

CRIMINAL LAW PROTECTION TO THE RIGHT TO PRIVACY IN THE UTILIZATION OF DIGITAL TECHNOLOGY

Andreas Eno Tirtakusuma
Universitas Pancasila, Jakarta, Indonesia
andreaseno@univpancasila.ac.id

Eleazar Josiah Tirtakusuma
Universitas Airlangga, Surabaya, Indonesia
eleazar.josiah.tirtakusuma-2023@fh.unair.ac.id

Abstract

The rapid development of digital technology, including artificial intelligence, has brought tremendous progress for human rights, but also a real threat to privacy, where states and companies can now easily track, analyze, predict, and even manipulate people's behavior on a massive scale such as through wiretapping, surveillance, or police raids related to online gambling without strict safeguards, which risks undermining individual dignity, autonomy, and rights. Therefore, this study aims to examine and formulate an ideal concept for protecting privacy rights within the confines of Indonesian criminal law, particularly amidst rapid technological evolution. The method used is normative legal research with a juridical and philosophical approach, to identify various laws and philosophies related to privacy protection in the criminal realm, while delving into the legal issues in depth. The results reveal that existing regulations still need to be supported by the theory of privacy as a human right and the concept of law as a protective sword and shield. In conclusion, the ideal concept must integrate these principles into the Indonesian legal framework, so that technology remains a driver of progress without sacrificing citizens' privacy.

Keyword: Artificial Intelligence, Criminal Law, Digital Technology, Privacy Rights, Protection of Human Rights.

A. INTRODUCTION

In the digital era, the use of mobile phones by students in school environments has become a complex issue. On the one hand, mobile phones can be a means of supporting learning and communication, but on the other hand, their use often gives rise to various ethical and disciplinary problems in schools.¹ Many educational institutions are trying to establish rules that limit or monitor the use of cell phones so that they do not disrupt the teaching and learning process. However, these supervisory measures often lead to

¹ Nehaluddin Ahmad, "Data privacy issues and risks with sharing on social media: An inquiry," *Russian Law Journal* 11, no. 4 (2023): 563.

incidents, especially when the boundaries between teacher authority and students' privacy rights are crossed.

An incident involving a teacher checking a student's mobile phone at school has sparked widespread discussion on social media, particularly on TikTok. In the circulating video, the teacher is seen scrolling through the student's phone screen as if inspecting its contents. This action has drawn mixed reactions from netizens. Most TikTok users believe that the teacher's behavior violated the student's right to privacy, which should still be respected even within the school environment. Comments flooded in, such as "Fortunately, my school respects privacy," and "We have privacy," while others criticized more harshly, saying, "The teacher doesn't understand privacy?" The incident has triggered a broader debate about the boundaries of a teacher's authority in enforcing discipline and the importance of protecting students' privacy rights in the digital age.²

Meanwhile, in Mataram, Lombok, a teacher at SMA Negeri 2 reportedly conducted a sudden inspection of students' mobile phones. Inspections like this are routinely carried out to anticipate suspicious access histories, including online gambling.³ In Surabaya, during a gangster raid, it was found that many of its members were still teenagers. Hence, the Head of the Surabaya City Education Office asked schools to conduct checks on students, especially checking cell phones and the contents of student bags to ensure that no students were members of gangs. The recommendation is to check the contents of students' bags, for example, to find out if there are sharp weapons. Checking mobile phones is more likely to find out if there is a direction of gangster membership or invitations/provocations to fights and other despicable activities. Checking students' cell phones and bags has been carried out for a long time, but is being improved again.⁴

There was also a case in Surabaya where a young man was raided by the police while playing online gambling at a coffee shop. When he was raided, he played the PG Mahjong Ways slot online gambling. The young man works as a cleaning service every day. From the dealer, it is proven that he is doing online slot gambling using money as a bet, so he was then taken to the local

² Yohanes Liestyo Poerwoto, "VIRAL Video Guru Mengecek HP Siswanya saat Ujian dan Diduga Langgar Privasi, Ini Klarifikasinya," *TRIBUNNEWS.COM*. Retrieved in July 23, 2025 from https://www.tribunnews.com/regional/2022/03/16/viral-video-guru-mengecek-hp-siswanya-saat-ujian-dan-diduga-langgar-privasi-ini-klarifikasinya#google_vignette.

³ Nirkomala, "SMAN 2 Mataram Sidak Handphone Siswa Antisipasi Konten Judi Online," *Antara News Mataram*. Retrieved in July 23, 2025 from <https://mataram.antaranews.com/berita/358458/sman-2-mataram-sidak-handphone-siswa-antisipasi-konten-judi-online>.

⁴ Esti Widiyana, "Pastikan Siswa Tak Gabung Gangster, Guru Diminta Rutin Cek HP Siswa". *Detik.com*, Retrieved in July 19, 2025 from <https://www.detik.com/jatim/berita/d-6446825/pastikan-siswa-tak-gabung-gangster-guru-diminta-rutin-cek-hp-siswa>.

Police Station to undergo further examination. The young man admitted that he had played online gambling several times with the excuse of looking for additional money for his daily needs. As a result, the police confiscated his cellphone, one screenshot of an online gambling game, one proof of deposit, and one proof of bank account mutation as evidence of his actions.⁵

The raid also targeted police members in Pali, South Sumatra. This mobile phone raid was carried out on police members to comb through online gambling applications, online loans, and online games in the cell phones of local police members. From the results of the raid, no police personnel played online gambling. However, in this activity, the police provost who tightened the investigation conveyed a message that they should not do things that violate internal police regulations and the police law. The raid on police members' cellphones was carried out in anticipation of an incident in Mojokerto, East Java. A member of the Jombang Police who is addicted to online gambling, Briptu Rian Dwi Wicaksono (27), was burned to death by his wife, who is also a member of the police, namely Briptu Fadhilatun Nikmah (28), a member of the Mojokerto City Police.⁶

Privacy is the right of every individual to keep their personal information from being disseminated or accessed by other parties without permission. In modern information and communication technology, privacy includes the protection of personal data, limitations on the collection of information by third parties, and individual control over data shared in the digital world.⁷ Privacy is an important issue because of technological developments, such as the Internet and social media, which allow massive and fast access to personal information. Privacy can be understood from several dimensions: information privacy, which ensures control over personal data; communication privacy, which protects private exchanges from unauthorized access; physical privacy, which restricts surveillance in personal spaces; and organizational privacy, which safeguards sensitive internal information critical to business continuity.⁸

Examples of privacy in everyday life include a variety of situations where individuals have the right to keep their personal information or activities from

⁵ Arry DwiSaputra, "Cleaning Service di Surabaya Digerebek Polisi Saat Bermain Judi Online di Warkop," *JPNN.com*, Retrieved in July 29, 2025 from <https://jatim.jpnn.com/kriminal/30772/cleaning-service-di-surabaya-digerebek-polisi-saat-bermain-judi-online-di-warkop>.

⁶ Heru, "Random, Propam Polres PALI Razia Hp Anggota Sore Jelang Pulang Dinas, Sweeping Aplikasi Judi Online dan Pinjol," *Sumateraekspres.id*. Retrived in Juny 14 2025 from <https://sumateraekspres.bacakoran.co/read/48956/random-propam-polres-pali-razia-hp-anggota-sore-jelang-pulang-dinas-sweeping-aplikasi-judi-online-dan-pinjol>.

⁷ Benedict Rumbold, and James Wilson, "Privacy rights and public information," *Journal of Political Philosophy* 27, no. 1 (2019): 12.

⁸ H. Jeff Smith, Tamara Dinev, and Heng Xu, "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* 5, no. 4 (2011): 996. See too, D. J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, 154, no. 3 (2006): 359.

being known or used by others. For example, personal data, namely information such as identity numbers, home addresses, telephone numbers, and health history that can only be accessed by certain parties, such as health institutions or governments; privacy on social media, such as users can choose to limit who can see their posts, photos, and profile information; conversation privacy, for example, the right to keep communications such as emails, text messages, and phone conversations confidential from being intercepted or read by other parties without permission.⁹ From this explanation, what is in the cellphone can be seen as the privacy of the owner of the cellphone, so the existence of raids and inspections, as described above, more or less invades the owner's privacy.

Privacy is part of human rights, as enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR), which states that no person should interfere in their personal life, family, or correspondence.¹⁰ In Indonesia, the regulation of the right to privacy as part of human rights can refer to [there is a formulation of Article 28G paragraph 1 of the 1945 Constitution, which protects the privacy of individuals from interference or violations that can threaten human honor and dignity.

Since privacy is directly related to individuals' security, freedom, and self-esteem, its protection is essential. Protecting privacy means giving individuals control over their personal information and protecting them from potential misuse that can be detrimental, such as identity fraud, defamation, and financial losses. In addition, privacy allows a person to maintain their integrity, living a life without worrying that their actions and personal information are constantly being monitored or freely accessed by others.¹¹

No wonder some resist hard when their right to privacy is threatened. In the modern era, communication technology devices (such as mobile phones and laptops) have become the storage of any data classified as private. Recently, there was an incident when a cadet of the Police Academy with the initials BVA was involved in a verbal and physical fight with his caregiver, which led to his dishonorable dismissal. It started when the caregiver found the laptop brought by the BVA Cadet Brigadier; the cadets of the Police Academy should not be allowed to bring laptops. Police Academy cadets tried to snatch

⁹ S. D. Warren, & Brandeis, L. D., "The Right to Privacy," *Harvard Law Review*, 4, No. 5, (1890): 849. See too, D. J. Solove, "I've Got Nothing to Hide and Other Misunderstandings of Privacy," *San Diego Law Review*, 44, no. 4, (2007): 578.

¹⁰ Susanne Barth, and Menno DT De Jon, "The Privacy Paradox—Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review," *Telematics and Informatics* 34, no. 7 (2017): 1043.

¹¹ Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science* 347, no. 6221 (2015): 510. See too, Herman T. Tavani, and James H. Moor, "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies," *ACM Sigcas Computers and Society* 31, no. 1 (2001): 9.

his computer, which was about to be detained by the caregiver officer and even pushed his caregiver to fall.¹²

In addition to the threat of privacy violations due to racial activities or inspections, as described above, technological developments can also increase the risk of privacy attacks. The more people rely on digital technology, the more vulnerable they are to data breaches, hacking, and other cyber threats. The progression of technology has additionally brought about innovative tools like artificial intelligence and the Internet of Things. These advancements, despite their numerous advantages, introduce fresh concerns about safeguarding personal information. Furthermore, a significant number of individuals are unaware of the potential dangers that could arise if their information is compromised.¹³

One of the main obstacles to ensuring data privacy in the digital era is the limited public awareness about safeguarding personal information. Many individuals remain unaware of the dangers posed when their data is misused, including identity theft and financial crimes. In addition, the lack of proper regulation is also a problem in protecting data privacy, especially in developing countries.¹⁴ The inadequate enforcement of data protection in Indonesia has triggered frequent data breaches. This is reflected in the increasing cybercrime cases, including social media account intrusions, which cause personal information leaks, blackmail, and digital fraud.¹⁵

While various previous studies have addressed privacy rights in the context of digital technology, such as studies on personal data regulation in Europe or the impact of AI on global surveillance, significant gaps remain in Indonesia, where the primary focus is often limited to civil or constitutional aspects without delving into integration with criminal law. Research on digital raids and privacy invasions, such as student or police mobile phone searches, rarely explores the theory of privacy as a human right and the concept of law as a protective sword and shield, leaving room for the development of ideal concepts contextualized to technological evolution in developing countries like

¹² Kiki dan Ihsanuddin Safitri, "Nasib Taruna Akpol Usai Dipecat karena Lawan Pengasuhnya," *Kompas.com*, Retrieved in July 23, 2025 from <https://nasional.kompas.com/read/2024/09/10/12163971/nasib-taruna-akpol-usai-dipecat-karena-lawan-pengasuhnya>.

¹³ KOMINFO, "Pentingnya Pelindungan Data Pribadi di Era Digital," *KOMINFO*, Retrieved in July 23, 2025 from <https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital/>.

¹⁴ University of Medan Area, "Data Privacy in the Digital Age: Challenges and Solutions," *University of Medan Area*. Retrieved in July 29, 2025 from <https://baraka.uma.ac.id/privasi-data-dalam-era-digital-tantangan-dan-solusi/>.

¹⁵ Kiki dan Ihsanuddin Safitri, "Nasib Taruna Akpol Usai Dipecat karena Lawan Pengasuhnya," *Kompas.com*, Retrieved in July 23, 2025 from <https://nasional.kompas.com/read/2024/09/10/12163971/nasib-taruna-akpol-usai-dipecat-karena-lawan-pengasuhnya>

Indonesia. Recent research on privacy rights in Indonesian criminal law highlights the growing impact of digital technologies. Studies on personal data protection in 2025 address rising cybercrime, while the new Criminal Code 2023 introduces sanctions for data falsification and theft. Research on personal data agencies 2025 emphasizes reform against doxing and digital vigilantism. Theoretical discussions frame privacy as a human right, balancing state surveillance with autonomy in the post-truth, AI, and IoT era.

The advancement of digital technology raises urgent questions about the protection of privacy rights in Indonesia, particularly within criminal law. On the one hand, it is necessary to examine how existing laws safeguard this right; on the other, it is increasingly important to expand such protection in line with technological developments. This study applies normative legal research through statutory and philosophical approaches to identify relevant regulations and principles. By doing so, it seeks to develop an ideal concept of privacy protection, positioning privacy as a fundamental human right and the law as both a sword to enforce justice and a shield to defend individual rights in the digital era.

This research is theoretically controversial, formulating an ideal concept of privacy rights protection in Indonesian criminal law, integrating the theory of privacy as a human right and law as a protective sword and shield, thereby enriching normative discourse in developing countries. Practically, the results can serve as recommendations for policymakers to strengthen regulations such as the new Criminal Code, including preventing invasive digital raids in schools and police, and increasing public awareness of the risks of cybercrime, ultimately supporting the implementation of more effective data protection laws in the technology era.

B. RESEARCH METHODS

Legal science carries a distinctive nature, characterized by its normative, practical, and predictive dimensions.¹⁶ Based on this view, the present study adopts normative legal research to address the problem formulations. This type of research positions law as a system of norms, encompassing principles, rules, statutory provisions, and judicial decisions. To analyze the issues, two approaches are employed: the statute approach, which examines relevant legislation, and the philosophical approach, which explores the underlying values and principles that form the foundation of legal protection.¹⁷

The reasoning used in this research is deductive, starting from general norms regarding the right to privacy as a human right in Indonesian criminal

¹⁶ Mukti Fajar, N. D., and Yulianto Achmad, *Dualisme Penelitian Hukum Normatif & Empiris*, (Yogyakarta: Pustaka Pelajar, 2013), 35.

¹⁷ Muhaimin, *Metode Penelitian Hukum*, (Mataram: Mataram University Press, 2020), 56.

law, then applying them to specific cases such as digital raids and technological surveillance. This approach allows for logical analysis to identify inconsistencies between existing regulations and contemporary challenges, such as invasion of privacy through student or police cell phone searches, thus formulating an ideal concept that aligns with the problem formulation.

The laws analyzed include primary sources such as the post-reform 2023 Criminal Code (KUHP) concerning criminal defamation and data embezzlement, Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments, and the 2022 Personal Data Protection Law (UU PDP), which regulates criminal sanctions for digital privacy violations. Furthermore, Article 28G paragraph (1) of the 1945 Constitution and Article 12 of the Universal Declaration of Human Rights (UDHR) serve as a philosophical basis for exploring privacy protection in the context of criminal law.

C. RESULTS AND DISCUSSION

1. Theoretical Foundation: Legal Framework for Privacy Rights Protection in Indonesia and International Comparisons

In Indonesia, privacy is protected by several regulations. Although not explicitly written or stated in the 1945 Constitution, the right to confidentiality is implicitly contained and protected as part of human rights protection by Article 28G section (1) of the 1945 Constitution.¹⁸ The formulation presented in the article corresponds with the protection of privacy rights as enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR) and later incorporated into Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Within the Indonesian context, Article 28G paragraph (1) of the 1945 Constitution affirms that every person has the right to personal protection, as well as to the protection of family, honor, dignity, and property.¹⁹ This constitutional guarantee is further reinforced by Law Number 27 of 2022 on Personal Data Protection, which sets out the rights and obligations of data subjects and imposes sanctions for violations of privacy. In addition, Law Number 11 of 2008, as amended by Law Number 19 of 2016 on Electronic Information and Transactions (EIT Law), prohibits unauthorized access to electronic information that infringes upon individual privacy.²⁰

¹⁸ Kadek Rima Anggen Suari, and I. Made Sarjana, "Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023): 139.

¹⁹ Thiara Dewi Purnama, and Abdurrahman Alhakim, "Pentingnya Uu Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia," *Jurnal Komunitas Yustisia* 4, no. 3 (2021): 1058.

²⁰ Some of its provisions were later repealed with *Kitab Undang-Undang Hukum Pidana*, Law Number 1 Year 2023, LN 2023/1, TLN 6842, namely related to the provisions stipulated in Article 27 paragraph (1), Article 27 paragraph (3), Article 28 paragraph (2), Article 30, Article 31

To give you an idea, in America, privacy protection arrangements are scattered in many laws. The concept of privacy pertains to a person's capacity to control the timing, method, and reason for which their private details are utilized by other parties. The safeguarding of privacy is essential in guaranteeing a person's respect, security, and autonomy. It empowers people to cultivate their character without constraint.²¹

A number of federal statutes in the United States regulate privacy and information security in various contexts. The Privacy Act of 1974, codified at 5 U.S.C. §552a, provides protections for personal records of individuals, including citizens and lawful permanent residents, that are maintained by federal agencies and accessed through personal identifiers. The Act obliges agencies to safeguard such records within a defined System of Records (SOR) and is currently undergoing revision to strengthen its provisions. Complementing this, the Federal Information Security Modernization Act of 2014 an amendment to the Federal Information Security Management Act of 2002 (44 U.S.C. 3541) requires agencies to establish and implement comprehensive programs that ensure the security of information and information systems supporting agency operations. Similarly, the E-Government Act of 2002 (44 U.S.C. 3601 et seq.) sets procedures to protect the privacy of personal information contained in electronic records. In terms of transparency, the Freedom of Information Act (FOIA) grants individuals the right to access federal agency records, subject to nine exemptions and three specific exclusions concerning law enforcement documents.

In addition, the Trade Secrets Act (18 U.S.C. 1905) imposes criminal liability for the unauthorized disclosure of trade secrets or other business-sensitive information. To reduce administrative burdens, the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.) aims to minimize redundant or unnecessary government surveys imposed on the public. Lastly, the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501–06) regulates the collection and use of personal information from children under the age of 13, particularly through its Online Privacy Protection Rule. The Social Security Number Fraud Prevention Act of 2017 (Public Law 115-59): (1) prohibits federal agencies from including any individual's Social Security account number on any document sent by mail unless the agency head determines

paragraph (1), Article 31 paragraph (2), Article 36, Article 45 paragraph (1), Article 45 paragraph (3), Article 45A paragraph (2), Article 46, Article 47, and Article 51 paragraph (2).

²¹ U.S. Department of Commerce, "Privacy Laws, Policies and Guidance," *Office of Privacy and Open Government*. Retrieved in July 23, 2025 from <https://www.commerce.gov/opog/privacy/privacy-laws-policies-and-guidance#:~:text=The%20Privacy%20Act%20of%201974,retrieved%20by%20a%20personal%20identifier>

that such inclusion is necessary; and (2) requires agencies that have Chief Financial Officers to issue regulations, within five years of this bill's enactment, that specify the circumstances under which such inclusion is necessary.

2. Privacy Rights and Technological Development

Mobile computing and smart devices have enabled us to make payments remotely, book conference rooms, access buildings, unlock computers, and even order coffee. Technological interconnectivity facilitates these transactions.²² This extends the benefits of technology, which has provided millions of additional conveniences, but some implications arise from these advances.²³

In the use of technology, protection not only needs to be provided to data, but protection to users is also essential. The user's perception of privacy in a multimedia environment will determine which information is private and in what context.²⁴ Determining which compromises users are prepared to accept reveals that a certain degree of privacy infringement is deemed permissible, even when the decision rests with the user. Consequently, safeguarding personal information becomes ineffective if technology users do not understand how crucial their privacy is, leading them to grant access to their data.²⁵ The wider adoption of multimedia communication technologies introduces potential downsides alongside their advantages. The connection between technology and privacy is notably intricate.²⁶

Digital technology today covers economic activities driven by the interconnectedness of individuals, businesses, devices, data, and processes. It involves online transactions across multiple sectors and is enabled by technologies such as the Internet, mobile applications, big data, and information and communication systems.²⁷ The digital economy is fundamentally rooted in the Internet, which functions as its primary

²² Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Harald Sundmaeker, Markus Eisenhauer, Klaus Moessner, Franck Le Gall, and Philippe Cousin, "Internet of Things Strategic Research and Innovation Agenda," In *Internet of things*, (Denmark: River Publishers, 2022), 151.

²³ Laurent Antonczak, *Creativity on the move. How Can Mobile Technology Enable Collaborative and Innovative Practices?* (PhD dissertation, Université de Strasbourg, 2022).

²⁴ CSA Teddy Lesmana, Eva Elis, and Siti Hamimah, "Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia," *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 3, no. 2 (2021): 5.

²⁵ Rama Dhianty, "Kebijakan privasi (privacy policy) dan peraturan perundang-undangan sektoral platform digital vis a vis kebocoran data pribadi," *Scripta: Jurnal Kebijakan Publik Dan Hukum* 2, no. 1 (2022): 190.

²⁶ Anne Adams, and Martina Angela Sasse, "Privacy in Multimedia Communications: Protecting Users, Not Just Data," In *People and Computers XV—Interaction without Frontiers: Joint Proceedings of HCI 2001 and IHM 2001*, (London: Springer London, 2001), 56.

²⁷ Mohd Javaid, Abid Haleem, Ravi Pratap Singh, and Anil Kumar Sinha, "Digital Economy to Improve the Culture of Industry 4.0: A Study on Features, Implementation and Challenges," *Green Technologies and Sustainability* 2, no. 2 (2024): 1083.

infrastructure. Digital platforms integrate software, networks, operations, and processes into complex systems that enable modern economic activities. With the rise of Industry 4.0 in the early twenty-first century, digital technologies began reshaping production and organizational models, creating interconnected systems that utilize data to support intelligent physical operations and transform entire industries. This transformation influences all sectors, regardless of whether individual firms directly adopt digital tools, making it evident that economic activity as a whole is increasingly part of the digital sphere. By enhancing efficiency, disrupting conventional business practices, and enabling technological breakthroughs, digitalization has far-reaching implications for present and future human development.²⁸ Moreover, the digital revolution creates opportunities to monitor sustainability, optimize resource use, reduce emissions, and foster circular economic practices, thereby opening global avenues for trade and innovation. Central to this process is the flow of data through the Internet, which sustains modern digital commerce, from the provision of non-physical products such as cloud services and video streaming to continuous global operations and flexible digital payment systems. As technologies advance, they will continue to generate new business models and innovative goods and services.²⁹

The evolution of the Internet has deeply influenced daily life, particularly in relation to personal data security.³⁰ Its origins can be traced to the late 1960s, when the ARPANET project was developed by the U.S. Department of Defense, though at that time, data protection was not yet a primary concern. With the commercial expansion of the Internet in the 1990s through the World Wide Web, online business activities grew rapidly but were accompanied by new threats such as viruses, malware, and data breaches.³¹ Entering the early 2000s, the rise of e-commerce increased the demand for secure transactions, leading to the adoption of encryption technologies like SSL, while cyberattacks such as phishing and hacking also became widespread. The popularity of social media in the 2000s to 2010s encouraged users to share personal information online, creating new risks of identity theft and

²⁸ Safira Widya Attidhira, and Yana Sukma Permana, "Review of Personal Data Protection Legal Regulations in Indonesia," *Awang Long Law Review* 5, no. 1 (2022): 289.

²⁹ Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga, "Optimizing personal data protection in Indonesia: Lesson learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (2020): 99.

³⁰ 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, no. 1 (2024): 15.

³¹ Lothar Determann, "Adequacy of data protection in the USA: myths and facts," *International Data Privacy Law* 6, no. 3 (2016): 248.

cybercrime.³² Growing awareness of these threats in the 2010s led to the establishment of data protection regulations, including Indonesia's Electronic Information and Transactions Law. Today, the emergence of advanced technologies such as artificial intelligence and the Internet of Things brings both innovation and new vulnerabilities, including deepfakes, AI-driven scams, and IoT-based attacks, compelling technology companies to continually develop stronger security measures.³³

The protection of personal data on the Internet has developed gradually through various technological innovations.³⁴ One of the earliest breakthroughs was data encryption, which secures information by converting it into coded form, readable only with the appropriate decryption key.³⁵ Encryption technologies such as SSL and TLS have since become standard for safeguarding sensitive communications and financial transactions online. To enhance security, Multi-Factor Authentication (MFA) was introduced, requiring verification through multiple credentials such as passwords, devices, or biometrics. Organizations also implemented Identity and Access Management (IAM) systems to control digital identities, manage user privileges, and track access. More recently, Artificial Intelligence (AI) and Machine Learning (ML) have been applied to detect anomalies and respond to threats in real time, serving as effective tools for preventing cyberattacks and protecting personal data.³⁶

The growing reliance on the Internet also exposes personal data to various risks.³⁷ Identity theft remains one of the most serious threats, as criminals can misuse stolen personal details to commit fraud or financial crimes.³⁸ Phishing schemes further exploit users by impersonating trusted entities through fake emails, messages, or websites designed to extract

³² Yohanes Leonardus Ngompat, and Mary Grace Megumi Maran, "Legal Development And Urgency Of Personal Data Protection In Indonesia," *JILPR Journal Indonesia Law and Policy Review* 5, no. 3 (2024): 629.

³³ Andi Rifky Maulana Efendy, "Towards enhanced personal data protection: A novel approach to regulation and practice in Indonesia," *E-Justice: Journal of Law and Technology* 1, no. 1 (2024): 15.

³⁴ Endang Lestari, and Rasji Rasji, "Legal study on personal data protection based on Indonesian legislation," *Awang Long Law Review* 6, no. 2 (2024): 478.

³⁵ Loso Judijanto, Nuryati Solapari, and Irman Putra, "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia," *The Easta Journal Law and Human Rights* 3, no. 01 (2024): 24.

³⁶ VIDA, "Perkembangan Internet Terhadap Keamanan Data Pribadi," *VIDA*. Retrieved in July 19, 2025 from <https://vida.id/id/blog/perkembangan-internet#:~:text=6.%20Era%20Teknologi%20Canggih%20dan,yang%20dapat%20menangka l%20serangan%20tersebut>.

³⁷ Sinta Dewi Rosadi, Andreas Noviandika, Robert Walters, and Firsta Rahadatul Aisy, "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?," *International Review of Law, Computers & Technology* 37, no. 1 (2023): 84.

³⁸ Raphael Gellert, and Serge Gutwirth, "The legal construction of privacy and data protection," *Computer Law & Security Review* 29, no. 5 (2013): 529.

sensitive information.³⁹ In addition, hacking and malware attacks compromise systems by secretly installing malicious software, often leading to data theft, system damage, or ransomware incidents. Less visible but equally concerning is tracking and data collection, where websites and applications harvest user information to build profiles often sold to third parties. Finally, corporate data breaches pose another danger, as insufficient safeguards in companies can result in leaked personal information, leaving users vulnerable to misuse.⁴⁰ The evolution of Internet security, from encryption to AI, has strengthened personal data protection. Yet, safeguarding sensitive information still requires joint efforts from users, providers, and regulators beyond technological solutions.

3. Protection of Privacy Rights in the Use of Digital Technology

Privacy needs to be protected because it is directly related to individuals' security, freedom, and self-esteem. Protecting privacy means giving individuals control over their personal information and protecting them from potential misuse that can be detrimental, such as identity fraud, defamation, and financial losses. In addition, privacy allows a person to maintain their integrity, living without worrying that their actions and personal information are constantly being monitored or freely accessed by others.⁴¹

Several cases highlight the privacy risks posed by digital technology. The Cambridge Analytica scandal revealed the misuse of millions of Facebook users' data for political campaigns such as the 2016 U.S. election. Similarly, Edward Snowden disclosed the U.S. government's extensive surveillance of private communications, including emails, phone calls, and online activity. In Indonesia, a comparable issue occurred in 2020 when Tokopedia suffered a massive data breach, exposing the personal information of millions of users. These cases highlight the ongoing risks to personal data in the digital era.⁴²

These incidents underline how easily personal data as part of the right to privacy can be compromised through technology. In today's world, data is often described as the "new oil," with users routinely sharing details like

³⁹ Octo Iskandar, "Analisis Kejahatan Online Phishing Pada Masyarakat," *Leuser: Jurnal Hukum Nusantara* 1, no. 2 (2024): 35.

⁴⁰ Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Harald Sundmaeker, Markus Eisenhauer, Klaus Moessner, Franck Le Gall, and Philippe Cousin, "Internet of Things Strategic Research and Innovation Agenda," In *Internet of things*, (Denmark: River Publishers, 2022), 153.

⁴¹ Alessandro Acquisti, Laura Brandimarte, and George Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science* 347, no. 6221 (2015): 511. See too, Herman T. Tavani, and James H. Moor, "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies," *ACM Sigcas Computers and Society* 31, no. 1 (2001): 9.

⁴² Jim Isaak, and Mina J. Hanna, "User data privacy: Facebook, Cambridge Analytica, and privacy protection," *Computer* 51, no. 8 (2018): 57. See too, Shoshana Zuboff, "Big Other: Surveillance Capitalism and the prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 79.

names, phone numbers, addresses, and emails. Such information, when misused by irresponsible actors, can lead to scams and other violations. To address this, governments have pushed for data protection measures, though many remain broad in scope. In Indonesia, for example, the Ministry of Communication and Informatics issued Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems, which has been in force since December 2016.⁴³ The issuance of Regulation Number 20 of 2016 later paved the way for Law Number 27 of 2022 on Personal Data Protection (PDP Law). Still, safeguarding data also begins at the individual level. Simple practices, such as enabling two-step verification, using backup codes, and monitoring email alerts, strengthen account security. Likewise, cultivating the habit of verifying information helps reduce the risk of hoaxes and fraud.

Personal data, as part of individual privacy, must be protected to prevent misuse, fraud, defamation, and online harassment, while ensuring control remains with its owner.⁴⁴ Because of its sensitivity, both awareness and responsibility are required to keep information secure. Users can take practical steps such as managing passwords wisely, separating emails for different purposes, staying alert to digital fraud, limiting oversharing, and maintaining vigilance, as digital footprints often outlast their owners.⁴⁵

William Prosser pioneered the framework of privacy lawsuits in the United States, giving legal recognition to claims that had previously lacked clear standing. However, his skepticism toward privacy and his belief that it lacked conceptual coherence restricted its growth in the context of the Information Age. He narrowed the scope of privacy law into four categories: intrusion into personal solitude, public disclosure of private facts, portraying someone in a false light, and misusing another person's likeness for personal gain.⁴⁶

It has been mentioned above that the right to privacy is implicitly contained and protected as part of the protection of human rights by Article 28G paragraph (1) of the 1945 Constitution, which states that everyone has the right to protection of themselves, their family, their honor, their dignity and their property rights. The article's formulation goes hand in hand with the protection of the rights of privacy formulated in Article 12 of the Universal

⁴³ KOMINFO, "Pentingnya Pelindungan Data Pribadi di Era Digital," *KOMINFO*. Retrieved in July 23, 2025 from <https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital/>.

⁴⁴ Muhammad Fikri, and Shelvi Rusdiana, "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Positif Indonesia," *Ganesha Law Review* 5, no. 1 (2023): 45.

⁴⁵ Ovidiu Vermesan, Peter Friess, Patrick Guillemin, Harald Sundmaeker, Markus Eisenhauer, Klaus Moessner, Franck Le Gall, and Philippe Cousin, "Internet of Things Strategic Research and Innovation Agenda," In *Internet of things*, (Denmark: River Publishers, 2022), 154.

⁴⁶ Daniel J. Solove, & Neil M. Richards, "Prosser's Privacy Law: A Mixed Legacy," *California Law Review* 98, no. 31 (2010): 1898.

Declaration of Human Rights (UDHR), which was then adopted in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Meanwhile, in the Decision of the Constitutional Court Number 50/PUU-VI/2008 on the Case of Judicial Review of Law Number 11 of 2008 on Electronic Information and Transactions, the Constitutional Court provides a translation of Article 12 UDHR and Article 17 ICCPR. In this translation, “privacy” is “personal/personal matters,” as stated in Article 28G 1945 Constitution.

In the digital age, privacy has become a major issue.⁴⁷ While digital technologies can drive innovation and support human rights, data-driven tools like artificial intelligence also enable governments and companies to monitor, predict, and influence human behavior on an unprecedented scale. Without proper safeguards, such advances pose serious threats to privacy, autonomy, dignity, and fundamental rights.⁴⁸

Across the globe, rapid technological progress is transforming lives and strengthening economies, yet the same tools often expose individuals to unprecedented risks of surveillance, profiling, and control.⁴⁹ Protecting the right to privacy enshrined in Article 12 of the Universal Declaration of Human Rights, Article 17 of the ICCPR, and other international frameworks is crucial in addressing these emerging digital threats, as personal data lies at the core of today’s interconnected societies.⁵⁰

In response, the OHCHR has held expert consultations and issued reports mandated by the UN General Assembly and Human Rights Council. One such report, prepared under Human Rights Council resolution 48/4, outlines current challenges to privacy, focusing on the misuse of invasive hacking technologies, the essential role of encryption in safeguarding rights, and the expansion of surveillance in public spaces. It warns that unchecked practices risk establishing systems of pervasive monitoring and control, ultimately undermining democratic and rights-based societies.⁵¹

Concerns over large-scale surveillance remain pressing, especially with the ongoing interception of online communications that affect vast segments of the population. Although some governments have introduced stricter

⁴⁷ I. Wayan Cenik Ardika, “Tinjauan hukum terhadap perlindungan data pribadi di era digital: Kasus kebocoran data pengguna layanan e-commerce,” *Indonesian Journal of Law and Justice* 2, no. 3 (2025): 11.

⁴⁸ Andri Pranata, Agustinus Arif Juono, and Aullia Vivi Yulianigrum Binarida, “Implementasi Asas Kehati-Hatian dalam Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi di Era Digital 5.0,” *Journal of Law and Nation* 3, no. 3 (2024): 725.

⁴⁹ Cindy Gladys Pratiwi Sianturi, Roida Nababan, and Ria Juliana Siregar, “Peran Hukum Dalam Melindungi Data Pribadi,” *Innovative: Journal Of Social Science Research* 4, no. 5 (2024): 2622.

⁵⁰ Fachriza Cakrafaksi Limuris, “Hak rakyat atas air bersih sebagai derivasi hak asasi manusia dalam deklarasi universal hak asasi manusia,” *Jentera: Jurnal Hukum* 4, no. 2 (2021): 524.

⁵¹ OHCHR, “Privacy in the Digital Age,” OHCHR. Retrieved in July 23, 2025 from <https://www.ohchr.org/en/privacy-in-the-digital-age>.

oversight, the practice of monitoring entire communities has not disappeared. In many countries, surveillance cameras are now a routine presence in streets, parking areas, transport terminals, and other public spaces. By 2021, their global number was projected to surpass one billion, with the most heavily monitored cities operating between 39 and 115 cameras per 1,000 residents. Such systems often disproportionately target marginalized groups, and the integration of artificial intelligence, particularly facial recognition, has amplified risks of racial or ethnic profiling. Predictive policing technologies have also been shown to reinforce patterns of discrimination.

Beyond discrimination, surveillance generates chilling effects on civil liberties, particularly freedom of expression and assembly. Empirical studies show that many writers (ranging from 34 to 61 percent depending on the country) deliberately avoided sensitive topics out of fear of being monitored. Similarly, a Norwegian survey revealed that nearly 40 percent of respondents refrained from using certain words or phrases online due to concerns over police surveillance.⁵²

Surveillance has become woven into daily life, from walking past street cameras to swiping access cards or browsing online. With advanced databases and monitoring technologies, institutions track individuals across personal and professional spaces.⁵³ Once associated primarily with policing or intelligence work, surveillance is now a routine aspect of modern existence. The concept of surveillance as social sorting highlights that its impact goes beyond curtailing individual freedoms. More critically, it functions as a mechanism that classifies people, verifies identities, evaluates risks, and assigns value, thereby reinforcing social divisions.⁵⁴ This process raises pressing ethical and political concerns over how such categories are established and applied. By examining case studies from North America and Europe, *Surveillance as Social Sorting* provides a novel lens on the relationship between surveillance practices, technology, and society, making it a significant reference for diverse academic fields.⁵⁵ However, it is understood that surveillance is carried out to protect people's rights, including their human rights. However, this protection actually

⁵² OHCHR, "Privacy in the Digital Age," *OHCHR*. Retrieved in July 23, 2025 from <https://www.ohchr.org/en/privacy-in-the-digital-age>.

⁵³ Rama Dhianty, "Kebijakan privasi (privacy policy) dan peraturan perundang-undangan sektoral platform digital vis a vis kebocoran data pribadi," *Scripta: Jurnal Kebijakan Publik Dan Hukum* 2, no. 1 (2022): 190.

⁵⁴ Giovanni Halbert, Shelvi Rusdiana, and Rufinus Hotmaulana Hutauruk, "Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia," *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat* 9, no. 3 (2023): 313.

⁵⁵ D. Lyon, "Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination," *Digital Media Ethics Journal*, 29, no. 2, (2003): 347.

causes a violation of privacy, which, in the discussion above, has been described as part of human rights.

In Indonesia, the right to privacy in the digital sphere is primarily safeguarded through Law Number 27 of 2022 on Personal Data Protection, which regulates personal data rights, obligations, and sanctions for violations.⁵⁶ Complementing this, Law Number 11 of 2008, as amended by Law Number 19 of 2016 on Electronic Information and Transactions, prohibits unauthorized access to electronic data. Further reinforcement is provided under the National Criminal Code (Law Number 1 of 2023), which affirms privacy protection as part of human rights within the scope of criminal law.⁵⁷

In this case, criminal law holds a paradoxical relationship with human rights. On the one hand, it serves as a tool for “human rights protection,” acting as a shield to safeguard rights by preventing abuses of power and ensuring justice within the legal system. On the other hand, it functions as a “duty to put criminal law in action,” acting as a sword that enforces the law against those who threaten human rights. Substantive criminal law protects human rights by preventing power misuse, while procedural criminal law protects rights throughout investigation, prosecution, trial, and sentencing. Moreover, criminal law acts preventively by deterring human rights violations and providing justice to victims by punishing perpetrators.⁵⁸ In this context, sometimes, criminal law approves the use of measures that can violate human rights, such as the discussion about surveillance above. On the other hand, criminal law is necessary to protect owners’ privacy. As in the cases of mobile phone sweeping, which are told in the Introduction section of this article,

Criminal law holds a paradoxical relationship with human rights. On the one hand, it serves as a tool for “human rights protection,” acting as a shield to safeguard rights by preventing abuses of power and ensuring justice within the legal system. On the other hand, it functions as a “duty to put criminal law in action,” acting as a sword that enforces the law against those who threaten human rights. Substantive criminal law protects human rights by preventing power misuse, while procedural criminal law protects rights throughout investigation, prosecution, trial, and sentencing. Moreover, criminal law acts preventively by deterring human rights violations and providing justice to victims by punishing perpetrators.

⁵⁶ Elfian Fauzy, and Nabila Alif Radika Shandy, “Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi,” *Lex Renaissance* 7, no. 3 (2022): 453.

⁵⁷ Gina Sabrina, and Fazal Akmal Musyarri, “Urgensi Penerapan Pidana Pengawasan Dalam Undang-Undang Nomor 1 Tahun 2023 Tentang KUHP,” *Jurnal Yudisial* 16, no. 1 (2023): 74.

⁵⁸ Topo Santoso, *Hukum Pidana: Tameng atau Pedang bagi HAM* (Public Lecture for the 10th Anniversary of Prof. Topo Santoso and Closing Meeting of TERAPI HAM, Depok: Universitas Indonesia, 2024).

To align with the challenges of privacy protection in the digital era, the reconstruction of Indonesian criminal law is essential. This includes integrating mandatory encryption requirements into Law Number 11/2008 on Electronic Information and Transactions (UU ITE), as amended, to enhance penal reforms.⁵⁹ Such measures would mandate secure data transmission in digital platforms, imposing stricter sanctions for non-compliance, thereby balancing surveillance needs with individual autonomy and preventing unauthorized access, ultimately fortifying privacy as a fundamental right amid technological advancements.⁶⁰

D. CONCLUSION

Legal protection for consumers and intellectual property rights holders in connection with the transformation of trade to e-commerce has been adopted with the expansion of the meaning of "trading place" in the Constitutional Court Decision dated February 29, 2024, No. 84/PUU-XXI/2023. Although the expansion of meaning was originally only in copyright protection, namely by improving the formulation of Article 10 and Article 114 of the Copyright Law, it should also apply to the protection of other intellectual property rights, including trademark protection. The state has the most significant and essential role in protecting copyrights and trademarks on online transaction activities. In practice, it is still necessary to collaborate well among the parties involved, whether the government, business actors, the community, or consumers, especially if the state neglects its responsibility to protect the rights outlined in the law. If the state fails to provide protection, then other parties (business actors, the community, and consumers themselves) can take over to take necessary actions. Protection of intellectual property and consumer rights in online transactions, particularly related to the protection of copyright and trademark in online transactions, essentially because Indonesia is a state of law and the protection given to achieve social justice.

⁵⁹ Jeremy Samuel Pangkey Sondakh, "Pemberlakuan Ketentuan Pidana Dalam Pasal 27 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *Lex Privatum* 9, no. 5 (2021): 24.

⁶⁰ Jim Isaak, and Mina J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer* 51, no. 8 (2018): 58. See too, Shoshana Zuboff, "Big other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 75.

BIBLIOGRAPHY

Book:

- Adams, Anne, and Martina Angela Sasse. "Privacy in Multimedia Communications: Protecting Users, Not Just Data." In *People and Computers XV—Interaction without Frontiers: Joint Proceedings of HCI 2001 and IHM 2001*, pp. 49-64. London: Springer London, 2001.
- Muhaimin. *Metode Penelitian Hukum*. Mataram: Mataram University Press, 2020.
- Mukti Fajar, N. D., and Yulianto Achmad. *Dualisme Penelitian Hukum Normatif & Empiris*. Yogyakarta: Pustaka Pelajar, 2013.
- Vermesan, Ovidiu, Peter Friess, Patrick Guillemin, Harald Sundmaeker, Markus Eisenhauer, Klaus Moessner, Franck Le Gall, and Philippe Cousin. "Internet of Things Strategic Research and Innovation Agenda." In *Internet of Things*, 7–151. Denmark: River Publishers, 2022.

Dissertation:

- Antonczak, Laurent. *Creativity on the Move: How Can Mobile Technology Enable Collaborative and Innovative Practices?* PhD dissertation., Université de Strasbourg, 2022.

Journal:

- Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. "Privacy and human behavior in the age of information." *Science* 347, no. 6221 (2015): 509-514.
- Ahmad, Nehaluddin. "Data privacy issues and risks with sharing on social media: An inquiry." *Russian Law Journal* 11, no. 4 (2023): 597-611.
- Ardika, I. Wayan Cenik. "Tinjauan hukum terhadap perlindungan data pribadi di era digital: Kasus kebocoran data pengguna layanan e-commerce." *Indonesian Journal of Law and Justice* 2, no. 3 (2025): 11-11.
- Attidhira, Safira Widya, and Yana Sukma Permana. "Review of Personal Data Protection Legal Regulations in Indonesia." *Awang Long Law Review* 5, no. 1 (2022): 280-294.
- Barth, Susanne, and Menno DT De Jong. "The Privacy Paradox—Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior—A Systematic Literature Review." *Telematics and informatics* 34, no. 7 (2017): 1038-1058.
- Determann, Lothar. "Adequacy of data protection in the USA: myths and facts." *International Data Privacy Law* 6, no. 3 (2016): 244-250.

- Dhianty, Rama. "Kebijakan privasi (privacy policy) dan peraturan perundang-undangan sektoral platform digital vis a vis kebocoran data pribadi." *Scripta: Jurnal Kebijakan Publik Dan Hukum* 2, no. 1 (2022): 186-199.
- Efendy, Andi Rifky Maulana. "Towards enhanced personal data protection: A novel approach to regulation and practice in Indonesia." *E-Justice: Journal of Law and Technology* 1, no. 1 (2024): 1-15.
- Fauzy, Elfian, and Nabila Alif Radika Shandy. "Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi." *Lex Renaissance* 7, no. 3 (2022): 445-461.
- Fikri, Muhammad, and Shelvi Rusdiana. "Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia." *Ganesha Law Review* 5, no. 1 (2023): 39-57.
- Gellert, Raphael, and Serge Gutwirth. "The legal construction of privacy and data protection." *Computer Law & Security Review* 29, no. 5 (2013): 522-530.
- Halbert, Giovanni, Shelvi Rusdiana, and Rufinus Hotmaulana Hutauruk. "Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia." *Jurnal Hukum To-Ra: Hukum Untuk Mengatur Dan Melindungi Masyarakat* 9, no. 3 (2023): 304-321.
- Isaak, Jim, and Mina J. Hanna. "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection." *Computer* 51, no. 8 (2018): 56-59.
- Iskandar, Octo. "Analisis Kejahatan Online Phishing Pada Masyarakat." *Leuser: Jurnal Hukum Nusantara* 1, no. 2 (2024): 32-36.
- Javid, Mohd, Abid Haleem, Ravi Pratap Singh, and Anil Kumar Sinha. "Digital Economy to Improve the Culture of Industry 4.0: A Study on Features, Implementation, and Challenges." *Green Technologies and Sustainability* 2, no. 2 (2024): 1083-1098.
- Judijanto, Loso, Nuryati Solapari, and Irman Putra. "An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia." *The Easta Journal Law and Human Rights* 3, no. 01 (2024): 20-29.
- Lesmana, CSA Teddy, Eva Elis, and Siti Hamimah. "Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia." *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia* 3, no. 2 (2021): 1-6.
- Lestari, Endang, and Rasji Rasji. "Legal study on personal data protection based on Indonesian legislation." *Awang Long Law Review* 6, no. 2 (2024): 471-477.

- Limuris, Fachriza Cakrafaksi. "Hak rakyat atas air bersih sebagai derivasi hak asasi manusia dalam deklarasi universal hak asasi manusia." *Jentera: Jurnal Hukum* 4, no. 2 (2021): 515-532.
- Lyon, D. "Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination". *Digital Media Ethics Journal*, 29, no. 2, (2003): 345-356.
- Ngompat, Yohanes Leonardus, and Mary Grace Megumi Maran. "Legal Development And Urgency Of Personal Data Protection In Indonesia." *JILPR Journal Indonesia Law and Policy Review* 5, no. 3 (2024): 627-635.
- Pranata, Andri, Agustinus Arif Juono, and Aullia Vivi Yulianigrum Binarida. "Implementasi Asas Kehati-Hatian dalam Perlindungan Data Pribadi Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi di Era Digital 5.0." *Journal of Law And Nation* 3, no. 3 (2024): 721-730.
- Purnama, Thiara Dewi, and Abdurrahman Alhakim. "Pentingnya Uu Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia." *Jurnal Komunitas Yustisia* 4, no. 3 (2021): 1056-1064.
- Rosadi, Sinta Dewi, Andreas Novindika, Robert Walters, and Firsta Rahadatul Aisy. "Indonesia's personal data protection bill, 2020: does it meet the needs of the new digital economy?." *International Review of Law, Computers & Technology* 37, no. 1 (2023): 78-90.
- Rumbold, Benedict, and James Wilson. "Privacy rights and public information." *Journal of Political Philosophy* 27, no. 1 (2019): 3-25.
- Sabrina, Gina, and Fazal Akmal Musyarri. "Urgensi Penerapan Pidana Pengawasan Dalam Undang-Undang Nomor 1 Tahun 2023 Tentang KUHP." *Jurnal Yudisial* 16, no. 1 (2023): 65-82.
- Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga. "Optimizing personal data protection in Indonesia: Lesson learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (2020): 95-109.
- 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, no. 1 (2024): 1-20.
- Sianturi, Cindy Gladys Pratiwi, Roida Nababan, and Ria Juliana Siregar. "Peran Hukum Dalam Melindungi Data Pribadi." *Innovative: Journal of Social Science Research* 4, no. 5 (2024): 2607-2624.
- Smith, H. Jeff, Tamara Dinev, and Heng Xu. "Information Privacy Research: An Interdisciplinary Review." *MIS Quarterly* 5, no. 4 (2011): 989-1015.
- Solove, D. J. "A Taxonomy of Privacy". *University of Pennsylvania Law Review* 154, no. 3, (2006): 354-368.
- Solove, D. J. "I've Got Nothing to Hide and Other Misunderstandings of Privacy". *San Diego Law Review* 44, no. 4, (2007): 569-578.

- Solove, Daniel J. dan Neil M. Richards. "Prosser's Privacy Law: A Mixed Legacy". *California Law Review* 98, no. 31 (2010): 1887-1923.
- Sondakh, Jeremy Samuel Pangkey. "Pemberlakuan Ketentuan Pidana Dalam Pasal 27 Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Lex Privatum* 9, no. 5 (2021): 10-31.
- Suari, Kadek Rima Anggen, and I. Made Sarjana. "Menjaga privasi di era digital: Perlindungan data pribadi di Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (2023): 132-142.
- Tavani, Herman T., and James H. Moor. "Privacy Protection, Control of Information, and Privacy-Enhancing Technologies." *ACM Sigcas Computers and Society* 31, no. 1 (2001): 6-11.
- Warren, S. D., & Brandeis, L. D. "The Right to Privacy". *Harvard Law Review* 4, No. 5, (1890): 847-857.
- Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30, no. 1 (2015): 75-89.

Public Lecture:

- Topo Santoso. Hukum Pidana: Tameng atau Pedang bagi HAM. Delivered Santoso, Topo. *Hukum Pidana: Tameng atau Pedang bagi HAM*. Public Lecture for the 10th Anniversary of Prof. Topo Santoso and Closing and Reflection Meeting of TERAPI HAM, Universitas Indonesia, Depok, 2024.

Website:

- Heru. "Random, Propam Polres PALI Razia Hp Anggota Sore Jelang Pulang Dinas, Sweeping Aplikasi Judi Online dan Pinjo". *Sumateraekspres.id*. Retrieved in July 23, 2025 from <https://sumateraekspres.bacakoran.co/read/48956/random-propam-polres-pali-razia-hp-anggota-sore-jelang-pulang-dinas-sweeping-aplikasi-judi-online-dan-pinjo>.
- KOMINFO. "Pentingnya Pelindungan Data Pribadi di Era Digital". *KOMINFO*. Retrieved in July 23, 2025 from <https://aptika.kominfo.go.id/2021/10/pentingnya-pelindungan-data-pribadi-di-era-digital/>.
- Nirkomala. "SMAN 2 Mataram Sidak Handphone Siswa Antisipasi Konten Judi Online". *Antara News Mataram*. Retrieved in July 23, 2025 from <https://mataram.antaranews.com/berita/358458/sman-2-mataram-sidak-handphone-siswa-antisipasi-konten-judi-online>.
- OHCHR. "Privacy in the Digital Age". OHCHR. Retrieved in July 23, 2025 from <https://www.ohchr.org/en/privacy-in-the-digital-age>.

- Poerwoto, Yohanes Liesty. "VIRAL Video Guru Mengecek HP Siswanya saat Ujian dan Diduga Langgar Privasi, Ini Klarifikasinya". *TRIBUNNEWS.COM*. Retrieved in July 23, 2025 from https://www.tribunnews.com/regional/2022/03/16/viral-video-guru-mengecek-hp-siswanya-saat-ujian-dan-diduga-langgar-privasi-ini-klarifikasinya#google_vignette.
- Safitri, Kiki dan Ihsanuddin. "Nasib Taruna Akpol Usai Dipecat karena Lawan Pengasuhnya". *Kompas.com*, Retrieved in July 23, 2025 from <https://nasional.kompas.com/read/2024/09/10/12163971/nasib-taruna-akpol-usai-dipecat-karena-lawan-pengasuhnya>.
- Saputra, Arry Dwi. "Cleaning Service di Surabaya Digerebek Polisi Saat Bermain Judi Online di Warkop". *JPNN.com*, Retrieved in July 29, 2025 from <https://jatim.jpnn.com/kriminal/30772/cleaning-service-di-surabaya-digerebek-polisi-saat-bermain-judi-online-di-warkop>.
- U.S. Department of Commerce. "Privacy Laws, Policies and Guidance." *Office of Privacy and Open Government*. Retrieved in July 23, 2025 from <https://www.commerce.gov/opog/privacy/privacy-laws-policies-and-guidance#:~:text=The%20Privacy%20Act%20of%201974,retrieved%20by%20a%20personal%20identifier>
- University of Medan Area. "Data Privacy in the Digital Age: Challenges and Solutions". *University of Medan Area*. Retrieved in July 29, 2025 from <https://baraka.uma.ac.id/privasi-data-dalam-era-digital-tantangan-dan-solusi/>.
- VIDA. "Perkembangan Internet Terhadap Keamanan Data Pribadi". *VIDA*. Retrieved in July 19, 2025 from <https://vida.id/id/blog/perkembangan-internet#:~:text=6.%20Era%20Teknologi%20Canggih%20dan,yang%20dapat%20menangkal%20serangan%20tersebut>.
- Widiyana, Esti. "Pastikan Siswa Tak Gabung Gangster, Guru Diminta Rutin Cek HP Siswa". *Detik.com*, Retrieved in July 19, 2025 from <https://www.detik.com/jatim/berita/d-6446825/pastikan-siswa-tak-gabung-gangster-guru-diminta-rutin-cek-hp-siswa>.