International Journal of Educational Review, Law, and Social Sciences (IJERLAS)
ISSN: 2808-487X
Edition: Vol. 6 No.2 (2026)
https://radjapublika.com/index.php/IJERLAS/index

Right to Be Forgotten in Indonesia and Thailand: Human Rights-Based Legal Reform Inspired by Korea, the U.S., and the European Union

Ampuan Situmeang[1]*, Lu Sudirman[2], Ida Bagus Rahmadi Supancana[3], Nurlaily[4], Hari Sutra Disemadi[5]
[1,2,4,5]Universitas Internasional Batam, Indonesia
[3]Universitas Katolik Indonesia Atma Jaya, Indonesia
***Corresponding Author:** ampuan.situmeang@uib.ac.id

Keywords:
Human Rights; Data Protection; Digital Privacy; Right to Be Forgotten; Technology Law.

Article Info.
Received:
10/02/2026
Revised:
28/02/2026
Accepted:
24/03/2026
Published:
31/03/2026

ABSTRACT

The central legal problem of this study lies in the normative inadequacy and weak enforcement construction of the right to be forgotten within the personal data protection regimes of Indonesia and Thailand amid escalating data breaches in Southeast Asia. This research aims to analyze and compare the normative framework governing the right to be forgotten in Indonesia and Thailand with selected global benchmarks, namely the European Union, South Korea, and the United States, in order to formulate ideal legal constructs adaptable to Southeast Asian contexts. This study employs a normative legal research method supported by a comparative legal approach, examining statutory regulations and secondary legal materials from Indonesia, Thailand, the EU (GDPR), South Korea (PIPA), and the United States (CCPA). The findings reveal that although Indonesia's Personal Data Protection Law and Thailand's Personal Data Protection Act formally recognize deletion rights, both frameworks remain incomplete due to limited procedural clarity, weak dispute resolution mechanisms, insufficient third-party deletion obligations, and ambiguous safeguards against re-identification risks. In contrast, the EU's GDPR mandates third-party takedown obligations and imposes severe financial sanctions, South Korea's PIPA provides strict deletion duties combined with criminal penalties, and the CCPA establishes structured compliance and notification mechanisms. Consequently, strengthening enforcement pathways, clarifying procedural guarantees, and integrating stricter controller obligations are essential for Indonesia and Thailand to ensure effective realization of the right to be forgotten in rapidly expanding digital societies.

How to cite: Situmeang, A., Sudirman, L., Supancana, I. B. R., Nurlaily, N., & Disemadi, H. S. (2026). Right to Be Forgotten in Indonesia and Thailand: Human Rights-Based Legal Reform Inspired by Korea, the U.S., and the European Union. International Journal of Educational Review, Law And Social Sciences (IJERLAS), 6(2), 345–358. https://doi.org/10.5281/zenodo.20420285

Introduction

Throughout years of digital transformation, the Southeast Asia region has faced rising cases of personal data leaks and breaches, representing 9% of the global data breach from 2004 to 2024,[1] as the region continues to experience digital economy growth and increasing reliance on internet-based services.[2] In 2023, it was even reported that Southeast Asian businesses experienced more than 36,000 online attacks on average.[3] These figures reflected a concerning prevalence and further risks, with Indonesia and Thailand

[1] Shanitamol Sojan Gracy, 'A Global Analysis of Data Breaches from 2004 to 2024' (University of London, 2024), doi:10.48550/arXiv.2502.05205.

[2] Henike Primawanti, Agus Subagyo, and Windy Dermawan, 'ASEAN 4.0. Era: Development in Digital Economy and Trade Sector', *Dinamika Global: Jurnal Ilmu Hubungan Internasional*, 7.2 (2022), pp. 333–49, doi:https://doi.org/10.36859/jdg.v7i02.1279.

[3] Sasha Lee and Alberto Iskandar, 'Southeast Asia, Cyber Threats, and Opportunities for Canadian Co-Operation: The Cases of Singapore and the Philippines', *The Asia Pacific Foundation of Canada (APF Canada)*, 2024 <https://www.asiapacific.ca/publication/southeast-asia-cyber-threats-and-opportunities-canadian-co> [accessed 18 February 2025].

having some of the highest number of breaches. One of the biggest cases in Indonesia was the data breach involving 1.3 billion SIM card numbers that were collected illegally from the country's Ministry of Communication and Information's system in 2022.[4] Similarly, Thailand has also faced numerous data breach issues, prompting questions on the government's tough stance in the private sector and glaring lack of focus on data breaches in the public sector, after a data breach case involving 20 million data of senior citizens being leaked.[5]

Data leaks among ASEAN countries are not only affecting the privacy of individuals but also posing significant threat to national security.[6] This issue also lowers the trust of the general public regarding that digitalization of government-related services, along with the commitment of the private sector in protecting consumer's data. A report done by IBM in 2022 titled "Cost of a Data Breach" showed that the average financial damage of data leaks in ASEAN countries is about USD2.87 million per incident, which is higher in comparison to other regions in the world.[7] The lack of comprehensive and strong regulation, followed by consistent and effective legal enforcements have been some of the most persistent issues that countries like Indonesia and Thailand have had to face regarding this.

One of the most important aspects of data privacy, is the enforcement of the right to be forgotten.[8] This right focuses on specific right of every data owner to have their data deleted from a data system that exist and is actively affecting the operation of a digital platform.[9] At a glance, this right seems rather simple and one dimensional, as it is quite straightforward in its ultimate goal.[10] However, many data collection, data processing, and data retention practices have prevented this simple privacy right to be fully protected. Ideally, people can and should have to right to request the deletion of their data, for whatever purpose. Taking into account the impacts of personal data in the digital space and how they can have real life consequences,[11] the legal enforcement of this specific digital right becomes a key aspect of data protection and privacy that can significantly impact a person's life.[12] Most importantly, the right to be forgotten can serve as the preemptive move to prevent oneself from data breach victimization,[13] which is increasingly threatening digital technology users worldwide.[14] Be it personal or non-personal, every person who use digital technologies and have their data collected and/or processed should have to right to request for deletion.

---

[4] Leski Rizkinaswara, 'Dugaan Kebocoran Data SIM Card, Kominfo Lakukan Koordinasi Dengan Ekosistem Pengendali Data', *Direktorat Jenderal Aplikasi Informatika KOMINFO*, 2022 <https://aptika.kominfo.go.id/2022/09/dugaan-kebocoran-data-sim-card-kominfo-lakukan-koordinasi-dengan-ekosistem-pengendali-data/> [accessed 18 February 2025].

[5] Surachanee Sriyai, 'Data Leaks: Thai Government Tough on Private Firms, Soft on Public Sector and Cybercriminals', *Fulcrum*, 2024 <https://fulcrum.sg/data-leaks-thai-government-tough-on-private-firms-soft-on-public-sector-and-cybercriminals/> [accessed 18 February 2025].

[6] Denny Indra Sukmawan and David Putra Setyawan, 'Hacker, Fear, and Harm: Data Breaches and National Security', *Jurnal Global & Strategis*, 17.1 (2023), pp. 153–82, doi:10.20473/jgs.17.1.2023.153-182.

[7] Ponemon Institute and IBM Security, *Cost of a Data Breach 2022*, *IBM Corportation and Ponemon Institute Research* (2022) <https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High>.

[8] Uta Kohl, 'The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy', *International and Comparative Law Quarterly*, 72.3 (2023), pp. 737–69, doi:DOI: 10.1017/S0020589323000258.

[9] Mika Nakashima, 'The Legal Frameworks of the Right to Request the Deletion of Personal Data in the EU, the U.S. and Japan and the Right to Be Forgotten: A Study Focusing on Search Businesses', in *IFIP Advances in Information and Communication Technology*, 2020, DXC, 29–40, doi:10.1007/978-3-030-62803-1_3.

[10] Not only the right to be forgotten itself, the discourse regarding it is also often quoted as one-dimensional, as it is can be difficult to strike the balance between regulating companies behind digital platforms and ensuring that they continue to bring benefits to many people through their services. *See* George Brock, *The Right to Be Forgotten: Privacy and the Media in the Digital Age*, 1st edn (I.B.Tauris & co. Ltd, 2016), p. 42. Furthermore, the review of this referenced book also highlights how this can be somewhat contrary to data protection law, which does have a basis for retention when the data that is requested to be deleted is true, in the name of public interest. *See also* Vincent Lawrance, 'Book Review: The Right to Be Forgotten: Privacy and Media in the Digital Age', *Media International Australia*, 167.1 (2018), pp. 182–83, doi:10.1177/1329878X18756108. However, it is important to note that this definition of public interest can be too broad and may be highly contested.

[11] Timo Jakobi and others, 'A Taxonomy of User-Perceived Privacy Risks to Foster Accountability of Data-Based Services', *Journal of Responsible Technology*, 10 (2022), pp. 1–14, doi:https://doi.org/10.1016/j.jrt.2022.100029.

[12] Carolina Pereira and others, 'Security and Privacy in Physical–Digital Environments: Trends and Opportunities', *Future Internet*, 17.2 (2025), pp. 1–23, doi:10.3390/fi17020083.

[13] Kopo Marvin Ramokapane and Awais Rashid, 'ExD: Explainable Deletion', in *New Security Paradigms Workshop* (ACM, 2023), pp. 34–47, doi:10.1145/3633500.3633503.

[14] Qian Wang and others, 'Information Technology Innovativeness and Data-Breach Risk: A Longitudinal Study', *Journal of Management Information Systems*, 40.4 (2023), pp. 1139–70, doi:10.1080/07421222.2023.2267319.

Furthermore, there are many data collection, data processing, and data retention practices that can nevertheless threaten the right to be forgotten,[15] which makes it even more important and urgent to address this issue. In the face of increasingly invasive data tracking technologies and the dangers of cybersecurity risks, the urgency to reassess and ensure the enforcement of the right to be forgotten naturally becomes even more pronounced. This is particularly important in the context of legal compliance, which is a key wall of protection to ensure that this particular right remains safeguarded and is well respected by those who collect and process data. The European Union is often regarded one of the leaders in this discourse, as its General Data Protection Regulation (GDPR) is widely regarded as the gold standard for data protection and privacy.[16] The United States, on the other hand, is widely regarded as the center of innovation in a fiercely competitive global tech market,[17] making its regulations regarding this discourse particularly important. Lastly, assessing South Korea's stance regarding this issue is also important as it's considered one of the leaders of the Asia's growing digital technology research and development,[18] combined with continuous public support for its continuation.[19] Assessing these key players and how they protect the right to be forgotten is important in the much-needed continuous development of Indonesian and Thai framework to sustain their immense digital growth.

Unfortunately, the development of legal framework for data protection and privacy in Indonesia and Thailand have been rather late and incomplete. Indonesia's Law No. 27 of 2022 on Personal Data Protection Law (PDP Law) remains the key framework for Indonesia, despite lacking technicalities and acknowledgement of advanced digital aspects that are relevant for data protection and privacy, particularly for the right to be forgotten.[20] Unfortunately, the country is still relying on the promise of future implementing regulations for the PDP Law.[21] Thailand, on the other hand, has their own equivalent through Personal Data Protection Act, which was signed in 2019 but took effect only years later in 2022.[22] The delay in the de facto enforcement of this law, despite its formal enactment years prior, underscores the lingering uncertainty regarding the effectiveness of the very regulation it sought to establish, particularly in the face of escalating threats to data privacy. From these realities alone, it is a fair perspective to question whether or not Indonesia and Thailand actually have adequate normative support for the enforcement of very specific rights like the right to be forgotten, which is increasingly ridden with complexities as data-reliant technologies continue to be developed.[23]

There have been many academic discourses regarding data protection and privacy all around the world. One study conducted by Santana and Ansari analyzes how data protection cannot be separated from the human rights perspective, particularly the right to privacy.[24] Additionally, a study conducted by Utomo further supports this by highlighting the basis of this right, which is Article 12 of the Universal Declaration

[15] Sherry Li Xie, 'Retention in "the Right to Be Forgotten" Scenario: A Records Management Examination', *Records Management Journal*, 26.3 (2016), pp. 279–92, doi:10.1108/RMJ-11-2015-0038.

[16] Alessandro Mantelero, 'The Future of Data Protection: Gold Standard vs. Global Standard', *Computer Law & Security Review*, 40 (2021), pp. 1–5, doi:https://doi.org/10.1016/j.clsr.2020.105500.

[17] Rosalie L Tung, Ivo Zander, and Tony Fang, 'The Tech Cold War, the Multipolarization of the World Economy, and IB Research', *International Business Review*, 32.6 (2023), pp. 1–14, doi:https://doi.org/10.1016/j.ibusrev.2023.102195.

[18] Leigh Dayton, 'How South Korea Made Itself a Global Innovation Leader', *Nature*, 581.7809 (2020), pp. S54–56, doi:10.1038/d41586-020-01466-7.

[19] Yongrok Choi, Siyu Li, and Hyoungsuk Lee, 'Korean Paradox of Public Support for the Research and Development Investment in the Sustainable Performance of the Regional Economy', *Land*, 13.6 (2024), pp. 1–20, doi:10.3390/land13060759.

[20] Moody Rizqy Syailendra, Gunardi Lie, and Amad Sudiro, 'Personal Data Protection Law in Indonesia: Challenges and Opportunities', *Indonesia Law Review*, 14.2 (2024), pp. 56–72 <https://scholarhub.ui.ac.id/ilrev/vol14/iss2/4/>.

[21] Ni Made Dwi Gayatri Putri, Ni Luh Made Mahendrawati, and Ni Made Puspasutari Ujianti, 'Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022', *Jurnal Preferensi Hukum*, 5.2 (2024), pp. 240–45, doi:10.22225/jph.5.2.8087.240-245.

[22] Lu Sudirman, Hari Sutra Disemadi, and Arwa Meida Aninda, 'Comparative Analysis of Personal Data Protection Laws in Indonesia and Thailand: A Legal Framework Perspective', *Jurnal Etika Demokrasi*, 8.4 (2023), pp. 497–510 <https://journal.unismuh.ac.id/index.php/jed/article/view/12875>.

[23] This is a global trend called "datafication" where technologies are continuously developed, maintained, and improved through various kinds of data, that are constantly being generated, collected, and processed. *See* Katarzyna Cieslik and Dániel Margócsy, 'Datafication, Power and Control in Development: A Historical Perspective on the Perils and Longevity of Data', *Progress in Development Studies*, 22.4 (2022), pp. 352–73, doi:10.1177/14649934221076580.

[24] Paulo Campanha Santana and Faiz Ayat Ansari, 'Data Protection and Privacy as a Fundamental Right: A Comparative Study of Brazil and India', *Journal of Liberty and International Affairs*, 9.3 (2023), pp. 456–70, doi:10.47305/JLIA2393555cs.

of Human Rights (UDHR).[25] While these studies do not focus on the right to be forgotten per se, it does highlights how control over data significantly impacts privacy rights, and that this should be the most important aspect in data protection regulation. In line with these insights, another study carried out by Prabasari, Sudharma, and Angelo discusses how important the right to be forgotten is, as a part of the broader privacy rights in the digital sphere.[26] However, this specific right is also highlighted as often not supported with concrete enforcement mechanism.

The European Union's General Data Protection Regulation (GDPR) has been cited many times throughout the literatures as the benchmark of data protection and privacy, as highlighted by a bibliometric analysis done by Judijanto, Solapari, and Karauwan.[27] The study also highlights how GDPR's influence goes beyond the European Union, influencing many regulations regarding data protection and privacy around the world. Unfortunately, the bibliometric analysis does not mention anything regarding the right to be forgotten, which shows the lack of focus on the literatures regarding this aspect of data protection and privacy, as opposed to other aspects. On the comparative side, Bakare et al. highlight the stark contrast between the EU GDPR's unified, rights-based data privacy framework with strict enforcement and global applicability and the U.S.'s fragmented, sector-specific approach with varying enforcement mechanisms, underscoring the challenges businesses face in navigating compliance across jurisdictions while adapting to evolving global privacy standards.[28]

Aside from the lack of focus on the right to be forgotten in comparison to other aspects of data protection and privacy, there also seems to be a gap in benchmarking through comparative approach on how key players in the global tech market regulate and protect the right to be forgotten. This is exactly what this paper is trying to dive deep into, with an added value of novelty by comparing Indonesia and Thailand's legal framework with key players like the European Union, the United States, and South Korea. This study can potentially help legal development quests for both Indonesia and Thailand as the Southeast Asia region and the rest of the world continues to utilize digital technologies. Limitation of this study mainly comes from the differences of legal system of the countries in the comparative analysis. It is therefore crucial to outline that the purpose of this study is to outline the normative constructs that can be adopted in any way possible in Indonesia and Thailand. The adoptability of these the identified norms in the analysis will also depend on the legal politics of Indonesia and Thailand, which ultimately dictates the direction of legal developments. Enforcement mechanisms might also depend on the technical capability of each government, which this study will not discuss. Despite these limitations, the value of this study remains, particularly as a crucial reference in the rapidly developing discourse regarding the protection of privacy rights in the digital space.

Method

This study utilizes the normative legal research method, focusing the weight of the research analysis on the implications of legal norms that exist within the relevant legal frameworks.29 Typically, at least in the purest sense, involves the analysis of a particular legal issue, using the lens of legal implications reflected by the relevant legal norms that are collected from secondary data in the form of primary law sources.30 Additionally, this study is supported by comparative approach, to ensure proper analysis in between relevant legal systems, namely Indonesian, Thai, South Korean, American, and European. Comparative approach is an essential part of this study, as it helps navigate the different legal challenges and implications presented by the legal systems being compared extensively in analysis. Secondary data utilized in this study include Indonesia's Law No. 11 of 2008 on Electronic

[25] Setyo Utomo, 'Personal Data Protection Through Law Number 27 of 2022: Challenges of Cybercrime in the Era of Globalization and Digital', *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, 23.3 (2024), pp. 2967–75, doi:10.31941/pj.v23i3.5611.

[26] Ni Kadek Dhea Ardi Prabasari, Kadek Januarsa Adi Sudharma, and Michael Angelo, 'The Right to Be Forgotten: Regulation of Personal Data Deletion in Indonesia', *KRTHA BHAYANGKARA*, 18.3 (2024), pp. 541–58, doi:10.31599/krtha.v18i3.3291.

[27] Loso Judijanto, Nuryati Solapari, and Donny Eddy Sam Karauwan, 'A Bibliometric Analysis of Legal Approaches to Personal Data Protection', *The Easta Journal Law and Human Rights*, 2.3 (2024), pp. 165–75, doi:10.58812/eslhr.v2i03.285.

[28] Seun Solomon Bakare and others, 'Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations', *Computer Science & IT Research Journal*, 5.3 (2024), pp. 528–43, doi:10.51594/csitrj.v5i3.859.

[29] Hari Sutra Disemadi, 'Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies', *Journal of Judicial Review*, 24.2 (2022), pp. 289–304, doi:10.37253/jjr.v24i2.7280.

[30] David Tan, 'Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum', *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, 8.5 (2021), pp. 2463–78 <https://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601>.

Information and Transactions, Law No. 19 of 2016 on Amendments to the Electronic Information and Transactions Law, Law No. 1 of 2024 on the Second Amendment to the Electronic Information and Transactions Law, Law No. 27 of 2022 on Personal Data Protection, Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems, and Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions; Thailand's Computer-Related Crime Act B.E. 2550 and Personal Data Protection Act B.E. 2562; South Korea's Personal Information Protection Act; the European Union's General Data Protection Regulation; and the United States' California Consumer Privacy Act of 2018.

Results and Discussion

Conceptualization of the right to be forgotten and ideal normative construction

Digital transformation has fundamentally changed not just how people do many commercial and non-commercial activities,[31] but also how people see identities.[32] With the rise and mass adaptation of social media platforms, digital identity becomes a fundamental aspect of every modern human.[33] Even outside of social media platforms, there are other platforms that are utilized connect people for a multitude of reasons, be the personal ones, or strictly business-related purposes.[34] Thus, it is no longer a surprise that a lot of people care about what people see and think about them in the digital space, as much as how people do in real life. This is because many aspects of digital identities have real-world implications and can even have long term impacts over one's life, spanning across many aspects of life.

There have been many cases involving people getting fired over questionable activities on social media,[35] or people having trouble finding a job because of the lack of digital presence.[36] Professionally, platforms like LinkedIn or Indeed have become some of the most important strategic digital networking platforms that a lot of professionals can utilize to support their career ambitions.[37] From the entertainment and communication perspective, social media have become a key aspect of daily life, connecting billions of people from all over the world and building real connections. Therefore, it is truly dismissive not to see the digital world and imprints that people have in it as important aspects of life that can significantly impact their real life.

Even more jarring is the rising threats of data breaches and other cybersecurity risks. This particular issue is a significant threat to the well-being of many digital technology users, whose data are collected and processed every day as they continue to operate in their personal and professional lives using technologies that are now considered essential for many people. Fundamentally, all data structures within the digital world are faced with risks of data breaches, despite the continued effort to enhance cybersecurity. This is inherently a part of the constantly evolving and dynamic nature of the digital realm, where computational knowledge and expertise are used for various purposes, including unethical ones.

Digital imprint is the core aspect of digital data governance. Through many discourses of data protection and privacy rights, many have addressed that data is often generated without users of digital systems even realizing it. Therefore, it is a fair assessment to think of what constructs a person in the present day cannot be freed from the

[31] Peter C Verhoef and others, 'Digital Transformation: A Multidisciplinary Reflection and Research Agenda', *Journal of Business Research*, 122 (2021), pp. 889–901, doi:https://doi.org/10.1016/j.jbusres.2019.09.022.

[32] The classical understanding of reality, where the identity of an entity relies entirely upon its mind through first-person perspective is continuously losing its relevancy in a digitalized world where sharing is a key element of interaction. This is mainly because of how easy it is to form relationship in the digitalized world, where people can connect, share experiences, and network regardless of the limitations in proximity. *See* Pierpaolo Donati, 'Being Human (or What?) In the Digital Matrix Land: The Construction of the Humanted', in *Post-Human Futures: Human Enhancement, Artificial Intelligence and Social Theory*, 2021, pp. 23–47, doi:10.4324/9781351189958-2.

[33] Kai Tai Chan, 'Emergence of the "Digitalized Self" in the Age of Digitalization', *Computers in Human Behavior Reports*, 6 (2022), pp. 1–7, doi:https://doi.org/10.1016/j.chbr.2022.100191.

[34] Joanna Davis and others, 'Networking via LinkedIn: An Examination of Usage and Career Benefits', *Journal of Vocational Behavior*, 118 (2020), pp. 1–15, doi:https://doi.org/10.1016/j.jvb.2020.103396.

[35] Janna M Parker and others, 'Should Employees Be "Dooced" for a Social Media Post? The Role of Social Media Marketing Governance', *Journal of Business Research*, 103 (2019), pp. 1–9, doi:https://doi.org/10.1016/j.jbusres.2019.05.027.

[36] Md. Sajjad Hosain and Abdullah Mohammad Ahshanul Mamun, 'The Roles of LinkedIn-Based Skill Endorsements and LinkedIn-Based Hiring Recommendations on Hiring Preferences: Evidence from Bangladeshi Employers LinkedIn-Based Hiring Recommendations on Hiring Preferences: Evidence from Bangladeshi Employers', *Management Matters*, 20.2 (2023), pp. 169–84, doi:10.1108/MANM-05-2023-0021.

[37] Jharna Agrawal and Suma Dawn, 'Analyzing the Anatomy of Strategic Networking in Professional Communities: A Case Study Approach', in *Proceedings of the 2024 Sixteenth International Conference on Contemporary Computing* (ACM, 2024), pp. 667–74, doi:10.1145/3675888.3676128.

past digital imprints. Although this is rather dramatic, this is nevertheless a reality that legal frameworks must fully acknowledge in the normative sense.[38] Thus, people who utilize digital technologies should have a decent amount of control over their digital imprints, which are coded inside many forms of digital data. This includes many formats that need to be fully understood and systematically structured in a comprehensive classification and taxonomy of data.

The right to be forgotten is an essential aspect of the privacy rights that must be safeguarded, as it can protect individuals in the digital space from the risks above. Past associations and activities that are no longer a part of someone's life, should not be utilized as a sentence to define that person. Deletion of the relevant data regarding that can ensure that person's perception of safety and identity in the digital space and prevent unnecessary emotional distress and even real-life consequences that may come with them. In the context of cybersecurity, the right to be forgotten plays a crucial role in preventing future data breaches from victimizing individuals, as they will have already deleted their data from the relevant data processors or digital systems.

The most relevant keywords regarding this discourse are perhaps control and autonomy. Individuals should have the ability to determine how their digital imprints are stored, processed, and eventually erased, if necessary. This control is fundamental in ensuring that individuals are not permanently tied to past actions or outdated representations of themselves, especially in a world where people continuously grow and evolve. The autonomy to request deletion or modification of one's digital presence is an essential mechanism to maintain personal agency over one's own identity,[39] preventing outdated, misleading, or irrelevant information from defining who they are.[40] Without such control, digital identities become more of an imposed construct rather than a self-managed extension of one's real-life identity, which can be fundamentally unfair and restrictive.[41]

However, the practical implementation of the right to be forgotten is a complex issue that requires a balance between individual rights and the broader public interest.[42] While individuals should be granted the ability to erase certain parts of their digital history, there must also be clear boundaries on what types of information can be removed and under what circumstances. For instance, removing negative news coverage that serves a legitimate public interest or erasing records of financial fraud or criminal activity could conflict with broader concerns about transparency and accountability. Therefore, an ideal normative construction of the right to be forgotten should incorporate well-defined limitations that prevent its misuse while still upholding the fundamental principle that people should not be permanently shackled to past digital traces that no longer reflect their present reality.

Another key challenge in implementing the right to be forgotten lies in the technical and legal feasibility of ensuring compliance across various platforms and jurisdictions. Digital data is often stored across multiple servers, sometimes in different countries with vastly different data protection laws. This globalized nature of digital ecosystems complicates the enforcement of such a right, as not all platforms may be subject to the same legal frameworks. Additionally, even when deletion requests are granted, data can still persist in archives, backups, or third-party sites beyond the individual's control. Thus, to make the right to be forgotten truly effective, there needs to be a robust, standardized mechanism that ensures proper enforcement while also considering the technical challenges associated with the deletion of digital data across a fragmented and decentralized digital landscape.

Key legal provisions in Indonesia and Thailand

Both Indonesia and Thailand have continued to develop their legal frameworks regarding digital governance. From digital conducts to commerce-related activities, data remains a key aspect that is inseparable and is perhaps even becoming increasingly important as digital technologies continue to develop while being reliant on data. Data as the core normative construct for the discourses involving digital technology highlights not only the importance

[38] Some would argue that this issue symbolizes the nefarious manner of one's past, particularly in the context the right to be forgotten. *See* Sylvie Delacroix and Neil D Lawrence, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance', *International Data Privacy Law*, 9.4 (2019), pp. 236–52, doi:10.1093/idpl/ipz014. However, such argument only adds to the importance of the right to be forgotten, as opposed to going against it.

[39] Hussein A. Abbass, George Leu, and Kathryn Merrick, 'A Review of Theoretical and Practical Challenges of Trusted Autonomy in Big Data', *IEEE Access*, 2016, 2808–30, doi:10.1109/ACCESS.2016.2571058.

[40] Paul Steinbart, Mark J. Keith, and Jeffry S. Babb, 'Measuring Privacy Concerns and the Right to Be Forgotten', in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2017, MMXVII-JANUA, 4967–76, doi:10.24251/hicss.2017.603.

[41] Shania Ann Kirk, 'Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy by Maurice E. Stucke, Oxford, Oxford University Press, 2022, 275 Pp.', *European Journal of Risk Regulation*, 14.4 (2023), pp. 823–25, doi:DOI: 10.1017/err.2023.6.

[42] Saharuddin Saharuddin, 'Pros-Cons of Implementing the Right to Be Forgotten Rules in the ITE Law', *Amsir Law Journal*, 2.1 (2020), pp. 27–30, doi:10.36746/alj.v2i1.31.

of data, but also how technical the nature of legal developments regarding data is. Thus, it is often the case that a lot of regulators end around the world end up focusing on utilizing technological capabilities in regulating digital-related issues, and rightfully so, as it supports legal enforcement.

In the midst of all the technical aspects, it can be easy to overlook the importance of fundamental legal aspects, such as the rights and obligations of all legal subjects involved. In the context of data protection and privacy, this is often the case with the right to be forgotten, which is a fundamental part of privacy rights in the increasingly digitalized world. With the continued mass adaptation of digital technologies, it is not a stretch to even say that privacy rights in the digital rights is one of the most important and dynamic human rights discourses in the world today. Stern legal compliance is key in ensuring that the right to be forgotten is properly protected in data-driven societies around the world. It also serves as the standard practice for data collection, data processing, and data retention, which can have varying practices.

Indonesia has been developing its legal framework for digital-related issues since 2008, with the enactment of Law No. 11 of 2008 on Electronic Information and Transaction (EIT Law). This framework has been updated twice, with the first amendment coming through Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transaction (First Amendment of EIT Law), and the latest one passed through Law No. 1 of 2024 on Second Amendment to Law No. 11 of 2008 on Electronic Information and Transaction (Second Amendment of EIT Law). The EIT Law framework governs general issues within the digital sphere, such as digital conducts and security of electronic systems. It also addresses the importance of data protection, although only in a brief manner, through Article 26 regarding consent.

For data-specific issues, Indonesia started the development of legal frameworks with Minister of Communication and Informatics Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems and Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions. The former introduced consent requirements for data collection and processing, alongside the right to access and correction, as outlined in Article 6 and Article 26. It also set obligations for electronic system providers to ensure data security and notify users of breaches, as stated in Article 5 and Article 28. The latter reinforced these principles by mandating data localization for public sector electronic system providers and regulating cross-border data transfers, as stated in Article 20 and Article 21. It further established the right to erasure and required electronic system providers to implement mechanisms for data removal, as outlined in Article 15 and Article 18.

Thailand, on the other hand, started its effort to regulate digital-related issues with the enactment of the computer-Related Crime Act B.E. 2550 (2007), which laid the foundation for digital governance by addressing offenses related to computer systems and data security. The act criminalized unauthorized access and data interception, as outlined in Section 5 and Section 8, while also prohibiting data modification and system interference, as stated in Section 9 and Section 10. It further imposed obligations on service providers to retain traffic data and cooperate with authorities, as established in Section 26. However, while it provided mechanisms for data seizure and takedown, the law did not establish key privacy rights such as the right to be forgotten, user control over their personal data, or explicit consent requirements for data processing. Its focus remained on cybersecurity and law enforcement rather than comprehensive personal data protection.

Specifically for data protection and privacy, now Indonesia relies on Law No. 27 of 2022 on Personal Data Protection (PDP Law), while Thailand frames its enforcement around Personal Data Protection Act B.E. 2562 (2019) (PDPA). Both regulations are the first comprehensive legal framework for data protection and privacy for their respective countries, setting up a wall of legal compliance that data collectors and processors must abide by. In the context of the right to be forgotten, it is crucial to dive deeply into the legal norms governed by both regulations. Here is the table comparing the normative structures around the right to be forgotten in the PDP Law and the PDPA.

Table 1. Comparative analysis of the right to be forgotten provisions in Indonesia and Thailand

Aspect	Indonesia's PDP Law (Law No. 27 of 2022)	Thailand's PDPA (Personal Data Protection Act B.E. 2562)
Legal Basis	Article 8 and Article 43 establish the right to request deletion of personal data.	Section 33 establishes the right to request deletion or anonymization of personal data.
Scope of Deletion Rights	Covers deletion of personal data upon request if it is no longer necessary (Article 42), consent is withdrawn (Article 43), or obtained unlawfully (Article 44).	Allows data subjects to request deletion when data is no longer needed (Section 33 (1)), consent is withdrawn (Section 33 (2)), or processing was unlawful (Section 33 (4)).

Conditions for Request	Data subjects can request deletion if data processing is no longer required (Article 42), consent is withdrawn (Article 43), or the data was obtained illegally (Article 44).	Requests can be made if data is no longer necessary (Section 33 (1)), consent is withdrawn (Section 33 (2)), or there is unlawful processing (Section 33 (4)).
Exceptions to Deletion	Exceptions apply when data is needed for public interest, law enforcement, or compliance with legal obligations (Article 50).	Exceptions include cases where retention is necessary for freedom of expression, legal claims, public health, or compliance with the law (Section 33 (Paragraph 2)).
Obligations of Data Controllers	Data controllers must delete or destroy data if requested, unless an exception applies, and notify data subjects of the action (Article 45).	Data controllers must take action to delete, anonymize, or restrict processing and inform third parties if data was publicly shared (Section 33 (Paragraph 3)).
Enforcement & Remedies	Failure to comply results in administrative sanctions, including fines and restrictions on data processing (Article 57).	Data subjects can file complaints if deletion requests are ignored; expert committees have authority to enforce compliance (Section 73 and Section 74).

Source: Research Analysis

Thailand's PDPA provides a stronger enforcement mechanism for the right to be forgotten, as it allows individuals to escalate complaints to expert committees with the authority to enforce data deletion, while Indonesia's PDP Law relies primarily on administrative sanctions without a structured dispute resolution process. However, Indonesia's regulation is stricter in imposing a direct obligation on data controllers to delete personal data, ensuring that compliance is not left to interpretation. The weakness of Indonesia's approach is its lack of procedural clarity, since if a data controller refuses a deletion request, individuals have no structured pathway to challenge it beyond regulatory oversight. Thailand, on the other hand, introduces anonymization as an alternative to deletion, which is an advantage because it allows data controllers to retain data for legitimate purposes while still protecting privacy. The issue is whether re-identification is sufficiently regulated, as the law does not explicitly outline strict safeguards against it, though it does authorize further regulations. While Indonesia's law eliminates this risk by requiring outright deletion, it also removes a practical option that balances privacy with operational needs. Neither law fully resolves the balance between strict legal obligations and effective enforcement, making both frameworks incomplete in their approach to the right to be forgotten.

Lessons from South Korea, the United States, and the European Union

South Korea is often regarding as one of the leaders of the Asian Tech industry,[43] who directly competes with global competition through various technologies invented by the country's highly competitive tech industry.[44] Not only that, the fact that it has one of the fastest and most extensive internet network in the world also has played a key role in ensuring the mass utilization of digital technology,[45] which ultimately increases the volume of data generated, collected, and processed every day. This ultimately positions the South Korean society as one of the most digitalized collective not just in Asia, but also the world. Having the sixth highest internet penetration rate among OECD countries[46] also proves this even more, showing that digital technology has truly become an essential part of the South Korean society. South Korea's main legal framework for data protection is Personal Information Protection Act (PIPA), which is considered as one of the toughest data protection laws in the world.[47] This comprehensive legal framework is designed to fulfill the needs of South Korea's highly digitalized society, which has been one of the main drivers of its economy.

[43] Nurwulan Rizkiya Anjani and Tulus Warsito, 'The Factors Driving Success in South Korean Exports: A Case Study of Samsung Electronics', *Jurnal Ilmiah Dinamika Sosial*, 7.1 (2023), pp. 77–86, doi:10.38043/jids.v7i1.4286.

[44] Myung-Hwan Cho, 'Technological Catch-up and the Role of Universities: South Korea's Innovation-Based Growth Explained through the Corporate Helix Model', *Triple Helix*, 1.1 (2014), pp. 2–21, doi:10.1186/s40604-014-0002-1.

[45] Gyeong Suk Jeon and Kyungwon Choi, 'Purposes of Internet Use and Its Impacts on Physical and Psychological Health of Korean Older Adults', *Healthcare (Switzerland)*, 12.2 (2024), pp. 1–12, doi:10.3390/healthcare12020244.

[46] Hyeongjik Lee, Seonkoo Jeong, and Kwanghee Lee, 'The South Korean Case of Deploying Rural Broadband via Fiber Networks by Implementing Universal Service Obligation and Public-Private Partnership Based Project', *Telecommunications Policy*, 47.3 (2023), pp. 1–17, doi:https://doi.org/10.1016/j.telpol.2023.102506.

[47] Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah Irwansyah, 'Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment', *Hasanuddin Law Review*, 10.1 (2024), pp. 1–20, doi:10.20956/halrev.v10i1.5016.

The United States has a rather unique and complex system regarding the legal development of data protection and privacy regulations. This is mainly because of the unique federal-states relationship that plays a major role in the country's legal system. At the federal level, the United States still mainly relies on [insert law here], which is far from enough in protecting data and privacy of its citizens in the digital space, which can be contributed to the fact that it was enacted in 1974. At the state level, the California Consumer Privacy Act (CCPA) stands out as an advanced regulation, mainly because it gives a comprehensive set of rights for consumers over their data, and is very often compared with GDPR.[48] Furthermore, the country's role as a leader in research and development of the global tech industry, makes this regulation all the more important, as some of the biggest tech companies in the world are located in California.

The European Union, to date, still remains as having the best regulation for data protection as privacy, with its globally influential General Data Protection Regulation (GDPR). This law does not only serve as a crucial legal safeguard to protect the data and privacy of Europeans, but also a cornerstone in modern data protection and privacy regulations. Having influenced many legal systems around the world beyond the European borders,[49] it is not an exaggeration to say that this regulation is one of the most influential regulations in the entire legal sphere, particularly because of the rising concerns regarding the development and utilization of data-driven digital technologies.[50]

Specifically for the right to be forgotten, each of the countries provide a set of relevant provisions to ensure that digital technology users have enough autonomy over their data, particularly the right to have them deleted from any digital systems. Here is the list of provisions that govern the right to be forgotten in South Korea, the European Union, and the United States.

Table 2. Provisions for the right to be forgotten in South Korea, the EU, and the US

Aspect	South Korea (PIPA)	European Union (GDPR)	United States (CCPA - California)
Legal Basis	Article 4 and Article 21 establish the right to request deletion of personal data.	Article 17 establishes the right to be forgotten.	Section 1798.105 grants the right to request deletion.
Scope of Deletion Rights	Covers deletion of personal data when it is no longer necessary (Article 4), consent is withdrawn (Article 21), or data is unlawfully collected (Article 37).	Covers deletion of personal data when it is no longer necessary (Article 17(1)(a)), consent is withdrawn (Article 17(1)(b)), or processing was unlawful (Article 17(1)(d)).	Consumers can request deletion of personal data collected from them by businesses (Section 1798.105(a)).
Conditions for Request	Data subjects can request deletion if data processing is no longer required (Article 21), consent is withdrawn (Article 37(2)), or data is inaccurate (Article 36).	Requests can be made if data is no longer relevant (Article 17(1)(a)), consent is withdrawn (Article 17(1)(b)), or processing is unlawful (Article 17(1)(d)).	Requests must be verified (Section 1798.105(c)(1)), and businesses must delete data unless an exception applies.
Exceptions to Deletion	Exceptions apply when data is needed for legal compliance, public interest, or national security (Article 21(3)).	Exceptions exist for freedom of expression, legal obligations, public interest, scientific research, and legal claims (Article 17(3)).	Exceptions include completing transactions, security purposes, legal compliance, and public interest research (Section 1798.105(d)).

[48] Richmond Y. Wong, Andrew Chong, and R. Cooper Aspegren, 'Privacy Legislation as Business Risks: How GDPR and CCPA Are Represented in Technology Companies' Investment Risk Disclosures', *Proceedings of the ACM on Human-Computer Interaction*, 7.CSCW1 (2023), pp. 1–26, doi:10.1145/3579515.

[49] Olukunle Oladipupo Amoo and others, 'GDPR's Impact on Cybersecurity: A Review Focusing on USA and European Practices', *International Journal of Science and Research Archive*, 11.1 (2024), pp. 1338–47, doi:10.30574/ijsra.2024.11.1.0220.

[50] Žaklina Spalević and Kosana Vićentijević, 'GDPR and Challenges of Personal Data Protection', *The European Journal of Applied Economics*, 19.1 (2022), pp. 55–65, doi:10.5937/ejae19-36596.

Obligations of Data Controllers	Data controllers must delete data upon request unless exceptions apply and must ensure data is irreversibly erased (Article 21(2)).	Data controllers must delete data upon request and inform third parties to remove copies or links to the data (Article 17(2)).	Businesses must delete data and notify service providers and third parties to delete shared data (Section 1798.105(c)(1)).
Enforcement & Remedies	Violations result in administrative fines, corrective orders, and potential criminal penalties (Article 64 and Article 71).	Failure to comply can result in fines of up to 4% of annual global turnover or €20 million (Article 83(5)(b)).	Failure to comply can lead to regulatory enforcement, fines, and potential lawsuits (Section 1798.199.55 and Section 1798.199.90).

Source: Research Analysis

The right to be forgotten provisions in South Korea, the European Union, and the United States offer stronger legal clarity, enforcement mechanisms, and broader consumer rights compared to Indonesia's PDP Law and Thailand's PDPA. The EU's GDPR is the most comprehensive, explicitly mandating not only the deletion of personal data but also requiring data controllers to inform third parties to remove copies or links (Article 17(2)), something neither Indonesia nor Thailand's laws address. South Korea's PIPA similarly provides a strict deletion mandate (Article 21) and includes criminal penalties for violations (Article 71), making enforcement more stringent than both Indonesia's reliance on administrative sanctions and Thailand's expert committee enforcement model. The CCPA in the United States, while limited to businesses, still requires companies to notify service providers and third parties to delete shared data (Section 1798.105(c)(1)), a provision missing in Indonesia and Thailand, where deletion obligations focus solely on the data controllers themselves.

Moreover, the EU and South Korea provide clearer conditions for deletion requests, allowing users to erase data not only when consent is withdrawn but also when data is inaccurate or irrelevant, whereas Indonesia and Thailand focus primarily on consent withdrawal as the main justification. South Korea and the EU further enforce strict obligations on data controllers, with the EU imposing fines of up to 4% of global annual turnover (Article 83(5)(b)) and South Korea enforcing corrective orders and criminal penalties (Article 64 and Article 71), surpassing the relatively weaker sanction frameworks in Indonesia and Thailand. Compared to Indonesia, which does not provide a structured dispute resolution mechanism, the US, EU, and South Korea offer better enforcement pathways through fines, lawsuits, and regulatory oversight, making their frameworks more effective at ensuring compliance and protecting data subjects' rights.

Conclusion

Despite the rising concerns of data protection and privacy rights, the right to be forgotten remains as a key aspect that is not as extensively analyzed and discussed as other data protection issues, like data breaches and cybersecurity measures. This shows the lack of respect emphasis on ensuring autonomy and control over data, which puts data subjects at serious risks. Unfortunately, normative analysis with comparative approach of this study finds that there are weaknesses that need to be fixed within the Indonesian and Thai framework for data protection and privacy. Normative issues like Indonesia's lack of structured enforcement mechanisms, Thailand's weaker mandate for data controllers to delete data, Indonesia's lack of procedural clarity for challenging deletion refusals, and the absence of clear regulations on re-identification risks in Thailand's anonymization framework create significant gaps in their legal structures governing the right to be forgotten. South Korea, the European Union, and the United States offer stronger enforcement mechanisms, clearer deletion conditions, and stricter obligations on data controllers compared to Indonesia and Thailand. The EU's GDPR mandates third-party takedowns, South Korea imposes criminal penalties, and the US's CCPA requires businesses to notify service providers of deletion requests, all of which enhance compliance. Additionally, South Korea and the EU allow deletion requests for inaccurate or irrelevant data, unlike Indonesia and Thailand, which primarily focus on consent withdrawal. Their stronger regulatory oversight and structured dispute resolution mechanisms highlight the need for clearer enforcement pathways and procedural safeguards in Indonesia and Thailand's frameworks. Future research can focus on assessing the practical enforcement of the right to be forgotten across different jurisdictions by utilizing the findings of this study, particularly regarding how regulatory mechanisms, deletion obligations, and dispute resolution processes impact compliance and data subject rights in Indonesia and Thailand.

Acknowledgement
The author(s) sincerely express their gratitude to the Editor and anonymous Reviewers for their constructive feedback, to prior scholars whose works have significantly enriched this study, and to Universitas Internasional Batam for its material and formal support in facilitating this collaborative research.

Author Contributions Statement
The author(s) contributed equally to the conceptualization, methodology, analysis, drafting, revision, and final approval of this manuscript.

AI Usage Statement
The author(s) declare that no generative AI or AI-assisted technologies were used in the preparation or writing of this manuscript, and that all content was independently conceived, developed, and written entirely by the author(s) without any automated assistance.

Conflict of Interest
The author(s) declare that there are no conflicts of interest regarding the publication of this manuscript, and that the research was conducted in the absence of any financial or commercial relationships that could be construed as a potential conflict of interest.

References

Abbass, Hussein A., George Leu, and Kathryn Merrick, 'A Review of Theoretical and Practical Challenges of Trusted Autonomy in Big Data', *IEEE Access*, 2016, 2808–30, doi:10.1109/ACCESS.2016.2571058

Agrawal, Jharna, and Suma Dawn, 'Analyzing the Anatomy of Strategic Networking in Professional Communities: A Case Study Approach', in *Proceedings of the 2024 Sixteenth International Conference on Contemporary Computing* (ACM, 2024), pp. 667–74, doi:10.1145/3675888.3676128

Amoo, Olukunle Oladipupo, Akoh Atadoga, Femi Osasona, Temitayo Oluwaseun Abrahams, Benjamin Samson Ayinla, and Oluwatoyin Ajoke Farayola, 'GDPR's Impact on Cybersecurity: A Review Focusing on USA and European Practices', *International Journal of Science and Research Archive*, 11.1 (2024), pp. 1338–47, doi:10.30574/ijsra.2024.11.1.0220

Anjani, Nurwulan Rizkiya, and Tulus Warsito, 'The Factors Driving Success in South Korean Exports: A Case Study of Samsung Electronics', *Jurnal Ilmiah Dinamika Sosial*, 7.1 (2023), pp. 77–86, doi:10.38043/jids.v7i1.4286

Bakare, Seun Solomon, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe, and Nkechi Emmanuella Eneh, 'Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations', *Computer Science & IT Research Journal*, 5.3 (2024), pp. 528–43, doi:10.51594/csitrj.v5i3.859

Brock, George, *The Right to Be Forgotten: Privacy and the Media in the Digital Age*, 1st edn (I.B.Tauris & co. Ltd, 2016)

Chan, Kai Tai, 'Emergence of the "Digitalized Self" in the Age of Digitalization', *Computers in Human Behavior Reports*, 6 (2022), pp. 1–7, doi:https://doi.org/10.1016/j.chbr.2022.100191

Cho, Myung-Hwan, 'Technological Catch-up and the Role of Universities: South Korea's Innovation-Based Growth Explained through the Corporate Helix Model', *Triple Helix*, 1.1 (2014), pp. 2–21, doi:10.1186/s40604-014-0002-1

Choi, Yongrok, Siyu Li, and Hyoungsuk Lee, 'Korean Paradox of Public Support for the Research and Development Investment in the Sustainable Performance of the Regional Economy', *Land*, 13.6 (2024), pp. 1–20, doi:10.3390/land13060759

Cieslik, Katarzyna, and Dániel Margócsy, 'Datafication, Power and Control in Development: A Historical Perspective on the Perils and Longevity of Data', *Progress in Development Studies*, 22.4 (2022), pp. 352–73, doi:10.1177/14649934221076580

Davis, Joanna, Hans-Georg Wolff, Monica L Forret, and Sherry E Sullivan, 'Networking via LinkedIn: An Examination of Usage and Career Benefits', *Journal of Vocational Behavior*, 118 (2020), pp. 1–15, doi:https://doi.org/10.1016/j.jvb.2020.103396

Dayton, Leigh, 'How South Korea Made Itself a Global Innovation Leader', *Nature*, 581.7809 (2020), pp. S54–56, doi:10.1038/d41586-020-01466-7

Delacroix, Sylvie, and Neil D Lawrence, 'Bottom-up Data Trusts: Disturbing the "One Size Fits All" Approach to Data Governance', *International Data Privacy Law*, 9.4 (2019), pp. 236–52, doi:10.1093/idpl/ipz014

Disemadi, Hari Sutra, 'Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies', *Journal of Judicial Review*, 24.2 (2022), pp. 289–304, doi:10.37253/jjr.v24i2.7280

Donati, Pierpaolo, 'Being Human (or What?) In the Digital Matrix Land: The Construction of the Humanted', in *Post-Human Futures: Human Enhancement, Artificial Intelligence and Social Theory*, 2021, pp. 23–47, doi:10.4324/9781351189958-2

Gracy, Shanitamol Sojan, 'A Global Analysis of Data Breaches from 2004 to 2024' (University of London, 2024), doi:10.48550/arXiv.2502.05205

Hosain, Md. Sajjad, and Abdullah Mohammad Ahshanul Mamun, 'The Roles of LinkedIn-Based Skill Endorsements and LinkedIn-Based Hiring Recommendations on Hiring Preferences: Evidence from Bangladeshi Employers LinkedIn-Based Hiring Recommendations on Hiring Preferences: Evidence from Bangladeshi Employers', *Management Matters*, 20.2 (2023), pp. 169–84, doi:10.1108/MANM-05-2023-0021

Jakobi, Timo, Maximilian von Grafenstein, Patrick Smieskol, and Gunnar Stevens, 'A Taxonomy of User-Perceived Privacy Risks to Foster Accountability of Data-Based Services', *Journal of Responsible Technology*, 10 (2022), pp. 1–14, doi:https://doi.org/10.1016/j.jrt.2022.100029

Jeon, Gyeong Suk, and Kyungwon Choi, 'Purposes of Internet Use and Its Impacts on Physical and Psychological Health of Korean Older Adults', *Healthcare (Switzerland)*, 12.2 (2024), pp. 1–12, doi:10.3390/healthcare12020244

Judijanto, Loso, Nuryati Solapari, and Donny Eddy Sam Karauwan, 'A Bibliometric Analysis of Legal Approaches to Personal Data Protection', *The Easta Journal Law and Human Rights*, 2.3 (2024), pp. 165–75, doi:10.58812/eslhr.v2i03.285

Kirk, Shania Ann, 'Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy by Maurice E. Stucke, Oxford, Oxford University Press, 2022, 275 Pp.', *European Journal of Risk Regulation*, 14.4 (2023), pp. 823–25, doi:DOI: 10.1017/err.2023.6

Kohl, Uta, 'The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy', *International and Comparative Law Quarterly*, 72.3 (2023), pp. 737–69, doi:DOI: 10.1017/S0020589323000258

Lawrance, Vincent, 'Book Review: The Right to Be Forgotten: Privacy and Media in the Digital Age', *Media International Australia*, 167.1 (2018), pp. 182–83, doi:10.1177/1329878X18756108

Lee, Hyeongjik, Seonkoo Jeong, and Kwanghee Lee, 'The South Korean Case of Deploying Rural Broadband via Fiber Networks by Implementing Universal Service Obligation and Public-Private Partnership Based Project', *Telecommunications Policy*, 47.3 (2023), pp. 1–17, doi:https://doi.org/10.1016/j.telpol.2023.102506

Lee, Sasha, and Alberto Iskandar, 'Southeast Asia, Cyber Threats, and Opportunities for Canadian Co-Operation: The Cases of Singapore and the Philippines', *The Asia Pacific Foundation of Canada (APF Canada)*, 2024 <https://www.asiapacific.ca/publication/southeast-asia-cyber-threats-and-opportunities-canadian-co> [accessed 18 February 2025]

Mantelero, Alessandro, 'The Future of Data Protection: Gold Standard vs. Global Standard', *Computer Law & Security Review*, 40 (2021), pp. 1–5, doi:https://doi.org/10.1016/j.clsr.2020.105500

Nakashima, Mika, 'The Legal Frameworks of the Right to Request the Deletion of Personal Data in the EU, the U.S. and Japan and the Right to Be Forgotten: A Study Focusing on Search Businesses', in *IFIP Advances in Information and Communication Technology*, 2020, dxc, 29–40, doi:10.1007/978-3-030-62803-1_3

Parker, Janna M, Shelly Marasi, Kevin W James, and Alison Wall, 'Should Employees Be "Dooced" for a Social Media Post? The Role of Social Media Marketing Governance', *Journal of Business Research*, 103 (2019), pp. 1–9, doi:https://doi.org/10.1016/j.jbusres.2019.05.027

Pereira, Carolina, Anabela Marto, Roberto Ribeiro, Alexandrino Gonçalves, Nuno Rodrigues, Carlos Rabadão, and others, 'Security and Privacy in Physical–Digital Environments: Trends and Opportunities', *Future Internet*, 17.2 (2025), pp. 1–23, doi:10.3390/fi17020083

Ponemon Institute, and IBM Security, *Cost of a Data Breach 2022*, *IBM Corportation and Ponemon Institute Research* (2022) <https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High>

Prabasari, Ni Kadek Dhea Ardi, Kadek Januarsa Adi Sudharma, and Michael Angelo, 'The Right to Be Forgotten: Regulation of Personal Data Deletion in Indonesia', *KRTHA BHAYANGKARA*, 18.3 (2024), pp. 541–58, doi:10.31599/krtha.v18i3.3291

Primawanti, Henike, Agus Subagyo, and Windy Dermawan, 'ASEAN 4.0. Era: Development in Digital Economy and Trade Sector', *Dinamika Global: Jurnal Ilmu Hubungan Internasional*, 7.2 (2022), pp. 333–49, doi:https://doi.org/10.36859/jdg.v7i02.1279

Putri, Ni Made Dwi Gayatri, Ni Luh Made Mahendrawati, and Ni Made Puspasutari Ujianti, 'Perlindungan Hukum Terhadap Data Pribadi Warga Negara Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022', *Jurnal Preferensi Hukum*, 5.2 (2024), pp. 240–45, doi:10.22225/jph.5.2.8087.240-245

Ramokapane, Kopo Marvin, and Awais Rashid, 'ExD: Explainable Deletion', in *New Security Paradigms Workshop* (ACM, 2023), pp. 34–47, doi:10.1145/3633500.3633503

Rizkinaswara, Leski, 'Dugaan Kebocoran Data SIM Card, Kominfo Lakukan Koordinasi Dengan Ekosistem Pengendali Data', *Direktorat Jenderal Aplikasi Informatika KOMINFO*, 2022 <https://aptika.kominfo.go.id/2022/09/dugaan-kebocoran-data-sim-card-kominfo-lakukan-koordinasi-dengan-ekosistem-pengendali-data/> [accessed 18 February 2025]

Saharuddin, Saharuddin, 'Pros-Cons of Implementing the Right to Be Forgotten Rules in the ITE Law', *Amsir Law Journal*, 2.1 (2020), pp. 27–30, doi:10.36746/alj.v2i1.31

Santana, Paulo Campanha, and Faiz Ayat Ansari, 'Data Protection and Privacy as a Fundamental Right: A Comparative Study of Brazil and India', *Journal of Liberty and International Affairs*, 9.3 (2023), pp. 456–70, doi:10.47305/JLIA2393555cs

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah, 'Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment', *Hasanuddin Law Review*, 10.1 (2024), pp. 1–20, doi:10.20956/halrev.v10i1.5016

Spalević, Žaklina, and Kosana Vićentijević, 'GDPR and Challenges of Personal Data Protection', *The European Journal of Applied Economics*, 19.1 (2022), pp. 55–65, doi:10.5937/ejae19-36596

Sriyai, Surachanee, 'Data Leaks: Thai Government Tough on Private Firms, Soft on Public Sector and Cybercriminals', *Fulcrum*, 2024 <https://fulcrum.sg/data-leaks-thai-government-tough-on-private-firms-soft-on-public-sector-and-cybercriminals/> [accessed 18 February 2025]

Steinbart, Paul, Mark J. Keith, and Jeffry S. Babb, 'Measuring Privacy Concerns and the Right to Be Forgotten', in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2017, mmxvii-Janua, 4967–76, doi:10.24251/hicss.2017.603

Sudirman, Lu, Hari Sutra Disemadi, and Arwa Meida Aninda, 'Comparative Analysis of Personal Data Protection Laws in Indonesia and Thailand: A Legal Framework Perspective', *Jurnal Etika Demokrasi*, 8.4 (2023), pp. 497–510 <https://journal.unismuh.ac.id/index.php/jed/article/view/12875>

Sukmawan, Denny Indra, and David Putra Setyawan, 'Hacker, Fear, and Harm: Data Breaches and National Security', *Jurnal Global & Strategis*, 17.1 (2023), pp. 153–82, doi:10.20473/jgs.17.1.2023.153-182

Syailendra, Moody Rizqy, Gunardi Lie, and Amad Sudiro, 'Personal Data Protection Law in Indonesia: Challenges and Opportunities', *Indonesia Law Review*, 14.2 (2024), pp. 56–72 <https://scholarhub.ui.ac.id/ilrev/vol14/iss2/4/>

Tan, David, 'Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum', *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, 8.5 (2021), pp. 2463–78 <https://jurnal.um-tapsel.ac.id/index.php/nusantara/article/view/5601>

Tung, Rosalie L, Ivo Zander, and Tony Fang, 'The Tech Cold War, the Multipolarization of the World Economy, and IB Research', *International Business Review*, 32.6 (2023), pp. 1–14, doi:https://doi.org/10.1016/j.ibusrev.2023.102195

Utomo, Setyo, 'Personal Data Protection Through Law Number 27 of 2022: Challenges of Cybercrime in the Era of Globalization and Digital', *Pena Justisia: Media Komunikasi Dan Kajian Hukum*, 23.3 (2024), pp. 2967–75, doi:10.31941/pj.v23i3.5611

Verhoef, Peter C, Thijs Broekhuizen, Yakov Bart, Abhi Bhattacharya, John Qi Dong, Nicolai Fabian, and others, 'Digital Transformation: A Multidisciplinary Reflection and Research Agenda', *Journal of Business Research*, 122 (2021), pp. 889–901, doi:https://doi.org/10.1016/j.jbusres.2019.09.022

Wang, Qian, Eric W.T. Ngai, Daniel Pienta, and Jason Bennett Thatcher, 'Information Technology Innovativeness and Data-Breach Risk: A Longitudinal Study', *Journal of Management Information Systems*, 40.4 (2023), pp. 1139–70, doi:10.1080/07421222.2023.2267319

Wong, Richmond Y., Andrew Chong, and R. Cooper Aspegren, 'Privacy Legislation as Business Risks: How GDPR and CCPA Are Represented in Technology Companies' Investment Risk Disclosures', *Proceedings of the ACM on Human-Computer Interaction*, 7.CSCW1 (2023), pp. 1–26, doi:10.1145/3579515

Xie, Sherry Li, 'Retention in "the Right to Be Forgotten" Scenario: A Records Management Examination', *Records Management Journal*, 26.3 (2016), pp. 279–92, doi:10.1108/RMJ-11-2015-0038