PENA LAW
International Journal of Law
In collaboration with: International College Rajaman Gala University of Technology Krungthep (ICUTK), Thailand

Balancing Privacy and Digital Security: A Transnational Approach to International Data Protection Law

Riko Nugraha[1], Yuhelson[2], Tubagus Achmad Doradjat[3]
Doctor of Law Studies Program, Postgraduate Program - Jayabaya University, Indonesia[1,2]
Rajamangala University Of Technology Krungthep, Thailand[3]
***Email Correspondence:** rijko.nugraha@yahoo.com, yuhelson2870@gmail.com, Tubagus.d@mail.rmutk.ac.th

Abstract
Write a brief summary of your research, including objectives, methods, results, and conclusions. Limit to 250 words.

Keywords: *List 3-5 keywords that are relevant to your research. Examples: tourism, culture, arts.*

Abstract
The growing tension between privacy rights and national security interests in the digital age points to a normative crisis in global data governance. While the European Union has adopted a rights-based approach such as the General Data Protection Regulation, many other jurisdictions have instead adopted sectoral or security-based models that widen international legal fragmentation. This article analyzes how transnational legal instruments—particularly Convention 108+, the APEC CBPR system, and OECD guidelines—can serve as a normative bridge in reconciling these differing regimes. Using a comparative-normative legal research method, this study proposes the concept of "digital precautionary principles" as a new paradigm for balancing individual privacy with legitimate security needs. The research highlights the limitations of soft law in ensuring cross-border accountability and emphasizes the importance of a principle-based harmonization approach. Conceptually, this article expands the normative framework in transnational data protection law and practically provides policy guidance for developing countries in building fair and adaptive legal infrastructure for data protection. In the midst of increasingly intensive global interconnectedness, privacy protection that does not sacrifice collective security can only be achieved through anticipatory, interoperable, and rights-based global norms.

Keywords: Transnational Data Governance; Privacy and Security; Digital Prudential Principles; Global Legal Interoperability; Data Protection

INTRODUCTION

In recent decades, the development of digital technology has created a major transformation in the way data is collected, processed, and disseminated (Harnowo, 2022; Li et al., 2019; Lucas et al., 2013; Werner et al., 2023). According to a UNCTAD report (2022), more than 64% of the world's population is now connected to the internet, and global data volume is estimated to increase tenfold between 2020 and 2030. Alongside this, the risks of privacy breaches and misuse of personal data have also increased exponentially. Scandals such as Cambridge Analytica and the revelation of the PRISM surveillance program by Edward Snowden have shown how individual data can be manipulated for political and security purposes, raising widespread concerns in the global

community about the boundaries between privacy protection and the legitimacy of state surveillance (I. Clark, 2016; Di Salvo, 2019; Kunelius & Russell, 2019; Markussen, 2022).

These concerns are deepened when considering the imbalance between states' efforts to protect national security and citizens' interests in maintaining their privacy. In many jurisdictions, data privacy is not yet fully recognized as a non-derogable human right, leaving it vulnerable to compromise in the name of greater interests (Buchan & Lubin, 2023; Gill, 2009). This situation underscores the urgency of examining how international law responds to the need for privacy protection amid growing global digital threats. Without an adequate and cross-border legal framework, privacy rights risk being degraded to mere policy preferences rather than legally binding obligations.

The urgency of this research also lies in the inconsistency of data protection regulatory approaches between countries. The European Union, through the General Data Protection Regulation (GDPR), has become a pioneer in setting high standards for privacy protection (Bennett, 2018; Hoofnagle et al., 2019), while the United States relies on a more lenient sectoral approach (Boyne, 2018; Stratford & Stratford, 1999). In Asia, countries like Indonesia are still in the early stages of developing data protection policies, facing significant challenges in implementation and enforcement (Judijanto et al., 2024; Ramadhan & Wijaya, 2022). This lack of harmonization creates barriers to cross-jurisdictional cooperation and fosters legal gray areas that are exploited by both state and non-state actors.

Although literature on international data protection has grown, there is a gap in the legal discourse on how transnational approaches can normatively and institutionally mediate conflicts between privacy and digital security interests. Existing research tends to be limited to descriptive studies of individual national or regional legal regimes and has not comprehensively examined how transnational frameworks can provide common principles, coordination mechanisms, and models of cross-border accountability in data protection.

Based on this background, this article aims to analyze and evaluate transnational approaches in international data protection law, emphasizing the importance of balancing privacy protection and the need for digital security. The academic contribution offered is the formulation of the concept of "digital precautionary principle" as a new approach that integrates human rights protection values and security interests into a single inclusive and sustainable legal framework.

RESEARCH OBJECTIVES

In the context of an evolving digital ecosystem and growing tensions between individual privacy rights and national security interests, this research is situated at the intersection of data protection law, transnational legal governance, and cybersecurity policy. The primary focus of this study is to examine how transnational approaches—both through binding international instruments and soft law frameworks—can effectively bridge the normative conflict between privacy rights protection and the fulfillment of legitimate national security interests.

Given the fragmented nature of data protection regimes across jurisdictions, this study aims to identify common legal denominators that enable legal interoperability without compromising the

DOI: https://doi.org/10.56107/penalaw.v3i2.xxx

sovereignty of each country. Cross-border data flows—where data is collected in one country but processed, stored, or monetized in another—require legal solutions that transcend domestic boundaries. Therefore, this study seeks to evaluate the potential of transnational legal mechanisms such as Convention 108+, OECD Privacy Guidelines, and APEC Cross-Border Privacy Rules (CBPR) as normative bridges capable of connecting different legal traditions.

In addition, this study aims to clarify how digital governance can adopt a human rights-based orientation that remains adaptive to security imperatives, without sacrificing fundamental principles such as data minimization, valid consent, transparency, and accountability. Through comparative legal analysis and case studies, this research also seeks to identify the implementation challenges of transnational standards, particularly in jurisdictions that are still in the early stages of developing data protection policies or that place a high priority on national security agendas.

Ultimately, this study aims to formulate a conceptual framework in the form of "digital precautionary principles" as a guiding norm for future transnational data governance. These principles are intended to ensure that digital security policies do not disproportionately erode individual rights, and that privacy-by-design approaches and data sovereignty are integral parts of the global cyber law discourse. As such, this research provides normative and practical contributions to strengthening a more harmonious, fair, and balanced international data protection regime.

RESEARCH METHODOLOGY

This study uses a normative legal approach (doctrinal legal research) with qualitative analysis methods to examine legal norms related to data protection in a transnational context (Negara, 2023; Smits, 2015). The primary focus is on the reading and interpretation of international, regional, and national legal instruments governing the protection of personal data and digital security. This approach was chosen because it allows for an in-depth exploration of the principles, norms, and normative structures that form the foundation of global data protection law.

The type of data used is secondary data, which consists of primary and secondary legal materials. Primary legal materials include international regulations such as the General Data Protection Regulation (GDPR), Convention 108+ of the Council of Europe, OECD Privacy Guidelines, APEC CBPR Framework, as well as domestic regulations such as the Personal Data Protection Act (UU PDP) in Indonesia and the California Consumer Privacy Act (CCPA). Additionally, relevant court rulings are analyzed, such as the Schrems I and II cases at the Court of Justice of the European Union (CJEU), as well as policy documents and bilateral agreements that have implications for cross-border data flows.

Secondary legal materials include academic journals, legal textbooks, reports from international organizations (such as UNCTAD, OECD, and Human Rights Watch), and policy documents from data protection authorities. To ensure the accuracy and depth of the analysis, all legal materials were reviewed using content analysis techniques, with an emphasis on identifying legal principles, governance structures, and provisions that could potentially create conflicts or harmonization in digital privacy and security regulations.

This study also applies a comparative method to analyze the differences and similarities between data protection regimes in various jurisdictions, particularly between the rights-based model applied by the European Union and the market-based/sector-specific model that is more common in

the United States. Through this approach, the researchers aim to map the potential for normative convergence through transnational legal instruments and identify normative gaps that need to be addressed through reform or strengthened international cooperation.

To ensure replicability and scientific accountability, all legal documents were analyzed using a thematic matrix that categorizes key elements based on jurisdiction, underlying legal principles, relevant legal instruments, and their impact on the balance between privacy protection and digital security. As a result, the method used not only enables a systematic understanding of the existing legal structure but also opens up space for the development of new adaptive normative frameworks that can respond to global dynamics.

RESULTS

Fragmentation of Data Protection Legal Regimes and Normative Tensions

This study reveals significant structural and philosophical fragmentation in global data protection regimes as its main finding. More fundamentally, this fragmentation is not merely a technical difference, but reflects deep normative tensions regarding the fundamental nature of personal data and the balance of social values to be protected. The European Union, through the General Data Protection Regulation (GDPR), explicitly embraces a rights-based approach (de Gregorio & Dunn, 2022; Seun Solomon Bakare et al., 2024).

In this paradigm, personal data protection is understood as a derivative of fundamental human rights, particularly the right to privacy (Khadzhiradieva et al., 2024; Kovalenko, 2022; Malgieri & Custers, 2018). This approach is embodied through strict principles such as explicit and meaningful consent requirements, data minimization, accountability, and purpose limitation, all of which are designed to give individuals substantive control over their data.

In contrast, the United States has adopted a sectoral data protection model that is philosophically more market-oriented (Laurer & Seidl, 2021; Mazur & Słok-Wódkowska, 2022). This model prioritizes economic interests, encourages technological innovation, and relies on industry self-regulation mechanisms reinforced by ex-post legal remedies. Instead of a single comprehensive law, the US has a mosaic of regulations such as the Health Insurance Portability and Accountability Act (HIPAA) for health data, the Children's Online Privacy Protection Act (COPPA) for children's data, and the California Consumer Privacy Act (CCPA/CPRA) for consumer rights, each with different scopes and strengths (M. Clark, 2024; ElBaih, 2023). These fundamental philosophical differences—between data as an inherent right of individuals versus data as an economic commodity—form the basis of the observed fragmentation of regimes.

This inherent normative tension is not merely theoretical, but manifests itself in real legal and operational challenges in cross-jurisdictional practice. The Schrems II ruling by the Court of Justice of the European Union (CJEU) is a paradigmatic example of the practical consequences of this tension. The ruling effectively invalidated the EU-US data transfer framework, Privacy Shield, because the CJEU found that the US government's mass surveillance program did not meet the "necessity, appropriateness, and proportionality" standards required by EU law (Albi, 2022; Brkan, 2019; Tzanou, 2021).

Critically, the ruling highlights how substantial disparities in protection standards—particularly regarding government access to data—directly cause deep legal uncertainty

for business entities and impede the flow of data that is essential to the digital economy. This landmark decision underscores that fundamental differences in legal philosophy, particularly regarding the balance between national security and individual rights, have concrete and far-reaching legal consequences.

These findings of fragmentation and normative tension underscore a broader conclusion: without convergence toward a shared normative foundation or robust reconciliation mechanisms, legal interoperability and global data security architecture are fundamentally fragile. When one legal regime legitimizes practices that are fundamentally at odds with the core principles of another regime—such as the broad use of national security to justify mass surveillance that disregards the principles of proportionality and effective protection—the foundation for international cooperation is eroded.

The consequences are multi-level: First, individual rights, particularly the right to privacy and data protection, are threatened with reduction outside their jurisdiction of origin. Second, public trust in government agencies and digital platforms that facilitate cross-border data transfers declines dramatically. Third, compliance costs for businesses operating globally are skyrocketing due to the need to meet conflicting standards, potentially hindering innovation. Therefore, the observed fragmentation is not merely a legal challenge; it is a structural barrier to the development of a safe, trustworthy, and human rights-respecting global digital ecosystem. Achieving meaningful interoperability requires more than technical solutions; it demands philosophical reconciliation or at least mutual recognition of existing normative tensions and a commitment to manage them constructively.

Limitations and Potential of Transnational Approaches

This study acknowledges the catalytic potential of transnational instruments in bridging the fragmentation of global data protection regimes. Specifically, the Council of Europe's Convention 108+ and the APEC Cross-Border Privacy Rules (CBPR) represent visionary efforts to create normative interoperability (Kalin, 2024; Sullivan, 2019). Convention 108+, although rooted in European legal tradition, has evolved into an open treaty framework with universal principles such as lawfulness, purpose specification, and individual participation. Its inclusive character—demonstrated by the accession of countries such as Argentina, Mauritius, and Senegal—shows its capacity to function as a common floor for data protection across legal civilizations. In parallel, the APEC CBPR offers market-based technical mechanisms through a system of company certification and tiered accountability agents, facilitating data flows in the dynamic Asia-Pacific economic region. Conceptually, the two frameworks represent complementary approaches: Convention 108+ emphasizes the harmonization of substantive principles, while the CBPR focuses on procedural interoperability.

However, critical analysis reveals structural weaknesses that limit the effectiveness of these instruments as solutions for global governance. The fundamental problem lies in their soft law nature, which lacks binding and internationally standardized enforcement mechanisms. Without coercive supranational sanctions or an independent supervisory body with cross-jurisdictional authority, implementation critically depends on two fragile factors: (1) the political will of member states to allocate institutional resources, and (2) the technical and administrative capacity of local authorities. This dual dependency creates systemic vulnerabilities: In developing countries such as Indonesia,

budget constraints, technical expertise deficits (such as certified Data Protection Officers), and inter-agency fragmentation hinder the meaningful internalization of principles. As a result, transnational frameworks risk becoming empty signifiers—formally adopted but failing to ensure real protection at the operational level.

More problematically, this study found widespread regulatory decoupling in the practices of participating countries. Many jurisdictions—including some that have ratified Convention 108+ or participate in CBPR—pursue ambivalent normative strategies: On the one hand, they establish progressive legal frameworks (comprehensive data protection laws) to meet market access or economic cooperation requirements (digital trade agreements). On the other hand, operational practices often diametrically contradict these formal commitments—for example, through bulk surveillance policies without judicial warrants, restrictions on the independence of supervisory authorities, or weak enforcement of corporate violations.

This structural misalignment reflects what could theoretically be called compliance theater: performative efforts to meet international standards without substantive transformation in regulatory culture or rights protection. Concrete examples include states that have ratified Convention 108+ but allow overly broad national security exemptions, or CBPR participants that do not adequately investigate cross-border complaints.

The implications of these findings are both paradoxical and urgent: although transnational instruments provide a technical blueprint for interoperability, their ontological effectiveness depends on the convergence of political commitment and institutional capacity, which are currently unevenly distributed globally. Without institutional breakthroughs in three critical areas—(1) the development of actionable compliance mechanisms, (2) allocation of technical resources to developing countries (capacity-building transfers), and (3) independent monitoring of government surveillance practices (surveillance oversight)—the transnational framework risks becoming a cosmetic legitimization tool for regimes that engage in contradictory data governance. Therefore, the future of global data governance requires not only more sophisticated technical design but, more importantly, a reconfiguration of the underlying political economy of knowledge and power that underpins its implementation.

DISCUSSION

The tension between privacy and security in today's digital age can no longer be addressed through a dichotomous approach that pits these two interests against each other. The complexity of the digital ecosystem and the escalation of cyber threats have necessitated a paradigm shift toward a more integrative and prescriptive approach. In this context, the digital precautionary principle emerges as a normative framework capable of guiding the balance between the need for data protection and the demands of security. This principle asserts that any form of intervention by the state or corporations involving the processing of personal data must be subject to documented risk assessments and meet strict proportionality standards, especially if such actions have the potential to systematically and broadly infringe upon privacy rights.

Furthermore, this principle of digital prudence serves as an important link between a security-centric approach that focuses on system stability and a rights-based approach that emphasizes the protection of individual freedoms. This integrative approach requires the existence of operational tools such as Data Protection Impact Assessments (DPIAs) as a legal obligation prior to

DOI: https://doi.org/10.56107/penalaw.v3i2.xxx

the implementation of strategic digital policies or projects. In addition, transparency in state digital surveillance and accountability in the use of algorithms based on personal data are also important prerequisites for maintaining the legitimacy of technological interventions in the private sphere of citizens. When these instruments are consistently implemented, the state not only fulfills its protective function but also ensures that every digital action impacting individual rights is grounded in principles of caution and measured protection.

However, the effectiveness of digital prudence principles cannot be relied solely on technocratic regulations. On the contrary, the successful implementation of these principles depends heavily on collaborative partnerships involving the state, the technology sector, and civil society simultaneously and equally. Experience from various multistakeholder initiatives such as the Global Privacy Assembly shows that cross-sector collaboration can accelerate the adoption of cross-jurisdictional data protection standards and strengthen the global digital governance architecture. Such cooperation models also contribute to filling regulatory gaps in developing countries that do not yet have adequate legal frameworks to address privacy and security challenges simultaneously.

In the Indonesian context, progress has been made through the enactment of Law No. 27 of 2022 on Personal Data Protection (Hapriyanto, 2023; Mayasari, 2023; Rizal et al., 2024). However, this study notes that the regulation still faces serious structural obstacles at the implementation level. Some of the main issues include the absence of an independent data protection authority, limited technical capacity of digital law enforcement agencies, and insufficient integration between data protection policies and national cybersecurity strategies. As a result, the privacy protection standards formally recognized in national law have not yet been able to provide tangible guarantees for citizens' privacy.

This situation shows that the transnationalization of data protection norms cannot be achieved through legal formalization alone (Fahey, 2018; Tzanou, 2018). A more comprehensive and adaptive institutional ecosystem needs to be developed. This ecosystem includes raising public awareness of privacy rights, strengthening the capacity and independence of supervisory bodies, and establishing regional cooperation mechanisms based on the principles of digital justice. As such, strengthening data governance is not only the responsibility of the government or the private sector, but also a collective agenda that requires the involvement of various stakeholders.

Ultimately, balancing privacy and security in the digital age is not about choosing one and sacrificing the other. Rather, both can be designed to support each other through measured, inclusive, and accountability-based principles of digital prudence. In this regard, developing countries like Indonesia need to go beyond mere normative adoption and move toward institutional reforms that prioritize the protection of human rights in the digital space. Only then can digital transformation truly be grounded in justice, participation, and sustainable legal certainty.

Scientific Novelty and Research Contribution

This study makes an important contribution to the international legal discourse on data protection by offering a new approach that integrates normative, conceptual, and practical dimensions within a transnational framework. In a landscape marked by sharp differences between legal systems and data protection models across countries, this article aims to address the academic gap regarding the need for a common framework capable of balancing privacy and digital security interests in a sustainable manner.

DOI: https://doi.org/10.56107/penalaw.v3i2.xxx

The scientific novelty offered in this research lies primarily in the formulation of the digital precautionary principle as a new paradigm for regulating cross-border data governance. This principle was developed in response to the increasing systemic risks to individual privacy rights posed by the collection, processing, and exchange of data on a global scale—especially when done without adequate accountability and transparency. Unlike the conventional precautionary principle widely used in environmental law, the digital precautionary principle emphasizes the obligation to prevent and test risks in a pre-emptive manner against actions by states or corporations that have the potential to harm civil liberties through digital instruments.

Normatively, this study contributes to the development of a transnational approach to data protection law. This approach does not impose uniformity, but emphasizes the interoperability of norms through the convergence of basic principles such as legal legitimacy, proportionality, transparency, and accountability. In this context, mechanisms such as Convention 108+, OECD Privacy Guidelines, and APEC CBPR are not merely viewed as technical tools but also as meeting points enabling legal dialogue among nations. By comprehensively addressing this approach, this research fills a theoretical gap in international law studies, which have traditionally been fragmented between public and private approaches or between regional and global frameworks.

The practical contribution of this research is also significant, particularly for developing countries that are designing or strengthening their data protection legal frameworks. The findings and analysis in this article can serve as guidelines for designing policies that are not only oriented toward formal compliance with global standards, but also build the institutional capacity necessary to substantively enforce digital rights. The emphasis on the need to strengthen the role of independent data supervisory authorities, integrate the principle of privacy-by-design, and establish inclusive regional cooperation forums are part of the practical recommendations offered.

Thus, this study not only contributes to the development of legal science in the domain of data protection and digital rights, but also offers a conceptual and normative roadmap to promote data governance that is more equitable, transparent, and adaptive to global challenges. The novelty offered is not purely theoretical but also practical, making it relevant for academics, policymakers, and the international community seeking a more balanced and equitable cross-border data governance model.

CONCLUSION

This study confirms that the main challenge in personal data protection in the digital age lies not only in the diversity of regulations between countries, but also in the structural imbalance between individual privacy rights and national security interests. The fragmentation of legal regimes reflecting philosophical differences between rights-based and security-driven approaches has created normative tensions that hinder the emergence of a fair and sustainable global data protection system.

Through an in-depth analysis of international and regional legal instruments such as the GDPR, Convention 108+, and APEC CBPR, this study finds that transnational approaches have great potential to build normative bridges between jurisdictions. However, the effectiveness of these approaches is highly dependent on political commitment, institutional capacity, and cross-border accountability mechanisms that are not yet fully developed. In this context, the principle of digital precaution proposed in this study could serve as a new conceptual framework to ensure that digital security policies do not arbitrarily sacrifice individual privacy rights.

As a scientific contribution, this article proposes an integrative approach that emphasizes legal interoperability, the participation of non-state actors, and the strengthening of fundamental data protection principles as the foundation for building a more equitable and responsible transnational data governance system. This contribution is significant not only at the conceptual level but also in providing practical policy direction for developing countries in designing adaptive and equitable legal frameworks for data governance.

Enforcing privacy rights in the global digital landscape requires an approach that is not only reactive, but also proactive and anticipatory. Therefore, the future of international data protection law lies in the ability of the global community to build a legal system capable of maintaining a balance between freedom and security within a single set of universal and equitable values.

REFERENCES

Albi, A. (2022). A Paradigm Shift in the Role of Courts? Disappearance of Judicial Review through Mutual Trust and other Neofunctionalist Tenets of EU Law. *Juridica International*, *31*. https://doi.org/10.12697/ji.2022.31.01

Bennett, C. J. (2018). The European General Data Protection Regulation: An instrument for the globalization of privacy standards? In *Information Polity* (Vol. 23, Issue 2). https://doi.org/10.3233/IP-180002

Boyne, S. M. (2018). Data Protection in the United States. *American Journal of Comparative Law*, *66*. https://doi.org/10.1093/ajcl/avy016

Brkan, M. (2019). The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU's constitutional reasoning. In *German Law Journal* (Vol. 20, Issue 6). https://doi.org/10.1017/glj.2019.66

Buchan, R., & Lubin, A. (2023). The Rights to Privacy and Data Protection in Times of Armed Conflict. *International Review of the Red Cross*, *105*(923). https://doi.org/10.1017/S1816383123000103

Clark, I. (2016). The digital divide in the post- Snowden era. *Journal of Radical Librarianship*, *2*(2016).

Clark, M. (2024). Consumer Privacy and the Dobbs Disruption. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4741909

de Gregorio, G., & Dunn, P. (2022). The European Risk-Based Approaches: Connecting Constitutional Dots Inthe Digital Age. *Common Market Law Review*, *59*(2). https://doi.org/10.54648/cola2022032

Di Salvo, P. (2019). From Snowden to Cambridge analytica: An overview of whistleblowing cases as scandals. In *The Routledge Companion to Media and Scandal*.

ElBaih, M. (2023). The Role of Privacy Regulations in AI Development (A Discussion of the Ways in Which Privacy Regulations Can Shape the Development of AI). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4589207

Fahey, E. (2018). Introduction: Institutionalisation Beyond the Nation State: New Paradigms? Transatlantic Relations: Data, Privacy and Trade Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3186123

Gill, P. (2009). Security intelligence and human rights: Illuminating the 'Heart of Darkness'? *Intelligence and National Security*, *24*(1). https://doi.org/10.1080/02684520902756929

Hapriyanto, A. R. (2023). The Urgency of Adopting Regulations on Artificial Intelligence Utilization to Enhance Personal Data Protection in Indonesia. *Asian Journal of Engineering, Social and Health*, *2*(12). https://doi.org/10.46799/ajesh.v2i12.179

Harnowo, T. (2022). Law as Technological Control of the Infringement of Intellectual Property Rights in the Digital Era. *Corporate and Trade Law Review*, *2*(1). https://doi.org/10.21632/ctlr.2.1.65-79

Hoofnagle, C. J., Sloot, B. van der, & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information and Communications Technology Law*, *28*(1). https://doi.org/10.1080/13600834.2019.1573501

Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. *The Easta Journal Law and Human Rights*, *3*(01), 20–29. https://doi.org/10.58812/eslhr.v3i01.351

Kalin, R. P. (2024). *Towards Reconciling Digital Trade and Data Privacy* (pp. 287–316). https://doi.org/10.1007/978-3-031-73857-9_6

Khadzhiradieva, S., Bezverkhniuk, B., Nazarenko, O., Bazyka, S., & Dotsenko, T. (2024). Personal data protection: Between human rights protection and national security. *Social Legal Studios*, *7*(3), 245–256. https://doi.org/10.32518/sals3.2024.245

Kovalenko, Y. (2022). The Right To Privacy And Protection Of Personal Data: Emerging Trends And Implications For Development In Jurisprudence Of European Court Of Human Rights. *Masaryk University Journal of Law and Technology*, *16*(1). https://doi.org/10.5817/MUJLT2022-1-2

Kunelius, R., & Russell, A. (2019). Surveillance scandals and the systemic crisis of the public. In *The Routledge Companion to Media and Scandal*. https://doi.org/10.4324/9781351173001-30

Laurer, M., & Seidl, T. (2021). Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation. *Policy and Internet*, *13*(2). https://doi.org/10.1002/poi3.246

Li, D., Landström, A., Fast-Berglund, Å., & Almström, P. (2019). Human-centred dissemination of data, information and knowledge in industry 4.0. *Procedia CIRP*, *84*. https://doi.org/10.1016/j.procir.2019.04.261

Lucas, H. C., Agarwal, R., Clemons, E. K., El Sawy, O. A., & Weber, B. (2013). Impactful research on transformational information technology: An opportunity to inform new audiences. In *MIS Quarterly: Management Information Systems* (Vol. 37, Issue 2). https://doi.org/10.25300/misq/2013/37.2.03

Malgieri, G., & Custers, B. (2018). Pricing privacy – the right to know the value of your personal data. *Computer Law and Security Review*, *34*(2). https://doi.org/10.1016/j.clsr.2017.08.006

Markussen, H. (2022). After Cambridge Analytica: Rethinking Surveillance in the Age of (Com)Modification. In *Problematising Intelligence Studies: Towards a New Research Agenda*. https://doi.org/10.4324/9781003205463-13

Mayasari, H. (2023). A examination on personal data protection in metaverse technology in Indonesia: a human rights perspective. *Journal of Law, Environmental and Justice*, *1*(1). https://doi.org/10.62264/jlej.v1i1.4

Mazur, J., & Słok-Wódkowska, M. (2022). Access to Information and Data in International Law How to Find a Path Forward from Human Rights-Oriented and Market-Oriented Approach? *Nordic Journal of International Law*, *91*(2). https://doi.org/10.1163/15718107-91020004

Negara, T. A. S. (2023). Normative Legal Research in Indonesia: Its Originis and Approaches. *Audito Comparative Law Journal (ACLJ)*, *4*(1). https://doi.org/10.22219/aclj.v4i1.24855

Ramadhan, K. R., & Wijaya, C. (2022). The Challenges of Personal Data Protection Policy in Indonesia: Lesson learned from the European Union, Singapore, and Malaysia. *Technium Social Sciences Journal*, *36*. https://doi.org/10.47577/tssj.v36i1.7442

Rizal, M., Rosadi, S. D., & Taryana, A. (2024). Legal Framework for consumer Data Protection For Digital Business SMES in Indonesia. *Journal of Law and Sustainable Development*, *12*(1). https://doi.org/10.55908/sdgs.v12i1.2809

Seun Solomon Bakare, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, & Nkechi Emmanuella Eneh. (2024). Data Privacy Laws And Compliance: A Comparative Review Of The EU GDPR and USA Regulations. *Computer Science & IT Research Journal*, *5*(3). https://doi.org/10.51594/csitrj.v5i3.859

Smits, J. M. (2015). What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2644088

Stratford, J. S., & Stratford, J. (1999). Data Protection and Privacy in the United States and Europe. *IASSIST Quarterly*, *22*(3). https://doi.org/10.29173/iq80

Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. *Computer Law and Security Review*, *35*(4). https://doi.org/10.1016/j.clsr.2019.05.004

Tzanou, M. (2018). The EU–US Data Privacy and Counterterrorism Agreements: What Lessons for Transatlantic Institutionalisation? In *Studies in European Economic Law and Regulation* (Vol. 10). https://doi.org/10.1007/978-3-319-50221-2_4

Tzanou, M. (2021). Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights. In *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*. https://doi.org/10.5040/9781509940691.ch-007

Werner, L., Puta, C., Chilalika, T., Walker Hyde, S., Cooper, H., Goertz, H., Rivera Hildebrand, M., Bernadotte, C., & Kapnick, V. (2023). How digital transformation can accelerate data use in health systems. *Frontiers in Public Health*, *11*. https://doi.org/10.3389/fpubh.2023.1106548