

Digital Surveillance and the Right to Privacy: A Comparative Study between Indonesia and the European Union

Author

Hajar Salamah Salsabila
Hariz¹, Siti Kunarti¹,
Akhmad Roja Badrus
Zaman²

¹ Faculty of Law,
Universitas Jenderal
Soedirman, Indonesia

² Universität Freiburg,
Germany

Corresponding Author:

* Hajar Salamah Salsabila
Hariz, Email:
salsabilahariz02@gmail.co
m

Data:

Received: Jan 28, 2026;
Accepted: Jun 02, 2026;
Published: Jun 18, 2026.

Keywords:

*Digital Surveillance;
Right to Privacy;
Personal Data
Protection;
Comparative Law.*

Abstract: The rapid expansion of digital surveillance technologies has intensified the tension between national security interests and the protection of individual privacy rights. This article examines the legal frameworks governing digital surveillance and the right to privacy through a comparative study of Indonesia and the European Union (EU). Employing a normative juridical approach with comparative legal analysis, the study reviews constitutional provisions, statutory regulations, judicial decisions, and international human rights instruments concerning data protection and state surveillance. The findings reveal that the European Union has established a comprehensive privacy regime through the General Data Protection Regulation (GDPR), the Charter of Fundamental Rights of the European Union, and robust judicial oversight, ensuring that surveillance measures comply with the principles of legality, necessity, and proportionality. In contrast, although Indonesia has strengthened its regulatory framework through the Personal Data Protection Law and electronic information legislation, significant challenges remain regarding institutional oversight, transparency, accountability, and effective legal remedies against unlawful surveillance. The study argues that Indonesia can enhance its digital governance by adopting a rights-based surveillance framework inspired by the EU model while accommodating its constitutional values and national security concerns. This comparative analysis contributes to the growing discourse on digital constitutionalism, privacy protection, and the development of balanced surveillance governance in the digital era.



©2026; This is an Open Access Research distributed under the term of the Creative Commons Attribution Licencee (<https://creativecommons.org/licenses/by-sa/4.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original works is properly cited.

INTRODUCTION

The unprecedented development of digital technologies has fundamentally transformed the relationship between the state, private corporations, and individuals.¹ Digital platforms, artificial intelligence, biometric identification systems, facial recognition technologies, and big data analytics have significantly enhanced governments' capacity to collect, process, and analyze personal information on an unprecedented scale. While these technological advancements have contributed to improving public services, strengthening national security, and combating cybercrime, they have simultaneously generated profound concerns regarding the protection of individual privacy. Digital surveillance has become an inevitable feature of contemporary governance, raising fundamental legal and ethical questions concerning the appropriate limits of state authority over personal data. Consequently, balancing national security objectives with the protection of fundamental rights has emerged as one of the most pressing legal challenges of the digital age.

The right to privacy has long been recognized as a fundamental human right within international human rights law. Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) explicitly prohibit arbitrary or unlawful interference with an individual's privacy, family, home, and correspondence. These international instruments establish privacy not merely as an individual interest but as a prerequisite for the exercise of other fundamental rights, including freedom of expression, freedom of association, and democratic participation. In the digital era, however, the traditional conception of privacy has evolved beyond physical spaces to encompass informational privacy, data autonomy, algorithmic transparency, and protection against pervasive digital monitoring. Consequently, legal systems worldwide are increasingly challenged to reinterpret constitutional privacy guarantees within rapidly changing technological environments.²

Digital surveillance encompasses a wide range of governmental practices involving the systematic collection, storage, monitoring, and analysis of electronic communications and personal information through digital technologies.³ Governments frequently justify surveillance measures as necessary tools for preventing terrorism, combating transnational crime, protecting cybersecurity, and maintaining public order. Nevertheless, extensive surveillance programs have raised significant concerns regarding excessive governmental intrusion, mass data collection, algorithmic profiling, and the potential abuse of surveillance powers. The expansion of surveillance capabilities has therefore intensified debates regarding the principles of legality, necessity, proportionality, accountability, and judicial oversight that should govern governmental access to citizens' personal data.

Within this global context, the European Union has emerged as one of the world's most influential jurisdictions in developing comprehensive legal protections for privacy and personal data. The enactment of the General Data Protection Regulation (GDPR) represents a

¹ Muhammad Maleno and Andriana Kusumawati, "Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights," *Indonesia Law College Association Law Journal* 3, no. 2 SE-Articles (December 9, 2024): 91–98, <https://ejournal.psthi.or.id/index.php/ILCALaw/article/view/21>.

² Valentina Ancillia Simbolon and Vishnu Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation," *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (December 30, 2022): 178, <https://doi.org/10.31314/pjia.11.2.178-190.2022>.

³ Muchamad Taufiq, Mochamad Reza Kurniawan, and Ananda Salsabila Kenyo, "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR," *International Journal of Business, Law, and Education* 6, no. 2 (July 30, 2025): 1260–68, <https://doi.org/10.56442/ijble.v6i2.1178>.

landmark achievement in establishing harmonized standards for personal data protection across member states. Supported by Article 8 of the Charter of Fundamental Rights of the European Union and extensive jurisprudence of the Court of Justice of the European Union (CJEU), the European legal framework emphasizes that data protection constitutes a fundamental right rather than merely a regulatory obligation. The GDPR introduces strict requirements concerning consent, transparency, data minimization, purpose limitation, accountability, and effective legal remedies, thereby creating one of the most sophisticated privacy governance regimes in the contemporary world.⁴

In contrast, Indonesia has experienced rapid digital transformation accompanied by increasing governmental reliance on electronic information systems for administrative governance, public service delivery, and national security operations.⁵ The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) represents a significant milestone in Indonesia's effort to modernize its data protection framework. The law complements existing regulations, including the Electronic Information and Transactions Law (ITE Law), and reflects Indonesia's commitment to strengthening personal data governance. Nevertheless, concerns remain regarding fragmented institutional arrangements, limited supervisory mechanisms, overlapping regulatory authorities, and the absence of sufficiently independent oversight institutions capable of ensuring accountability for digital surveillance practices. These challenges indicate that legislative reform alone may be insufficient without corresponding institutional and procedural safeguards.

Recent developments further demonstrate the growing complexity of privacy protection in Indonesia. The expansion of digital identity systems, electronic government services, biometric verification, mobile applications, financial technology, and artificial intelligence has substantially increased the volume of personal data processed by both public institutions and private entities. At the same time, incidents involving data breaches, unauthorized information disclosure, and allegations of unlawful digital surveillance have intensified public concerns regarding cybersecurity and governmental accountability. These developments illustrate that technological innovation simultaneously generates opportunities for efficient governance while exposing individuals to heightened risks of privacy violations, identity theft, discriminatory profiling, and excessive state monitoring.⁶

Despite the increasing scholarly attention devoted to digital privacy, existing literature continues to exhibit several important limitations.⁷ First, many studies focus exclusively on either personal data protection or cybersecurity regulation without comprehensively examining digital surveillance as a constitutional and human rights issue. Second, comparative legal analyses between Indonesia and the European Union remain relatively limited, despite the significant influence of European privacy principles on emerging data protection legislation worldwide. Third, previous research frequently concentrates on statutory analysis while paying insufficient attention to the broader normative principles governing surveillance,

⁴ Rudi Natamiharja and Ikhsan Setiawan, "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France," *Jambe Law Journal* 7, no. 1 (July 30, 2024): 233–51, <https://doi.org/10.22437/home.v7i1.349>.

⁵ Dona Budi Kharisma and Alvalerie Diakanza, "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union," *International Journal of Human Rights in Healthcare* 17, no. 2 (May 16, 2024): 157–69, <https://doi.org/10.1108/IJHRH-04-2022-0035>.

⁶ Loso Judijanto, Nuryati Solapari, and Irman Putra, "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia," *The Easta Journal Law and Human Rights* 3, no. 01 SE-Articles (October 31, 2024): 20–29, <https://doi.org/10.58812/eslhr.v3i01.351>.

⁷ Rahayudin Rahayudin et al., "Digital Sovereignty and The Right to Data: A Comparative Study Between Indonesia, The European Union, and The United States," *Journal of Law and Social Politics* 3, no. 2 SE-Articles (December 22, 2025): 84–96, <https://doi.org/10.59261/jlsp.v3i2.71>.

including legality, necessity, proportionality, transparency, accountability, and effective judicial review. Consequently, a substantial research gap remains concerning how different legal systems reconcile competing interests between national security and the protection of fundamental rights.

This article seeks to address these gaps by conducting a comparative legal analysis of digital surveillance and the right to privacy in Indonesia and the European Union. The comparison is particularly relevant because both jurisdictions recognize privacy as a protected legal interest while adopting significantly different regulatory structures, institutional mechanisms, and constitutional traditions. The European Union emphasizes comprehensive rights-based governance supported by supranational institutions and independent supervisory authorities, whereas Indonesia continues to develop its regulatory framework within a constitutional system balancing democratic governance, national security, and administrative modernization. Examining these contrasting approaches provides valuable insights into the strengths, weaknesses, and future directions of privacy governance in emerging digital societies.⁸

Methodologically, this research employs a normative juridical approach using comparative legal analysis. Primary legal materials include constitutional provisions, statutory regulations, international human rights instruments, judicial decisions, and official policy documents governing digital surveillance and personal data protection.⁹ Secondary materials consist of scholarly literature, legal commentaries, journal articles, and comparative studies addressing privacy rights, digital governance, cybersecurity, and constitutional law. The comparative analysis evaluates substantive legal principles, institutional arrangements, enforcement mechanisms, and judicial safeguards in order to identify convergences and divergences between the Indonesian and European legal frameworks.

This study argues that effective digital surveillance governance requires a legal framework that simultaneously protects national security and safeguards fundamental rights through robust institutional accountability.¹⁰ Drawing lessons from the European Union's rights-based regulatory model, this article proposes that Indonesia should strengthen independent oversight mechanisms, improve judicial authorization procedures, enhance transparency obligations, and reinforce effective remedies for unlawful surveillance while respecting constitutional values and domestic legal traditions. By integrating comparative constitutional law, international human rights law, and digital governance perspectives, this study contributes to the expanding scholarship on digital constitutionalism and offers policy recommendations for developing a more balanced, accountable, and human rights-oriented surveillance regime in Indonesia.

RESEARCH METHODS

This study employs a normative juridical research design using a comparative legal approach to examine the regulatory frameworks governing digital surveillance and the

⁸ Atmari Atmari and Sudjai Sudjai, "Digital Workplace Monitoring and Employees' Privacy Rights in Indonesia," *Jurnal Mahkamah: Kajian Ilmu Hukum Dan Hukum Islam* 11, no. 1 SE-Articles (June 9, 2026): 151–70, <https://doi.org/10.25217/jm.v11i1.7719>.

⁹ Ridwan Tahir and Titie Yustisia Lestari, "Children's Digital Rights: An In-Depth Analysis of Indonesia, Europe, and the US," *Eduvest - Journal of Universal Studies* 5, no. 2 (February 20, 2025): 1942–64, <https://doi.org/10.59188/eduvest.v5i2.50770>.

¹⁰ A Syafik, "Digital Surveillance and the Right to Privacy: Legal Challenges of State Authority in the Era of Big Data Governance," *International Journal of Law and Political Authority* 1, no. 2 SE-Articles (April 7, 2026): 10–26, <https://researchfrontiers.id/corpus/article/view/123>.

protection of the right to privacy in Indonesia and the European Union.¹¹ Normative legal research is appropriate because the analysis focuses on legal norms, constitutional principles, statutory regulations, judicial interpretations, and international human rights instruments rather than empirical observations. The comparative approach enables a systematic examination of similarities and differences between the two jurisdictions in regulating state surveillance, personal data protection, and privacy rights. Primary legal materials consist of the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 on Personal Data Protection, the Electronic Information and Transactions Law and its amendments, the General Data Protection Regulation (GDPR), the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights (ECHR), the International Covenant on Civil and Political Rights (ICCPR), and relevant decisions of the Constitutional Court of Indonesia, the Court of Justice of the European Union (CJEU), and the European Court of Human Rights (ECtHR). Secondary legal materials include scholarly books, peer-reviewed journal articles, policy papers, official reports, and legal commentaries addressing digital surveillance, privacy rights, constitutional law, and comparative data protection governance.

The collected legal materials were analyzed through qualitative doctrinal analysis and functional comparative legal methods. The doctrinal analysis identifies the legal principles governing digital surveillance, including legality, legitimate purpose, necessity, proportionality, transparency, accountability, judicial oversight, and effective legal remedies. Subsequently, the comparative analysis evaluates how these principles are institutionalized and enforced within the legal systems of Indonesia and the European Union by examining their constitutional foundations, legislative structures, supervisory authorities, enforcement mechanisms, and judicial safeguards. The findings are interpreted using a human rights-based framework to assess the extent to which each jurisdiction balances national security interests with the protection of fundamental privacy rights. Finally, the study formulates normative recommendations for strengthening Indonesia's digital surveillance governance by adapting relevant best practices from the European Union while taking into account Indonesia's constitutional framework, legal traditions, and socio-political context.

ANALYSIS AND DISCUSSION

The Legal Framework of Digital Surveillance and Privacy Protection in Indonesia and the European Union

Digital surveillance has become a defining characteristic of contemporary governance, reflecting the growing reliance of states on information and communication technologies to monitor, collect, process, and analyze personal data.¹² Unlike traditional surveillance, which primarily involved physical observation or targeted interception, digital surveillance encompasses sophisticated technologies such as artificial intelligence, biometric identification, facial recognition systems, metadata analysis, geolocation tracking, and algorithmic profiling. These technologies have significantly enhanced governmental capacity to address national security threats, cybercrime, terrorism, and public emergencies. However, they have also expanded the state's ability to intrude into individuals' private lives, thereby creating complex legal challenges regarding the permissible limits of surveillance in democratic societies.

From a legal perspective, digital surveillance is no longer understood merely as an administrative or technological activity but as a constitutional issue involving the protection of fundamental rights. Modern constitutional democracies increasingly recognize that

¹¹ John Creswell and J David Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Sage publications, 2017).

¹² Brahmantyo Suryo Satwiko, "Privacy and Data Protection: Indonesian Legal Framework," *Corporate and Trade Law Review* 1, no. 2 (2021): 106–8.

unrestricted governmental access to personal information threatens individual autonomy, freedom of expression, freedom of association, and democratic participation. Consequently, international human rights law requires surveillance measures to comply with universally accepted principles of legality, legitimate purpose, necessity, proportionality, accountability, and effective judicial oversight. These principles serve as normative benchmarks for evaluating whether state surveillance constitutes a legitimate exercise of public authority or an unlawful interference with individual privacy.

Indonesia has gradually incorporated privacy protection into its constitutional framework despite the absence of an explicit constitutional provision specifically addressing digital privacy. The constitutional basis for privacy protection is generally derived from several provisions of the 1945 Constitution, particularly Article 28G paragraph (1), which guarantees protection of personal dignity, security, and property, as well as Article 28F, which recognizes every person's right to communicate and obtain information through available channels. These constitutional guarantees have increasingly been interpreted as encompassing informational privacy, especially in response to the rapid expansion of digital technologies and electronic communication systems.¹³ Accordingly, constitutional protection provides an important normative foundation for regulating governmental access to personal data.

The Constitutional Court of Indonesia has played an increasingly important role in developing constitutional interpretations concerning privacy and electronic communications. Through several landmark decisions concerning electronic interception, telecommunications, and constitutional rights, the Court has emphasized that restrictions on privacy must be based on clear statutory authority and implemented through lawful procedures consistent with constitutional guarantees. The Court has further acknowledged that electronic surveillance constitutes an interference with constitutional rights and therefore requires strict legal justification. Although the Court has not yet established a comprehensive constitutional doctrine equivalent to European privacy jurisprudence, its decisions demonstrate a gradual recognition that surveillance powers should remain subject to constitutional limitations and judicial scrutiny.

Indonesia's legislative framework governing digital surveillance has developed significantly with the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). As Indonesia's first comprehensive personal data protection legislation, the PDP Law establishes legal principles governing the collection, processing, storage, transfer, and deletion of personal data by both public institutions and private entities. The law introduces fundamental concepts such as lawful processing, purpose limitation, data accuracy, transparency, accountability, and data subject rights. Nevertheless, the legislation primarily focuses on personal data governance rather than comprehensively regulating governmental surveillance activities, leaving several issues concerning intelligence operations, national security exceptions, and independent oversight insufficiently addressed.

The Electronic Information and Transactions Law (ITE Law), together with its implementing regulations, constitutes another important component of Indonesia's digital regulatory framework.¹⁴ Originally enacted to facilitate electronic commerce and digital transactions, the legislation also provides legal mechanisms concerning electronic evidence, cybercrime investigations, and electronic information management. In practice, however, the ITE Law has generated considerable debate because several provisions permit governmental

¹³ Heppy Endah Palupy, "Privacy and Data Protection: Indonesia Legal Framework," *Journal Master Law and Technology Di Universiteit van Tilburg, Tilburg*, 2011.

¹⁴ Junaidi Eko Widodo, Atma Suganda, and Tubagus Achmad Darodjat, "DATA PRIVACY AND CONSTITUTIONAL RIGHTS IN INDONESIA," *PENA LAW: International Journal of Law* 2, no. 2 (September 30, 2024), <https://doi.org/10.56107/penalaw.v2i2.187>.

authorities to access electronic information for law enforcement purposes. Critics argue that ambiguities surrounding electronic interception procedures, judicial authorization, and institutional accountability create uncertainty regarding the balance between legitimate security interests and constitutional privacy protection.¹⁵

Beyond the PDP Law and the ITE Law, digital surveillance in Indonesia is also influenced by sectoral legislation governing telecommunications, cybersecurity, intelligence, and national security. These laws authorize various governmental institutions to conduct surveillance activities under specific circumstances related to criminal investigations, counterterrorism operations, and public security. However, the coexistence of multiple regulatory instruments has resulted in fragmented governance characterized by overlapping institutional authority and inconsistent oversight mechanisms. The absence of a fully independent supervisory authority further limits public accountability and raises concerns regarding the effectiveness of legal remedies available to individuals subjected to unlawful surveillance.

In contrast to Indonesia's fragmented regulatory model, the European Union has developed one of the most comprehensive legal frameworks for privacy and personal data protection worldwide. The cornerstone of this framework is the General Data Protection Regulation (GDPR), which entered into force in 2018 and harmonized data protection standards across all EU member states. The GDPR recognizes personal data protection as a fundamental right and establishes comprehensive obligations for both public authorities and private organizations processing personal information. Its regulatory architecture is founded upon principles of lawfulness, fairness, transparency, purpose limitation, data minimization, storage limitation, integrity, confidentiality, and accountability, thereby creating a coherent legal regime governing digital information processing.¹⁶

The constitutional foundation of privacy protection within the European Union extends beyond the GDPR. Article 7 of the Charter of Fundamental Rights of the European Union guarantees respect for private and family life, while Article 8 explicitly recognizes the protection of personal data as an autonomous fundamental right. These constitutional guarantees are reinforced by the European Convention on Human Rights (ECHR), particularly Article 8, which protects individuals against arbitrary interference with private life, correspondence, and communications. Collectively, these instruments establish a robust constitutional framework requiring any surveillance measure to satisfy strict conditions of legality, necessity, proportionality, and democratic legitimacy before governmental authorities may interfere with individual privacy.

Digital surveillance conducted for criminal justice and national security purposes within the European Union is additionally regulated through the Law Enforcement Directive (Directive (EU) 2016/680). Unlike the GDPR, which primarily governs general personal data processing, the Directive specifically addresses data processing by competent authorities for the prevention, investigation, detection, and prosecution of criminal offences. The Directive seeks to reconcile effective law enforcement with the protection of fundamental rights by imposing safeguards concerning lawful processing, independent supervision, security measures, data accuracy, and effective judicial remedies. Consequently, the European legal framework differentiates between ordinary administrative data processing and surveillance conducted for public security purposes while maintaining consistent human rights standards across both domains.

Judicial institutions have significantly contributed to shaping the European legal doctrine governing digital surveillance. The Court of Justice of the European Union (CJEU) has

¹⁵ Tahir and Lestari, "Children's Digital Rights: An In-Depth Analysis of Indonesia, Europe, and the US."

¹⁶ Syafik, "Digital Surveillance and the Right to Privacy: Legal Challenges of State Authority in the Era of Big Data Governance."

repeatedly invalidated legislative measures permitting indiscriminate or mass data retention on the grounds that they violate the principles of proportionality and fundamental rights protection. Similarly, the European Court of Human Rights (ECtHR) has consistently held that state surveillance must be accompanied by adequate legal safeguards, independent authorization procedures, effective oversight mechanisms, and accessible judicial remedies. Through this extensive jurisprudence, both courts have established that national security considerations cannot justify unrestricted surveillance powers and that democratic societies require continuous judicial supervision over governmental access to personal information.

The comparative analysis demonstrates that Indonesia and the European Union share a common recognition that privacy constitutes a fundamental legal right deserving constitutional protection.¹⁷ Nevertheless, the two jurisdictions adopt significantly different regulatory approaches in implementing that principle. Indonesia primarily relies on sectoral legislation and evolving constitutional interpretation, resulting in fragmented surveillance governance and relatively limited institutional oversight. By contrast, the European Union has constructed an integrated rights-based framework that combines constitutional guarantees, comprehensive legislation, independent supervisory authorities, and active judicial review. These differences indicate that while both legal systems acknowledge the importance of privacy in the digital era, the European Union places greater emphasis on institutional accountability and enforceable human rights safeguards, whereas Indonesia continues to strengthen its regulatory and institutional architecture to achieve a more balanced relationship between national security and the protection of individual privacy.

Comparative Analysis of State Surveillance, Judicial Oversight, and Privacy Protection

The comparative analysis reveals that Indonesia and the European Union adopt fundamentally different legal philosophies in regulating digital surveillance.¹⁸ While both jurisdictions acknowledge that surveillance is necessary for maintaining national security, combating cybercrime, and protecting public order, they differ considerably in how they balance these objectives with the protection of individual privacy. The European Union approaches surveillance through a rights-based legal framework that places fundamental rights at the center of regulatory design, whereas Indonesia primarily regulates surveillance through a security-oriented legal framework in which privacy protection is progressively developing but remains secondary to broader governmental security objectives. These differences are reflected in legislative structures, institutional arrangements, judicial oversight, and the implementation of fundamental legal principles.

The first significant distinction concerns the legal basis governing digital surveillance. Indonesia regulates surveillance through multiple sectoral statutes, including the Personal Data Protection Law, the Electronic Information and Transactions Law, telecommunications legislation, intelligence legislation, criminal procedure laws, and various implementing regulations. Although these legal instruments collectively provide a regulatory basis for digital surveillance, they operate independently and often contain overlapping or inconsistent provisions. Consequently, the Indonesian legal framework remains fragmented, making it difficult to establish a coherent system governing governmental access to personal data and electronic communications.¹⁹

By contrast, the European Union has developed an integrated legal framework in which

¹⁷ Satwiko, "Privacy and Data Protection: Indonesian Legal Framework."

¹⁸ Pawan Bindal and Ramveer Singh, "Survival of Right to Privacy under Administrative Surveillance: A Comparative Legal Study," *Journal of Humanities and Education Development* 8, no. 2 (2026): 29–40.

¹⁹ Konrad Lachmayer and Normann Witzleb, "The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective," *UNSWLJ* 37 (2014): 748.

surveillance-related regulation is systematically coordinated through constitutional principles, the General Data Protection Regulation (GDPR), the Law Enforcement Directive, the Charter of Fundamental Rights of the European Union, and the European Convention on Human Rights.²⁰ Rather than regulating surveillance through isolated statutory provisions, the EU establishes a comprehensive legal architecture in which all public authorities are required to comply with common data protection principles and fundamental rights standards. This harmonized framework promotes legal certainty, regulatory consistency, and greater protection of individual privacy across member states.

A second major distinction concerns institutional oversight. Effective surveillance governance requires independent institutions capable of supervising governmental access to personal information while ensuring compliance with legal standards.²¹ In Indonesia, supervisory responsibilities remain dispersed among several governmental agencies with differing mandates and institutional interests. Although the Personal Data Protection Law introduces mechanisms for data protection governance, the institutional structure has not yet produced an entirely independent supervisory authority possessing sufficient legal autonomy, investigative powers, and enforcement capacity comparable to international best practices. This institutional fragmentation limits public accountability and weakens external oversight over surveillance activities.

The European Union, on the other hand, has established a sophisticated institutional oversight mechanism through independent Data Protection Authorities (DPAs) operating within each member state. These authorities possess statutory independence from executive governments and are responsible for monitoring compliance with data protection legislation, investigating complaints, imposing administrative sanctions, and ensuring accountability in both public and private sectors. Their independence constitutes a fundamental safeguard against arbitrary governmental interference with individual privacy and reinforces public confidence in surveillance governance.²²

Institutional coordination within the European Union is further strengthened through the European Data Protection Board (EDPB), which promotes consistent application of data protection law across member states. The EDPB issues binding decisions, regulatory guidance, interpretative opinions, and best practice recommendations concerning privacy and surveillance issues.²³ This supranational coordination mechanism minimizes regulatory divergence while enhancing legal certainty throughout the European Union. Indonesia currently lacks a comparable national coordinating institution with similar independence and regulatory authority capable of harmonizing surveillance governance across different governmental sectors.

The third area of comparison concerns judicial control over surveillance activities. Judicial oversight represents one of the most important safeguards against abuse of

²⁰ Reva Naidu, "THE RIGHT TO PRIVACY AND MASS SURVEILLANCE: COMPARATIVE ANALYSIS POST-2020.," *New York University Journal of International Law & Politics* 58, no. 1 (2025): 263.

²¹ I. S. Rubinstein, G. T. Nojeim, and R. D. Lee, "Systematic Government Access to Personal Data: A Comparative Analysis," *International Data Privacy Law* 4, no. 2 (May 1, 2014): 96–119, <https://doi.org/10.1093/idpl/ipu004>.

²² TJ McIntyre, "Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective," in *Judges as Guardians of Constitutionalism and Human Rights* (Edward Elgar Publishing, 2016), <https://doi.org/10.4337/9781785365867.00014>.

²³ Arifa Zahra, "Algorithmic Surveillance and the Erosion of Privacy: Reconciling National Security and Human Rights in the Digital Era - A Comparative Study of the USA and UAE," in *2025 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)* (IEEE, 2025), 633–38, <https://doi.org/10.1109/ICCIKE67021.2025.11318249>.

surveillance powers because it subjects executive actions to independent legal scrutiny.²⁴ In Indonesia, judicial review primarily operates through constitutional adjudication before the Constitutional Court or judicial examination of administrative actions after alleged violations have occurred. However, prior judicial authorization for surveillance activities remains relatively limited, and statutory procedures governing interception, digital monitoring, and access to electronic information are not always accompanied by sufficiently transparent judicial approval mechanisms. As a result, executive agencies frequently exercise substantial discretion in conducting surveillance operations.

The European Union applies a significantly more rigorous system of judicial supervision. Both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR) have consistently required surveillance measures to satisfy strict constitutional and human rights standards before governmental authorities may interfere with private communications. Judicial authorization frequently constitutes a prerequisite for intrusive surveillance activities, while courts routinely assess whether governmental actions satisfy the principles of legality, necessity, and proportionality. Individuals whose privacy rights are violated also possess effective legal remedies through national courts and supranational judicial institutions, thereby strengthening accountability and ensuring meaningful protection against unlawful surveillance.²⁵

Another important distinction concerns the implementation of the principle of legality. In both jurisdictions, surveillance activities must possess a legal basis established through statutory legislation. Nevertheless, the European Union interprets legality more substantively by requiring surveillance legislation to be precise, foreseeable, accessible, and accompanied by sufficient safeguards against arbitrary governmental action. Indonesian legislation likewise requires statutory authorization, yet fragmented regulatory provisions and overlapping institutional mandates occasionally generate legal uncertainty regarding the scope of surveillance powers, institutional competence, and procedural guarantees. Consequently, the practical implementation of legality remains stronger and more consistent within the European Union.²⁶

The principles of necessity and proportionality further illustrate contrasting regulatory approaches. Under European law, surveillance measures are permitted only when they are strictly necessary to achieve legitimate objectives and when less intrusive alternatives are unavailable. Courts routinely conduct proportionality assessments by balancing national security interests against the severity of interference with individual rights. Indonesia increasingly recognizes these principles through constitutional interpretation and data protection legislation; however, explicit proportionality assessments are not uniformly integrated into surveillance authorization procedures. As a result, surveillance practices continue to emphasize security considerations more strongly than comprehensive human rights balancing.

Differences are equally apparent in the implementation of transparency, accountability, data minimization, and purpose limitation. The GDPR imposes extensive obligations requiring public authorities to collect only data necessary for specified legitimate purposes, maintain transparency concerning processing activities, ensure institutional accountability, and provide

²⁴ Agnidipto Tarafder, "Surveillance, Privacy and Technology: A Comparative Critique of the Laws of USA And India," *Journal of the Indian Law Institute*, 2015, 550–78.

²⁵ Stency Mariya Mark and Aaratrika Pandey, "Shielding Privacy in the Surveillance Era," *Law, State and Telecommunications Review* 16, no. 2 (October 16, 2024): 215–35, <https://doi.org/10.26512/lstr.v16i2.51916>.

²⁶ M Salman, "Digital Surveillance and the Right to Privacy under International Human Rights Law: A Comparative Study of State Practices," *Pinnacle in Social Sciences* 1, no. 01 SE-Articles (n.d.): 01–10, <https://ojs.pinnaclearsearchcompany.com/index.php/PSS/article/view/1>.

individuals with enforceable rights over their personal information. Independent audits, supervisory investigations, breach notification requirements, and administrative sanctions collectively reinforce these obligations. Indonesia has adopted similar principles through the Personal Data Protection Law, yet practical implementation remains constrained by institutional capacity, limited supervisory independence, and the absence of comprehensive transparency mechanisms governing state surveillance activities. Consequently, enforcement remains less effective than the European model.

The overall comparison demonstrates that the European Union has constructed a mature rights-based surveillance governance model in which constitutional guarantees, integrated legislation, independent supervisory authorities, robust judicial oversight, and enforceable legal remedies collectively protect individual privacy. Indonesia has made significant progress through constitutional interpretation and legislative reform, particularly with the enactment of the Personal Data Protection Law, but its surveillance framework continues to reflect a predominantly security-oriented governance model characterized by fragmented regulation, developing institutional oversight, and comparatively limited judicial safeguards. These findings suggest that future legal reform in Indonesia should prioritize institutional independence, integrated regulatory harmonization, judicial authorization mechanisms, and stronger implementation of proportionality and accountability principles to achieve a more balanced relationship between national security and the protection of fundamental privacy rights.

Towards a Rights-Based Digital Surveillance Governance Model for Indonesia

The comparative findings presented in the previous sections demonstrate that Indonesia has made significant progress in regulating personal data protection through constitutional interpretation and legislative reform, particularly following the enactment of Law Number 27 of 2022 concerning Personal Data Protection.²⁷ Nevertheless, the existing legal framework remains fragmented, with surveillance governance primarily shaped by sectoral legislation that emphasizes national security and law enforcement objectives. This study argues that future legal reform should move beyond fragmented regulatory adjustments toward a comprehensive governance model that simultaneously safeguards national security and fundamental privacy rights. Drawing upon comparative insights from the European Union, this article proposes a Rights-Based Digital Surveillance Governance Model as a normative framework for strengthening Indonesia's digital constitutionalism.

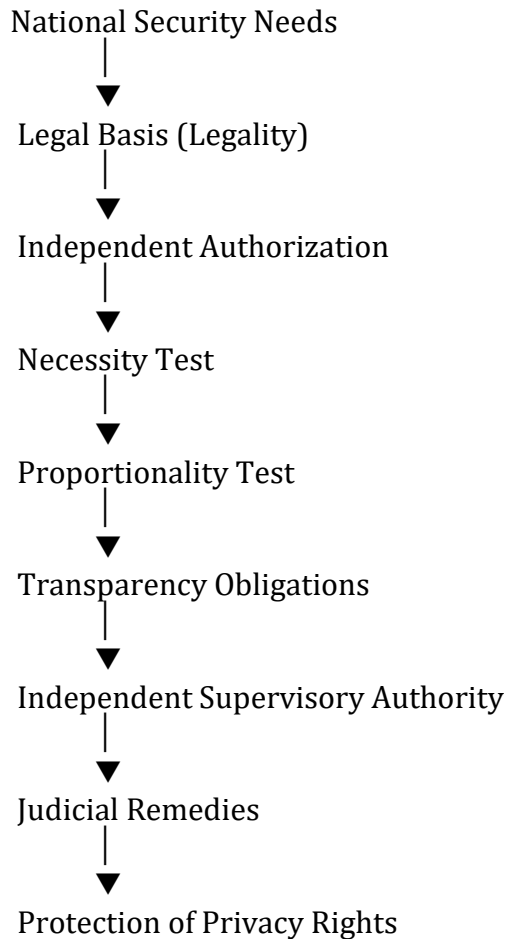
The proposed model does not reject the legitimacy of state surveillance. Rather, it recognizes that digital surveillance constitutes a necessary governmental function in addressing terrorism, cybercrime, transnational organized crime, and emerging digital threats. However, surveillance should not be regarded as an unlimited executive power. Instead, every surveillance measure must be embedded within a legal framework that prioritizes constitutional rights, democratic accountability, and judicial supervision. Accordingly, the proposed governance model integrates security interests with human rights principles through a sequential system of legal safeguards that ensures surveillance remains proportionate, transparent, and accountable.²⁸

The governance model developed in this study consists of eight interconnected

²⁷ Amira Paripurna, Sebastien Lafrance, and Masitoh Indriani, "Intelligence Surveillance, Counterterrorism, and the Right to Privacy in Indonesia and Canada," *JSEHR* 9 (2025): 304.

²⁸ Aris Sarjito and Suyono Thamrin, "DIGITAL GOVERNANCE REFORM IN INDONESIA: A COMPARATIVE ANALYSIS WITH ESTONIA," *Вопросы Государственного и Муниципального Управления*, no. 5 (2026): 92–116.

components arranged as a normative decision-making process.²⁹ Each component functions as a legal safeguard designed to prevent arbitrary governmental interference with individual privacy while preserving the effectiveness of legitimate law enforcement activities. The proposed framework is illustrated as follows:



The first component is constitutional protection, which positions privacy as a fundamental constitutional right rather than merely an administrative interest. Constitutional recognition ensures that privacy serves as the normative foundation upon which all surveillance legislation must be evaluated.³⁰ In Indonesia, Articles 28G and 28F of the 1945 Constitution provide an important constitutional basis for protecting personal security and communication rights. Nevertheless, future constitutional interpretation should explicitly recognize informational privacy as an essential element of democratic governance. By elevating privacy to the status of a constitutional benchmark, all surveillance legislation would become subject to constitutional review whenever disproportionate restrictions upon individual rights occur.

The second component is legal basis (legality). Every surveillance activity should be conducted exclusively under clear statutory authority enacted through democratic legislative procedures. The legality principle requires surveillance laws to define precisely the circumstances permitting surveillance, the categories of data that may be collected, the

²⁹ Atin Prabandari, Emma Seruni Ketaren, and Balya Arung Segara, "Rethinking Digital Migration Governance in Southeast Asia: Protecting or Restricting Human Rights?," *JSEHR* 9 (2025): 248.

³⁰ Dwi Saleha et al., "Legal Analysis of Human Rights Protection within Smart City Policy Implementation in Indonesia," *The Easta Journal Law and Human Rights* 4, no. 01 (October 31, 2025): 63–73, <https://doi.org/10.58812/eslhr.v4i01.778>.

competent authorities responsible for implementation, procedural safeguards, retention periods, and mechanisms for accountability. Fragmented sectoral regulations should therefore be harmonized into a coherent legal framework that minimizes overlapping authority and legal uncertainty. Such harmonization would strengthen legal certainty while limiting discretionary executive power.³¹

The third component involves independent surveillance authorization. One of the principal weaknesses identified within Indonesia's current regulatory framework is the concentration of surveillance authorization within executive institutions.³² The proposed model recommends that highly intrusive surveillance measures—including interception of electronic communications, access to encrypted data, and large-scale digital monitoring—should require prior authorization from an independent judicial authority or another legally autonomous institution. Independent authorization functions as an *ex ante* safeguard by ensuring that surveillance requests undergo impartial legal scrutiny before implementation. This mechanism substantially reduces the risk of politically motivated or arbitrary surveillance.

The fourth component is the necessity test, which requires governmental authorities to demonstrate that surveillance constitutes the least restrictive means of achieving a legitimate public objective. Under this principle, surveillance should only be authorized when alternative investigative methods are demonstrably insufficient to prevent or investigate serious threats. National security or public order should not automatically justify unrestricted monitoring of electronic communications. Instead, competent authorities must establish objective evidence demonstrating that surveillance is genuinely required under the specific factual circumstances of each individual case. Incorporating the necessity test into statutory procedures would significantly strengthen constitutional protection against excessive governmental intrusion.³³

Closely related to necessity is the proportionality test, which represents the fifth component of the proposed model. Proportionality requires decision-makers to balance the anticipated public benefits of surveillance against the degree of interference with individual privacy rights.³⁴ Even where surveillance pursues legitimate objectives, excessive data collection or indiscriminate monitoring may violate constitutional guarantees if the intrusion exceeds what is reasonably required. Inspired by the jurisprudence of the Court of Justice of the European Union and the European Court of Human Rights, Indonesia should institutionalize proportionality review within judicial authorization procedures, enabling courts to evaluate whether surveillance measures remain narrowly tailored to their intended objectives.

The sixth component concerns data minimization and purpose limitation. Government institutions should only collect personal data strictly necessary for achieving specifically defined legal purposes. Excessive data accumulation, indefinite storage, or secondary use of surveillance information beyond its original objective should be prohibited unless expressly authorized by law. The Personal Data Protection Law already incorporates these principles for general data processing; however, their application should be extended explicitly to surveillance activities conducted by intelligence agencies, law enforcement institutions, and other public authorities. Strengthening data minimization would reduce unnecessary governmental access to personal information while improving public trust in digital

³¹ Prabandari, Ketaren, and Segara, "Rethinking Digital Migration Governance in Southeast Asia: Protecting or Restricting Human Rights?"

³² Yosua Nicholas Tan, Abdurrahman Alhakim, and Nurlaily Nurlaily, "Human Rights Protection in the Digital Sphere: The Problematics of Legal Certainty and Its Relevance to the SDGs," *SIGn Jurnal Hukum* 8, no. 1 (April 6, 2026): 18–31, <https://doi.org/10.37276/sjh.v8i1.652>.

³³ Paripurna, Lafrance, and Indriani, "Intelligence Surveillance, Counterterrorism, and the Right to Privacy in Indonesia and Canada."

³⁴ Iffatin Nur et al., "Wisdom in the Digital Era: Bridging Human Rights, Indonesian Cyber Law, and Progressive Fiqh," *The Journal of Society and Media* 10, no. 1 (April 30, 2026): 315–40, <https://doi.org/10.26740/jsm.v10n1.p315-340>.

governance.

The seventh component establishes an independent supervisory authority responsible for monitoring surveillance practices. Comparative analysis demonstrates that effective privacy protection depends not only upon legislation but also upon independent institutions possessing sufficient authority to investigate complaints, conduct compliance audits, review surveillance practices, impose administrative sanctions, and publish periodic reports regarding governmental surveillance activities. Establishing an autonomous supervisory authority—functionally comparable to the Data Protection Authorities operating within the European Union—would significantly enhance institutional accountability while strengthening democratic oversight over executive surveillance powers.

The eighth component integrates judicial remedies, transparency, and accountability into a comprehensive system of post-surveillance oversight. Individuals who believe their privacy rights have been violated should possess accessible legal mechanisms to challenge unlawful surveillance before independent courts and obtain appropriate remedies, including compensation, cessation of unlawful processing, or deletion of unlawfully obtained data. At the institutional level, transparency should be reinforced through periodic public reporting, independent audits, parliamentary oversight, and mandatory disclosure of aggregate surveillance statistics where national security considerations permit. Such mechanisms promote public confidence by ensuring that surveillance activities remain subject to continuous democratic scrutiny rather than executive discretion alone.

The Rights-Based Digital Surveillance Governance Model proposed in this study represents the principal theoretical contribution of the research.³⁵ Unlike existing approaches that primarily emphasize either national security or personal data protection independently, this model integrates constitutional rights, legality, independent authorization, necessity, proportionality, data minimization, institutional oversight, judicial remedies, transparency, and democratic accountability into a unified governance framework. By adapting relevant elements of the European Union's rights-based regulatory approach while respecting Indonesia's constitutional structure and legal traditions, the model provides a practical roadmap for future legislative reform. Ultimately, this framework demonstrates that effective digital surveillance and robust privacy protection are not mutually exclusive objectives but complementary pillars of democratic digital governance founded upon the rule of law, respect for human rights, and accountable public administration.

CONCLUSION

This study demonstrates that Indonesia and the European Union share a common constitutional commitment to protecting the right to privacy in the digital era, yet they differ substantially in the legal and institutional approaches adopted to regulate digital surveillance. The comparative analysis reveals that the European Union has developed a comprehensive rights-based surveillance governance framework through the integration of the General Data Protection Regulation (GDPR), the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights, independent Data Protection Authorities, and robust judicial oversight by the Court of Justice of the European Union and the European Court of Human Rights. In contrast, Indonesia's regulatory framework remains relatively fragmented, relying on sectoral legislation such as the Personal Data Protection Law, the Electronic Information and Transactions Law, and other security-related statutes. Although these legal

³⁵ EN Dewi, "The Right to Be Forgotten and Digital Reputation: A Normative Analysis within Indonesian Cyber Law," *Lex Recta: Journal of Law and Normative Justice* 1, no. 1 SE-Articles (March 4, 2026): 31–39, <https://sovereignresearch.org/lex-recta/article/view/49>.

instruments have strengthened the protection of personal data and constitutional privacy rights, challenges persist regarding institutional independence, regulatory harmonization, judicial authorization, transparency, accountability, and effective legal remedies against unlawful surveillance. Consequently, Indonesia's current surveillance governance continues to reflect a predominantly security-oriented approach, while the European Union has institutionalized a more mature rights-based model grounded in constitutionalism and human rights protection. Building upon these findings, this study proposes a Rights-Based Digital Surveillance Governance Model as its principal theoretical contribution to the literature on digital privacy and comparative constitutional law. The proposed framework integrates constitutional protection of privacy, legality, independent surveillance authorization, necessity and proportionality assessments, data minimization, purpose limitation, independent supervisory authorities, judicial remedies, transparency, and democratic accountability into a coherent governance structure capable of balancing national security interests with the protection of fundamental rights. Rather than treating security and privacy as competing objectives, the model conceptualizes them as complementary principles within democratic digital governance under the rule of law. Accordingly, future legal reform in Indonesia should prioritize regulatory harmonization, strengthen independent oversight institutions, institutionalize judicial authorization mechanisms, and enhance transparency and accountability in surveillance practices. By adapting relevant principles from the European Union while respecting Indonesia's constitutional framework and socio-legal context, Indonesia can develop a more effective, legitimate, and human rights-oriented system of digital surveillance governance capable of responding to the challenges of the rapidly evolving digital society.

REFERENCES

- Atmari, Atmari, and Sudjai Sudjai. "Digital Workplace Monitoring and Employees' Privacy Rights in Indonesia." *Jurnal Mahkamah : Kajian Ilmu Hukum Dan Hukum Islam* 11, no. 1 SE-Articles (June 9, 2026): 151–70. <https://doi.org/10.25217/jm.v11i1.7719>.
- Bindal, Pawan, and Ramveer Singh. "Survival of Right to Privacy under Administrative Surveillance: A Comparative Legal Study." *Journal of Humanities and Education Development* 8, no. 2 (2026): 29–40.
- Creswell, John, and J David Creswell. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage publications, 2017.
- Dewi, EN. "The Right to Be Forgotten and Digital Reputation: A Normative Analysis within Indonesian Cyber Law." *Lex Recta: Journal of Law and Normative Justice* 1, no. 1 SE-Articles (March 4, 2026): 31–39. <https://sovereignresearch.org/lex-recta/article/view/49>.
- Judijanto, Loso, Nuryati Solapari, and Irman Putra. "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia." *The Easta Journal Law and Human Rights* 3, no. 01 SE-Articles (October 31, 2024): 20–29. <https://doi.org/10.58812/eslhr.v3i01.351>.
- Kharisma, Dona Budi, and Alvalerie Diakanza. "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union." *International Journal of Human Rights in Healthcare* 17, no. 2 (May 16, 2024): 157–69. <https://doi.org/10.1108/IJHRH-04-2022-0035>.
- Lachmayer, Konrad, and Normann Witzleb. "The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective." *UNSWLJ* 37 (2014): 748.
- Maleno, Muhammad, and Andriana Kusumawati. "Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights." *Indonesia Law College Association Law*

- Journal* 3, no. 2 SE-Articles (December 9, 2024): 91–98. <https://ejournal.psthi.or.id/index.php/ILCALaw/article/view/21>.
- Mariya Mark, Stency, and Aaratrika Pandey. "Shielding Privacy in the Surveillance Era." *Law, State and Telecommunications Review* 16, no. 2 (October 16, 2024): 215–35. <https://doi.org/10.26512/lstr.v16i2.51916>.
- McIntyre, TJ. "Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective." In *Judges as Guardians of Constitutionalism and Human Rights*. Edward Elgar Publishing, 2016. <https://doi.org/10.4337/9781785365867.00014>.
- Naidu, Reva. "THE RIGHT TO PRIVACY AND MASS SURVEILLANCE: COMPARATIVE ANALYSIS POST-2020." *New York University Journal of International Law & Politics* 58, no. 1 (2025): 263.
- Natamiharja, Rudi, and Ikhsan Setiawan. "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France." *Jambe Law Journal* 7, no. 1 (July 30, 2024): 233–51. <https://doi.org/10.22437/home.v7i1.349>.
- Nur, Iffatin, Indri Hadisiswati, Hiba Fajarwati, Haniefah Nuruddienil Fithriy, and Muhammad Diyaulhaq Rais. "Wisdom in the Digital Era: Bridging Human Rights, Indonesian Cyber Law, and Progressive Fiqh." *The Journal of Society and Media* 10, no. 1 (April 30, 2026): 315–40. <https://doi.org/10.26740/jsm.v10n1.p315-340>.
- Palupy, Heppy Endah. "Privacy and Data Protection: Indonesia Legal Framework." *Journal Master Law and Technology Di Universiteit van Tilburg, Tilburg*, 2011.
- Paripurna, Amira, Sebastien Lafrance, and Masitoh Indriani. "Intelligence Surveillance, Counterterrorism, and the Right to Privacy in Indonesia and Canada." *JSEHR* 9 (2025): 304.
- Prabandari, Atin, Emma Seruni Ketaren, and Balya Arung Segara. "Rethinking Digital Migration Governance in Southeast Asia: Protecting or Restricting Human Rights?" *JSEHR* 9 (2025): 248.
- Rahayudin, Rahayudin, Muchammad Naseer, Nova Agustina, and Antonio Guterres. "Digital Sovereignty and The Right to Data: A Comparative Study Between Indonesia, The European Union, and The United States." *Journal of Law and Social Politics* 3, no. 2 SE-Articles (December 22, 2025): 84–96. <https://doi.org/10.59261/jlsp.v3i2.71>.
- Rubinstein, I. S., G. T. Nojeim, and R. D. Lee. "Systematic Government Access to Personal Data: A Comparative Analysis." *International Data Privacy Law* 4, no. 2 (May 1, 2014): 96–119. <https://doi.org/10.1093/idpl/ipu004>.
- Saleha, Dwi, Djuhrrijani Djuhrrijani, Reni Awaliyah, Wahyul Furqon, and Eko Sudarmanto. "Legal Analysis of Human Rights Protection within Smart City Policy Implementation in Indonesia." *The Easta Journal Law and Human Rights* 4, no. 01 (October 31, 2025): 63–73. <https://doi.org/10.58812/eslhr.v4i01.778>.
- Salman, M. "Digital Surveillance and the Right to Privacy under International Human Rights Law: A Comparative Study of State Practices." *Pinnacle in Social Sciences* 1, no. 01 SE-Articles (n.d.): 01–10. [https://ojs.pinnacleresearchcompany.com/index.php/PSS/article/view/1](https://ojs.pinnaceleresearchcompany.com/index.php/PSS/article/view/1).
- Sarjito, Aris, and Suyono Thamrin. "DIGITAL GOVERNANCE REFORM IN INDONESIA: A COMPARATIVE ANALYSIS WITH ESTONIA." *Вопросы Государственного и Муниципального Управления*, no. 5 (2026): 92–116.
- Satwiko, Brahmantyo Suryo. "Privacy and Data Protection: Indonesian Legal Framework." *Corporate and Trade Law Review* 1, no. 2 (2021): 106–8.
- Simbolon, Valentina Ancillia, and Vishnu Juwono. "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation." *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (December 30, 2022): 178.

<https://doi.org/10.31314/pjia.11.2.178-190.2022>.

- Syafik, A. "Digital Surveillance and the Right to Privacy: Legal Challenges of State Authority in the Era of Big Data Governance." *International Journal of Law and Political Authority* 1, no. 2 SE-Articles (April 7, 2026): 10–26. <https://researchfrontiers.id/corpus/article/view/123>.
- Tahir, Ridwan, and Titie Yustisia Lestari. "Children's Digital Rights: An In-Depth Analysis of Indonesia, Europe, and the US." *Eduvest - Journal of Universal Studies* 5, no. 2 (February 20, 2025): 1942–64. <https://doi.org/10.59188/eduvest.v5i2.50770>.
- Tan, Yosua Nicholas, Abdurrahman Alhakim, and Nurlaily Nurlaily. "Human Rights Protection in the Digital Sphere: The Problematics of Legal Certainty and Its Relevance to the SDGs." *SIGn Jurnal Hukum* 8, no. 1 (April 6, 2026): 18–31. <https://doi.org/10.37276/sjh.v8i1.652>.
- Tarafder, Agnidipto. "Surveillance, Privacy and Technology: A Comparative Critique of the Laws of USA And India." *Journal of the Indian Law Institute*, 2015, 550–78.
- Taufiq, Muchamad, Mochamad Reza Kurniawan, and Ananda Salsabila Kenyo. "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR." *International Journal of Business, Law, and Education* 6, no. 2 (July 30, 2025): 1260–68. <https://doi.org/10.56442/ijble.v6i2.1178>.
- Widodo, Junaidi Eko, Atma Suganda, and Tubagus Achmad Darodjat. "DATA PRIVACY AND CONSTITUTIONAL RIGHTS IN INDONESIA." *PENA LAW: International Journal of Law* 2, no. 2 (September 30, 2024). <https://doi.org/10.56107/penalaw.v2i2.187>.
- Zahra, Arifa. "Algorithmic Surveillance and the Erosion of Privacy: Reconciling National Security and Human Rights in the Digital Era - A Comparative Study of the USA and UAE." In *2025 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 633–38. IEEE, 2025. <https://doi.org/10.1109/ICCIKE67021.2025.11318249>.