to prevent data misuse across systems, as well as to maintain the legitimacy of legal processes conducted electronically. The fact that the principle of the data protection has not been absorbed in various lines, including the Indonesian judiciary, has made Indonesia one of the countries with the eighth highest rate of personal data violations in the world.[17]

---

[16] Afrison Samosir and Roida Nababan, 'Tinjauan Hukum Terhadap Pelaksanaan Sidang Elektronik Di Pengadilan Negeri Medan Berdasarkan Putusan Pengadilan No.971/Pdt.G/2023/PN.MDN' (2025) 2 HELIUM: Journal of Health Law Information and Humanities.[643].

[17] Ni Komang Sutrisni and others, 'The Compliance of Governance on Family Data Protection Regulation' (2024) 4 Journal of Human Rights, Culture and Legal System.[709].

In terms of time frame, MA Regulation 7/2022 was enacted first on October 10, 2022, while the PDP Law was issued in October of the same year but only came into effect two years later, in 2024. This situation creates a lack of synchronization between the two legal instruments that are closely related in practice. In a civil law legal system like Indonesia, the synchronization of norms between regulations is very important to ensure legal certainty and the effectiveness of public policy implementation.[18] While the MA regulation serves as an internal product of a judicial institution that regulates the technical administration of cases electronically, on the other hand, the PDP Law is an organic law entitled to establish the basic principles of data protection. The substantial disconnection between the two will create a legal gap that has the potential to endanger the rights of data subjects and reduce the legitimacy of the EJS system as a whole.[19]

From a substantive perspective, the MA Regulation 7/2022 has not demonstrated the integration of the fundamental principles regulated in the PDP Law. MA Regulation 7/2022 was designed with an administrative procedural approach in mind, not a rights-based approach as adopted by the PDP Law. As a result, EJS regulations in Indonesia are at great risk of violating the principles of lawfulness and accountability as the data processing is carried out without a comprehensive and holistic data protection foundation. The MA Regulation as a judicial technical instrument must be able to derive provisions of the law in the form of operational and detailed implementing regulations. However, the implementation of the PDP Law was effective later after the MA Regulation 7/2022 was enacted, while it had not absorbed the important regulatory components that had been included in the PDP Law, especially regarding data protection, monitoring mechanisms, remediation, and reporting obligations in the event of a data leak incident. This condition creates a gray area around enforcing the right to privacy due to it being unclear whether

[18] I Nyoman Putu Budiartha, I Made Pria Dharsana and Indrasari Kresnadjaja, 'Penguatan Konstruksi Hukum Perihal Perlindungan Data Pribadi' (2023) 12 Udayana Master Law Review.[63].

[19] Rizki Alamsyah and Sidi Ahyar Wiraguna, 'Dilema Media Massa Di Era Digital: Antara Perlindungan Data Pribadi Dan Kebebasan Pers Dalam UU PDP' (2025) 3 Media Hukum Indonesia. [110-114].

violations of data in the EJS constitute violations of public, administrative, or civil law, and who has the authority to prosecute such violations.

The comparison with international practice further confirms this inconsistency. In countries that have already integrated e-justice systems with the principle of personal data protection, there is a close functional and substantive relationship between the technical regulations of judicial institutions and the national legal framework on data protection. For example, the United Kingdom as a common law country has an e-justice system through HM Courts and Tribunals Service (HMCTS) that strictly refers to the Data Protection Act 2018, which adopted the GDPR.[20] The internal regulations of the English courts not only follow administrative procedures but also accommodate explicit clauses that require the application of the principle of privacy by design, regular security audits, and the appointment of a data protection officer. In addition, all electronic processes in court are subject to the supervision of the national data protection authority (Information Commissioner's Office).[21] This model not only guarantees the maximum legal protection for data subjects but also increases the accountability of the judicial institution in the use of information technology. When the court has both authority and responsibility regarding the data processing, the security norms become an integral part of modern judicial practice.

In the context of guaranteeing the protection of human rights and legal certainty, it is evident that the fundamental principles of data protection regulated in the PDP Law have not been absorbed into the MA Regulation 7/2022 in which it creates an urgency that cannot be delayed anymore to immediately harmonize regulations. This harmonization does not only include editorial adjustments or the insertion of data protection clauses in MA Regulations alone. It also demands a paradigm shift in understanding the function of the internal regulations of judicial institutions. The Supreme Court needs to adopt data protection principles as an

[20] Budi Agus Riswandi and Alif Muhammad Gultom, 'Protecting Our Mosts Valuable Personal Data: A Comparison Of Transborder Data Flow Laws In The European Union, United Kingdom, And Indonesia' (2023) 5 Prophetic Law Review.[181].

[21] Federica Casarosa, 'Transnational Collective Actions for Cross-Border Data Protection Violations' (2020) 9 Internet Policy Review.[2].

integral part of electronic justice governance. This can be concluded through the revision of MA Regulation 7/2022 by including articles that regulate the rights of data subjects, the principles of lawful processing, and the responsibilities of data controllers in the court environment. In addition, comprehensive training is required for judicial officials on the importance of protecting personal data as a component of human rights and as a prerequisite for the legitimacy of digital justice. With this typical regulatory reform, Indonesia will not only be able to catch up with international practices but also ensure that digital transformation in the judicial sector is truly in line with the principles of justice, transparency, and respect for citizens' constitutional rights.

The Vacuum of Norms in Supreme Court Regulation Number 7 of 2022

In normative legal studies, several forms of norm weaknesses are known, which are generally divided into three categories: vague norms, conflict norms, and vacuum norms.[22] These three have fundamental differences in their nature and implications for legal certainty. Vague norms refer to regulations that contain ambiguity, both in terms of their wording and substantive meaning, making it difficult when it comes to practical implementation.[23] Conflict norms refer to situations where a legal rule conflicts with another legal rule, in which both regulate the same substantive aspect.[24] The void of norms, in the most extreme sense, refers to the absence of any rules in a legal system regarding an issue that is already real and has legal consequences. In the context of MA Regulation 7/2022, the vacuum of norms becomes a concrete issue when viewed from the perspective of personal data protection in the electronic justice system due to the absence of explicit clauses that explicitly touch on the protection, management, security, or rights of data subjects and supervision.

[22] Sofwan, Haeruman Jayadi and Rusnan, 'Kejelasan Perumusan Norma Dalam Pembentukan Undang-Undang (Kajian Terhadap Penggunaan Frasa Hukum Dalam Perumusan Norma Undang-Undang)' (2021) 2 Jurnal Risalah Kenotariatan.[32-33].

[23] Aan Efendi and Dyah Octhorina Susanti, *Logika & Argumentasi Hukum* (Kencana Prenada Media Group 2020).

[24] ibid.

The void of norms is caused by the lack of synergy between the MA Regulation 7/2022 and the PDP Law, which should be the main legal protection in terms of personal data protection. The PDP Law explicitly regulates the legal principles that must be adopted by every institution that processes electronic data, including judicial institutions. In the context of data protection, there are provisions regarding the rights of data subjects, the principles of lawful processing, and the responsibilities of data controllers to ensure information security.[25] However, MA Regulation 7/2022, which regulates the digital justice system and is a milestone in enforcing justice, does not comply with these provisions. This shows the imparity of the regulations between the Supreme Court's legal products and the general national legislation. As a high state institution, the Supreme Court has a moral and legal responsibility to ensure that its legal products are in line with the principles of protecting constitutional rights, including the right to privacy and personal data.[26]

Given the complexity of the issues elevated by this normative vacuum, systematic steps are needed to identify, classify, and reorganize the regulatory instruments related to the electronic justice system (EJS). One approach that can be implemented is through a regulatory impact assessment (RIA) of Supreme Court Regulation 7/2022, to examine the extent to which the regulation provides adequate protection for individual rights.[27] RIA can also be used to identify the crucial areas that require new legal intervention, either through revisions to the Supreme Court Regulations (PERMA), the preparation of a Supreme Court Circular (SEMA), or even the preparation of a complementary Supreme Court Regulation that specifically regulates data protection in the judicial information system. This approach must be accompanied by the involvement of multiple stakeholders, including legal experts, judicial practitioners, data protection institutions, and civil society representatives, so then the regulatory updates are not elitist but rather reflect the real needs of

[25] Sinta Dewi Rosadi, *Pembahasan UU Perlindungan Data Pribadi* (Sinar Grafika 2023).

[26] Graham Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press Inc 2014).

[27] Ambar Widaningrum, *Regulatory Impact Analysis (Analisis Dampak Regulasi) : Konsep Dan Penerapannya* (Gadjah Mada University Press 2024).

justice seekers in the digital era. Thus, the electronic justice system is not only modern in technology but also mature in terms of legal protection.

Comparison of the Electronic Justice System in the United Kingdom which adopts the Common Law System

The United Kingdom is one of the earliest common law countries to adopt and integrate an electronic-based justice system into its national legal framework.[28] Through Her Majesty's Courts and Tribunals Service (HMCTS), the United Kingdom has built a digital justice system infrastructure that is not only efficient in terms of procedure but also pays close attention to the aspect of personal data protection. Since 2016, HMCTS has launched a court modernization program worth more than one billion pounds that includes the digitization of the entire court process, from filing cases, paying fees, collecting evidence, to online trials. What distinguish the UK's approach from many developing countries is the full integration of information technology and the principles of human rights protection, especially through the implementation of the Data Protection Act 2018 which substantively adopts the EU's General Data Protection Regulation (GDPR). Thus, the UK's digital justice system is not only developed as an administrative tool but is as an integral part of constitutional efforts to ensure equal legal protection and justice for all citizens.[29]

One of the main pillars of the UK data protection system is the obligation of privacy by design and by default, which is strictly applied in all developments of public technology systems, including those managed by the judiciary.[30] Under this framework, every digital platform designed by HMCTS must undergo a Data Protection Impact Assessment (DPIA), which is a comprehensive risk analysis of

[28] Dory Reiling, *Teknologi Untuk Keadilan: Bagaimana Teknologi Informasi Dapat Mendukung Reformasi Pengadilan* (Alumni Penerbit Akademik 2009).

[29] Graham Greeleaf, 'Now 157 Countries: Twelve Data Privacy Laws in 2021/22' (2022) 176 UNSW Law Research.

[30] Yose Indarta, *Cyber Law: Dimensi Hukum Dalam Era Digital* (Pustaka Galeri Mandiri 2025).

potential breaches of an individual's privacy before the system is implemented.[31] In addition, each court is required to appoint a Data Protection Officer (DPO) whose task is ensuring that all data processing processes comply with the principles of the GDPR, from data collection, storage, access, to deletion. Referring to this ,provision means that courts must not retain the personal information for longer than necessary, and that individuals who are part of a legal process have the right to request a copy, correction, or deletion of their data. This policy not only strengthens public trust in the legal system, but also ensures that digital modernization is not carried out at the expense of the right to privacy.[32]

In addition, the UK has established an independent external oversight mechanism for the digital justice system through the Information Commissioner's Office (ICO). It has the authority to oversee the compliance of all state institutions with the principles of personal data protection.[33] The ICO has the power to conduct inspections, investigate violations, and impose administrative and criminal sanctions on institutions found to have violated the data protection regulations. In several cases, public institutions including courts have been reprimanded or fined for failing to protect the personal data of their citizens. This mechanism shows that the UK is adopting a balanced oversight model between the internal authority of the judicial institution and an independent institution tasked with safeguarding the public interest.[34] This contrasts with the situation in Indonesia, where to date there has been no active data protection supervisory authority, even though the PDP law has mandated its establishment. Thus, the UK's approach provides an important lesson that data protection is

[31] Tegar Islami Putra, Nurul Fibrianti and Mohammad Raziq Fakhrullah, 'Data Protection Impact Assessment Indicators in Protecting Consumer Personal Data on E-Commerce Platforms' (2024) 6 The Indonesian Journal of International Clinical Legal Education.[120-128].

[32] Yuyut Prayuti, 'Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce Dan Perlindungan Data Konsumen Di Indonesia' (2025) 5 Jurnal Interpretasi Hukum.[907].

[33] Rosadi (n 25).

[34] Fanisa Mayda Ayiliani and Elfia Farida, 'Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara' (2024) 6 Jurnal Pembangunan Hukum Indonesia.[441-442].

not enough to be regulated only in norms; it must be equipped with concrete law enforcement that is accessible to the public.

Comparison of the Legal Framework of Indonesia and the United Kingdom

A comparison of the legal systems of Indonesia and the United Kingdom in terms of the regulation of personal data protection in the electronic justice system reflects fundamental differences, both in the dimensions of institutional structure and its normative substance. The United Kingdom, a country with a common law tradition, has long integrated the principles of individual rights protection into its judicial system, especially since the enactment of the GDPR and the Data Protection Act 2018. This integration is not only formal in the form of written regulations but it is also manifested in an institutional structure that supports the implementation of these principles.[35] On the other hand, Indonesia, which adopts a civil law legal system, is still in a transition phase where the application of technology in the justice system is taking place faster than the readiness of regulations and the data protection infrastructure. This has led to the emergence of regulatory lag, which is the lag in the legal norms responding to the development of information technology. For example, this is present in the failure to absorb the principle of data protection, which is a fundamental issue in the electronic justice system.

Institutionally, HMCTS in the UK is supported by a solid and complementary oversight ecosystem. This institution is not only responsible for the development and management of the digital justice system but is also required to coordinate with the Information Commissioner's Office (ICO), which is an independent authority overseeing personal data protection. The ICO has broad authority, including providing policy recommendations, preparing technical guidelines, conducting regular audits, and imposing sanctions on institutions that violate data protection provisions. In Indonesia, a similar institutional structure has not been established operationally. The PDP Law has mandated the establishment of a data

[35] Montassar Naghmouchi and others, 'Comparative Analysis of Technical and Legal Frameworks of Various National Digial Identity Solutions' [2023] arXiv:2310.01006 (cs.SE).[13-15].

protection supervisory institution but until now, there has been no clarity regarding its structure, authority, or coordination with other state institutions, including the Supreme Court. This condition creates a sharp institutional gap between Indonesia and the UK, especially in terms of accountability and the ongoing monitoring of the implementation of data protection principles in the digital justice system.[36]

In terms of legal substance, the differences between the two countries can be seen from how the principles of data protection are integrated into the judicial legal system. The UK makes the principles of data protection part of the legal value system that binds all institutional processes, including the judiciary. In other words, principles such as data minimization, lawfulness, purpose limitation, storage limitation, and accountability are not just normative jargon but are applied concretely in the design of technology systems, HR training, and the formulation of SOPs. Meanwhile, in Indonesia, the Supreme Court Regulation 7/2022 as the main regulation for the implementation of electronic justice does not explicitly contain these principles. There are no provisions regarding the rights of data subjects, objection mechanisms for data processing, or the responsibility of the court as the data controller. As a result, the protection of the personal data in the Indonesian justice system is more implicit, limited to administrative efforts without a strong substantive legal foundation.

The technical operational aspects also show striking disparities. In the UK, the digital justice system is built on a strong data security foundation, such as the use of layered encryption, regular system audits, security risk mapping, and a mandatory data breach incident reporting mechanism within 72 hours.[37] HMCTS also sets standards for information system interoperability that allow integration with other institutions without compromising the principle of data protection.[38] In Indonesia,

[36] Imam Hanafi and Arief Fahmi Lubis, 'Protection of Privacy and Intellectual Property Rights in Digital Data Management in Indonesia' (2023) 2 The Easta Journal Law and Human Rights (ESLHR).[35].

[37] Hastin Lia, 'UU PDP Dan Pelanggaran Data: Tindakan Yang Harus Diambil Perusahaan'' (*SiberMate*, 2024) <https://sibermate.com/hrmi/uu-pdp-dan-pelanggaran-data-tindakan-yang-harus-diambil-perusahaan> accessed 28 May 2025.

[38] Ministry of Justice of the United Kingdom's Government, 'Data Sharing For The Criminal Justice System Guidance' (2023).

the electronic justice system has experienced rapid development in terms of service digitalization but has not been equipped with comparable information security standards. There are no specific provisions that require regular security audits or a data breach incident reporting system. In fact, the court as the manager of personal data in cases is not required to appoint a data protection officer or prepare a privacy policy that can be accessed by the service users. This disparity confirms that the modernization of technological systems does not necessarily result in adequate legal protection if it is not accompanied by the standardization of technical standards and effective supervision.

This comparison provides an important lesson for Indonesia, that personal data protection in the judicial system cannot be separated from the institutional structure and normative design that favors individual rights. The reform of the electronic justice system (EJS) in Indonesia is not enough to be carried out only at the technical and administrative levels. It must be started by the restructuring of norms and institutions. The Supreme Court is entitled to revise the MA Regulation 7/2022 to comply with the principles of data protection mandated by the PDP Law, including adding the provisions that clarify the rights of data subjects, the obligations of data controllers, and the remediation mechanisms for violations. On the other hand, the establishment of an independent data protection supervisory institution that has a clear institutional relationship with the judiciary is also an urgent need. Thus, the digital justice system in Indonesia can be built on a foundation that is not only efficient and modern but also fair, transparent, and respecting the constitutional rights of citizens in the digital realm.

Comparative Study Results: Between National Data Protection Management Regulations and UK State Regulations

The results of the comparison between Indonesia and the UK in managing the personal data protection in the electronic justice system environment shows a significant gap. This finding requires serious attention in the context of national legal reform. Indonesia's backwardness lies not only in the lack of integration of the

data protection principles in technical regulations such as the MA Regulation 7/2022 but also the lack of coordination between institutions, the absence of a definitive supervisory authority, and the as yet weak institutional accountability in handling highly sensitive data. This comparison emphasizes that the modernization of the justice system must work alongside the development of the legal instruments that provide guarantees of protection for the fundamental rights of citizens, including the right to privacy and control of personal data. Notably, when the technology system develops faster than the legal norms that regulate it, the risk of inequality and injustice will increase systemically.[39]

With such conditions, it is appropriate for the policymakers to align the regulations both vertically and horizontally to create a continuity of norms and legal certainty. In the Indonesian system that adheres to the principle of the hierarchy of laws and regulations, every technical regulation under the law, including the Supreme Court regulations, should be subject to and consistent with the provisions of national legislation. However, the Supreme Court Regulation 7/2022 was issued in the same year as the PDP Law, in 2022, but the PDP Law only came into effect two years after it was issued, in 2024. The essential principles contained in the PDP Law had not been fully absorbed into the Supreme Court Regulation 7/2022. This shows the weakness of the regulatory harmonization mechanism across the state institutions. Regulatory reform must begin with the preparation of a regulatory alignment mechanism that involves collaboration between the Supreme Court, the Ministry of Communication and Information, and the personal data supervisory authority. The aim is to ensure that every legal instrument, whether administrative or substantive, is able to complement the rest while not encouraging elevation to interpretive conflicts.[40]

Furthermore, the comparison with the UK also shows the importance of institutional strengthening in the form of establishing a special unit or division

[39] Tegar Islami Putra and Nurul Fibrianti, 'Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia' (2024) 9 Lambung Mangkurat Law Journal.[68-69].

[40] Nawal Sholehuddin and others, 'A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries' (2024) 7 Journal of Muwafaqat.[24-28].

tasked with handling data protection issues in the judicial environment. In Indonesia, there is currently no structure that is explicitly responsible for the management and protection of data in the electronic justice system (EJS), leading to no clarity regarding the response procedures when the data leaks or privacy violations occur. In fact, international practice has shown that the appointment of a data protection officer (DPO) in public institutions, including Justice itself, is a strategic step in ensuring compliance with the principles of data protection and in educating all legal apparatus regarding the importance of protecting personal information.[41]

Another essential factor is building an evaluation and supervision framework based on the principles of accountability and transparency. A comparison with the United Kingdom underlines the effectiveness of the compliance-based monitoring system, where judicial institutions are required to undergo regular audits by external authorities and are subject to administrative and criminal sanctions if proven to have violated data protection provisions. Indonesia does not yet have a similar system. Then there is monitoring and evaluation by a supervisory institution that has independent authority and is not subject to institutional influence. In this way, the principle of the external supervision of judicial institutions is maintained within the corridor of the independence of judicial power but does not allow this power to escape the principle of public accountability, which is a key element in a modern democratic system.

The results of this comparative study encourage the urgency of a paradigm shift in the development of an electronic justice system (EJS) in Indonesia. The digital transformation in the justice sector is not only for procedural efficiency but also to substantially strengthen the fulfillment of citizens' rights. Furthermore, the national regulatory reform that places personal data protection as the core of the digital legal system will earn greater public trust in the judicial institutions. The existence of integrated regulations, the strong supervisory institutions, and a

[41] 'Memahami Peran Data Protection Officer Dalam Ekosistem Pelindungan Data Pribadi' (*Asosiasi Praktisi Perlindungan Data Indonesia*, 2021) <https://appdi.or.id/memahami-peran-data-protection-officer-dalam-ekosistem-pelindungan-data-pribadi/> accessed 28 May 2025.

competent internal structures will encourage the creation of a judicial ecosystem that is adaptive to technological developments while still being based on the principles of justice, accountability, and respect for human dignity. In other words, lessons from England are not to be copied outright but to be used as an inspiration to build a system that is in accordance with the needs and character of the Indonesian law.

Conclusion

The digital transformation of the judicial system through Supreme Court Regulation No. 7 of 2022 represents a progressive step in modernizing Indonesia's legal bureaucracy. However, its lack of attention to personal data protection reveals a critical normative gap. The absence of explicit data protection principles in the regulation not only creates a legal vacuum but also poses a threat to citizens' constitutional rights, particularly the right to privacy. This issue becomes more pressing when compared to the standards set by Law No. 27 of 2022 on Personal Data Protection (PDP Law) which, despite being enacted in the same year, has yet to be substantially integrated into the Supreme Court Regulation. Consequently, a gap persists between the development of electronic justice (EJS) and the adequacy of the regulations governing it. Without policy revision and regulatory harmonization, the electronic justice system may ultimately undermine the legitimacy of judicial institutions and erode public trust in a digital justice system that should be inclusive, transparent, and respectful of human rights. In response to these challenges, it is recommended to revise Supreme Court Regulation No. 7 of 2022 to align it with the PDP Law by incorporating provisions on the data subjects' rights and the court's responsibilities as a data controller. A dedicated personal data protection unit should be established within the judiciary to oversee supervision, incident reporting, and internal awareness programs. Furthermore, a secure and inclusive technology infrastructure must be developed, including strong cybersecurity measures such as encryption and multi-factor authentication. Regular training on personal data protection, digital ethics, and information

security should be provided to judicial officials. Finally, independent authorities should conduct regular audits and evaluations of the electronic justice system to ensure its accountability and transparency.

Bibliography

Alamsyah R and Wiraguna SA, 'Dilema Media Massa Di Era Digital: Antara Perlindungan Data Pribadi Dan Kebebasan Pers Dalam UU PDP' (2025) 3 Media Hukum Indonesia.

Ayiliani FM and Farida E, 'Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara' (2024) 6 Jurnal Pembangunan Hukum Indonesia.

Bintarawati F, 'The Influence Of The Personal Data Protection Law (UU PDP) On Law Enforcement In The Digital Era' (2024) 1 Anayas: Journal of Legal Studies.

Budiartha INP, Dharsana IMP and Kresnadjaja I, 'Penguatan Konstruksi Hukum Perihal Perlindungan Data Pribadi' (2023) 12 Udayana Master Law Review.

Efendi A and Susanti DO, *Logika & Argumentasi Hukum* (Kencana Prenada Media Group 2020).

Federica Casarosa, 'Transnational Collective Actions for Cross-Border Data Protection Violations' (2020) 9 Internet Policy Review.

Firmansyah PD and others, 'Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Perlindungan Data Dengan Teknologi Lanjutan' (2024) 2 Jurnal Kewirausahaan dan Multi Talenta.

Flora HS and others, *Perkembangan Ilmu Hukum Di Era Globalisasi* (Cedikia Mulia Mandiri 2025).

Government M of J of the UK, 'Data Sharing For The Criminal Justice System Guidance' (2023).

Graham Greeleaf, 'Now 157 Countries: Twelve Data Privacy Laws in 2021/22' (2022) 176 UNSW Law Research.

Greenleaf G, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (Oxford University Press Inc 2014).

Hanafi I and Lubis AF, 'Protection of Privacy and Intellectual Property Rights in Digital Data Management in Indonesia' (2023) 2 The Easta Journal Law and Human Rights (ESLHR).

Huda UN, Gumelar DR and Hadad A Al, 'Forifying Democracy: Deploying Electoral Justice For Robust Personal Data Protection in The Indonesian Election' (2024) 6 Khazanah Hukum.

Indarta Y, *Cyber Law: Dimensi Hukum Dalam Era Digital* (Pustaka Galeri Mandiri 2025).

Jaya IB and others, 'Inovasi Teknologi Peradilan Modern (E-Court) Mahkamah Agung Republik Indonesia Dalam Menjawab Tantangan Global' (20224) 2 Faedah Jurnal Hasil Kegiatan Pengabdian Masyarakat Indonesia.

Jumadi and Sarah, 'Transformasi Digital Sistem E-Court Dalam Modernisasi Persidangan Kasus Hukum Pidana, Perdata, Dan Hukum Islam Di Indonesia' (2025) 5 Jurnal Ilmu Hukum, Humaniora dan Politik.

Lia H, 'UU PDP Dan Pelanggaran Data: Tindakan Yang Harus Diambil Perusahaan'' (*SiberMate*, 2024) <https://sibermate.com/hrmi/uu-pdp-dan-pelanggaran-data-tindakan-yang-harus-diambil-perusahaan> accessed 28 May 2025.

Luo Y, 'The Development of Online Courts in The Digital Age and The Prospect of Future Justice: Based on The Innovation of Judicial Methods in China and The United Kingdom' (2024) 42 Journal of Education Humanities and Social Sciences.

'Memahami Peran Data Protection Officer Dalam Ekosistem Pelindungan Data Pribadi' (*Asosiasi Praktisi Perlindungan Data Indonesia*, 2021) <https://appdi.or.id/memahami-peran-data-protection-officer-dalam-ekosistem-pelindungan-data-pribadi/> accessed 28 May 2025.

Muhktar and Lailam T, 'Implementasi Peradilan Elektronik Pada Pengadilan Negeri Dan Agama Di Daerah Istimewa Yogyakarta' (2024) 53 Jurnal Masalah-Masalah Hukum.

Naghmouchi M and others, 'Comparative Analysis of Technical and Legal Frameworks of Various National Digial Identity Solutions' [2023] arXiv:2310.01006 (cs.SE).

P. AA and Jatmiko L, 'Jaminan Kesehatan Dalam Hak Konstitusional Bagi Pekerja Migran Dalam Konstruksi Negara Kesejahteraan' 1 The Presecutor Law Review.

Prayuti Y, ‘Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce Dan Perlindungan Data Konsumen Di Indonesia’ (2025) 5 Jurnal Interpretasi Hukum.

Putra TI and Fibrianti N, ‘Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia’ (2024) 9 Lambung Mangkurat Law Journal.

Putra TI, Fibrianti N and Fakhrullah MR, ‘Data Protection Impact Assessment Indicators in Protecting Consumer Personal Data on E-Commerce Platforms’ (2024) 6 The Indonesian Journal of International Clinical Legal Education.

Rahmi T, ‘Transformasi Digital Dan Pengaruhnya Terhadap Budaya Organiasasi: Tinjauan Literatur Sistematis’ (2024) 1 Jurnal Manajemen AKuntansi dan Ilmu Ekonomi.

Ramadhani SA, ‘Komparasi Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa’ (2022) 3 Jurnal Hukum Lex Generalis.

Rasji and Priyono MYS, ‘Tantangan Terhadap Privasi Dan Kebebasan Berpendapat Di Indonesia Pada Era Digital: Analisis Pandangan Filsafat Hukum’ (2024) 5 Jurnal Hukum Lex Generalis.

Reiling D, *Teknologi Untuk Keadilan: Bagaimana Teknologi Informasi Dapat Mendukung Reformasi Pengadilan* (Alumni Penerbit Akademik 2009).

Riswandi BA and Gultom AM, ‘Protecting Our Mosts Valuable Personal Data: A Comparison Of Transborder Data Flow Laws In The European Union, United Kingdom, And Indonesia’ (2023) 5 Prophetic Law Review.

Rosadi SD, *Pembahasan UU Perlindungan Data Pribadi* (Sinar Grafika 2023).

Samosir A and Nababan R, ‘Tinjauan Hukum Terhadap Pelaksanaan Sidang Elektronik Di Pengadilan Negeri Medan Berdasarkan Putusan Pengadilan No.971/Pdt.G/2023/PN.MDN’ (2025) 2 HELIUM: Journal of Health Law Information and Humanities.

Setiawan H and others, ‘Digitalization of Legal Transformation on Judicial Review in the Constitutional Court’ (2024) 4 Journal of Human Rights, Culture and Legal System.

Sholehuddin N and others, ‘A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries’ (2024) 7 Journal of Muwafaqat.

Sofwan, Jayadi H and Rusnan, 'Kejelasan Perumusan Norma Dalam Pembentukan Undang-Undang (Kajian Terhadap Penggunaan Frasa Hukum Dalam Perumusan Norma Undang-Undang)' (2021) 2 Jurnal Risalah Kenotariatan.

Suadi A, *Sistem Pengawasan Badan Peradilan Indonesia* (Rajawali Press 2014).

Supancana IBR, *Berbagai Perspektif Harmonisasi Hukum Nasional Dan Hukum Internasional* (Penerbit Universitas Atma Jaya 2012).

Sutrisni NK and others, 'The Compliance of Governance on Family Data Protection Regulation' (2024) 4 Journal of Human Rights, Culture and Legal System.

Widaningrum A, *Regulatory Impact Analysis (Analisis Dampak Regulasi) : Konsep Dan Penerapannya* (Gadjah Mada University Press 2024).

HOW TO CITE: Dody Novizar Mardyansyah, Sukarmi, Adi Kusumaningrum, and Yenny Eta Widyanti, 'Harmonization of Personal Data Protection Principles With Electronic Justice Systems in Indonesia ' (2025) 40 Yuridika.