Jurnal Komunikasi
Vol. 3 No. 2 2025, hal. 264-276 e-ISSN: 2988-1331

SURVEILLANCE AND IMPLICATIONS OF WIRETAPPING IN INTERNATIONAL AND NATIONAL LAW: A COMPARATIVE STUDY OF ARRANGEMENTS AND PRACTICES

Gunawan Widjaja
Faculty of Law Universitas 17 Agustus 1945 Jakarta, Indonesia
widjaja_gunawan@yahoo.com

Adrian Bima Putra
Faculty of Law Universitas 17 Agustus 1945 Jakarta

Abstract

This research addresses the surveillance and implications of wiretapping in the perspective of international and national law through a comparative study of regulation and practice, with a focus on the cases of Indonesia and Australia. Wiretapping is an important instrument in law enforcement and state security, but at the same time has the potential to violate human rights, particularly the right to privacy. At the international level, wiretapping is regulated through various human rights instruments such as the UDHR, ICCPR, and the Vienna Convention, which emphasise the protection of privacy and the principle of non-intervention, while leaving room for exceptions for serious crimes. At the national level, Indonesia faces challenges of regulatory fragmentation, weak oversight, and the absence of a specific law that comprehensively regulates wiretapping. The case study of Australia's wiretapping of Indonesia shows that the practice of wiretapping without adequate oversight can damage diplomatic relations and reduce trust between countries. This research recommends harmonising national regulations with international standards, establishing a comprehensive wiretapping law, and strengthening independent oversight institutions to ensure lawful, proportionate and accountable wiretapping practices, while protecting human rights and maintaining stable international relations.
Keywords: wiretapping, surveillance, international law, national law, human rights, privacy, international relations, Indonesia, Australia.

Abstrak

Penelitian ini membahas pengawasan dan implikasi penyadapan dalam perspektif hukum internasional dan nasional melalui studi perbandingan pengaturan dan praktik, dengan fokus pada kasus Indonesia dan Australia. Penyadapan merupakan instrumen penting dalam penegakan hukum dan keamanan negara, namun pada saat yang sama berpotensi melanggar hak asasi manusia, khususnya hak atas privasi. Di tingkat internasional, penyadapan diatur melalui berbagai instrumen HAM seperti UDHR, ICCPR, dan Konvensi Wina, yang menegaskan perlindungan privasi dan prinsip non-intervensi, meskipun tetap membuka ruang pengecualian untuk kejahatan berat. Di tingkat nasional, Indonesia menghadapi tantangan berupa fragmentasi regulasi, lemahnya pengawasan, dan belum adanya undang-undang khusus yang secara komprehensif mengatur penyadapan. Studi kasus penyadapan Australia terhadap

Indonesia menunjukkan bahwa praktik penyadapan tanpa pengawasan yang memadai dapat merusak hubungan diplomatik dan menurunkan kepercayaan antarnegara. Penelitian ini merekomendasikan harmonisasi regulasi nasional dengan standar internasional, pembentukan undang-undang penyadapan yang komprehensif, serta penguatan lembaga pengawas independen untuk memastikan pelaksanaan penyadapan yang sah, proporsional, dan akuntabel, sekaligus melindungi hak asasi manusia dan menjaga stabilitas hubungan internasional.
Kata kunci: penyadapan, pengawasan, hukum internasional, hukum nasional, hak asasi manusia, privasi, hubungan internasional, Indonesia, Australia

Introduction

Wiretapping as a practice of secretly gathering information has become a central issue in international relations, especially when it involves sovereign states. This phenomenon has come under increasing scrutiny due to advances in communication technology that facilitate access to personal data and important conversations of state officials. One of the most prominent cases is the Australian wiretapping scandal against Indonesia in the 2007-2009 period, which was revealed to the public in 2013 through the leak of classified documents by Edward Snowden, a former US NSA contractor (Sinta Dewi Rosadi ., 2020)

The scandal revealed that a number of high-ranking Indonesian officials, including President Susilo Bambang Yudhoyono, his wife Kristiani Herawati, Vice President Boediono, as well as several ministers and other key officials were targeted for wiretapping by Australia's Defence Signals Directorate (DSD). These actions were carried out with the aim of obtaining strategic information that could be used for Australia's political and security interests, including in the context of international meetings such as the G20 Summit in London and the UN Climate Change Conference in Bali (Andrew Roberts, 2023) .

The revelation of these wiretapping practices caused strong reactions from the Indonesian government and society. Many considered that Australia's actions had violated the code of ethics in international relations and the principles of state sovereignty. The Indonesian people responded with various protests, including demonstrations in front of the Australian Embassy in Jakarta, as well as calls for the government to take firm diplomatic steps (Paul Schwartz, 2021) .

The Indonesian government immediately took action, one of which was to recall the Indonesian Ambassador to Australia as a form of protest and evaluation of the bilateral cooperation that had been established, especially in the military sector and intelligence exchange. Foreign Minister Marty Natalegawa also took diplomatic steps by requesting an official explanation from the Australian government and reviewing all forms of ongoing cooperation (Jukka Lohse & Jari Viitanen, 2020) .

This wiretapping case not only impacts the diplomatic relations between the two countries, but also raises fundamental questions about the boundaries of the legality of

wiretapping in international and national law. In the context of international law, the act of wiretapping by one state against another state's officials can be categorised as a violation of the principle of non-intervention and the norms of diplomacy stipulated in the 1961 Vienna Convention. However, the practice of wiretapping is often regarded as "normal" in the intelligence world, creating ambiguity in the enforcement of international law and ethics (Anna Johnston, 2022) .

On the other hand, Australia seeks to justify its actions on the grounds of the need to gather information to safeguard national security and strategic interests. However, this argument does not necessarily eliminate the negative impact on trust and stability of bilateral relations, especially when the actions are publicly exposed and cause uproar in the target country. In some statements, Australian officials have stated that the wiretapping was done to assist an ally and not to cause harm, but this remains unacceptable to Indonesia, which feels its sovereignty has been violated (Marko Milanovic, 2022) .

The impact of the wiretapping scandal is far-reaching, not only limited to the realm of politics and diplomacy, but also touching aspects of law, security and human rights. Wiretapping of high-ranking state officials can jeopardise national security, undermine public trust, and worsen the international image of the perpetrator country in the eyes of the world. In addition, this case also shows the weakness of monitoring mechanisms and protection of the privacy of state officials in the midst of the rapid development of communication technology (Lee, 2022) .

In the national context, Indonesia faces great challenges in strengthening regulations and supervision of wiretapping practices, both by state apparatus and foreign parties. Fragmentation of regulations in various laws makes law enforcement against wiretapping cases suboptimal. This prompts the need for regulatory harmonisation and the establishment of an independent oversight institution capable of ensuring that wiretapping practices are in accordance with legal principles and the protection of human rights (Daniel J. Solove, 2023) .

The Australian wiretapping case against Indonesia is also an important momentum for the two countries to review cooperation mechanisms in the field of intelligence and security. Evaluating bilateral agreements and strengthening diplomacy are strategic steps to prevent the recurrence of similar incidents in the future. In addition, openness and transparency in communication between countries are the main keys in building trust and maintaining the stability of international relations (David Gray, 2022) .

Globally, this wiretapping scandal adds to a long list of similar cases involving major countries such as the United States, the United Kingdom and Germany. This phenomenon shows that wiretapping is not an issue limited to one or two countries, but has become a common challenge in the era of globalisation and digitalisation of information. Therefore, collective efforts at the international level are needed to

formulate clear norms and standards regarding the boundaries of wiretapping, privacy protection, and dispute resolution mechanisms between countries (Stency Mariya Mark, 2024) .

This research will discuss in depth the surveillance and implications of wiretapping in the perspective of international and national law, taking a case study of the Australia-Indonesia wiretapping scandal. The analysis will focus on a comparison of legal arrangements in the two countries, the impact of wiretapping practices on bilateral relations, and policy recommendations to strengthen the protection of human rights and state sovereignty in the digital era.

By understanding the complexities and dynamics of wiretapping in the context of international and national law, it is hoped that this research can make a real contribution to the development of more comprehensive and effective regulations. In addition, this research also aims to raise awareness of the importance of protecting privacy and human rights amid increasingly complex global security challenges.

Finally, this research is expected to be an important reference for policy makers, academics and legal practitioners in formulating strategic steps to address the issue of cross-border wiretapping. Thus, a balance is created between the needs of national security and the protection of the fundamental rights of citizens and state officials in a just and civilised legal order.

Research Methods

This research uses a normative juridical method with a *comparative approach*, which focuses on analysing primary legal materials such as international treaties (UDHR 1948, ICCPR 1966), Indonesian national regulations (UU ITE, UU Telekomunikasi), and Australian law (Telecommunications Act 1979). Secondary data includes legal journals, reports from human rights organisations (Privacy International), and expert doctrine related to the principles of *lawful interception* and proportionality. Qualitative analysis was conducted on Australia-Indonesia wiretapping cases to identify regulatory gaps and impacts on human rights, with verification techniques through triangulation of legal sources and court decisions (Rothstein et al., 2006) .

Results and Discussion

Wiretapping Arrangements in International and National Law

Wiretapping is strictly regulated in international law through instruments such as the Universal Declaration of Human Rights (UDHR) 1948 and the International Covenant on Civil and Political Rights (ICCPR) 1966, which guarantee the right to privacy as part of human rights. The 1961 Vienna Convention also prohibits wiretapping of diplomatic representatives, emphasising the principle of non-intervention in international relations. However, exceptions are allowed for serious crimes such as

genocide, terrorism, or crimes against humanity under the 1998 Rome Statute, subject to proportionality and urgent necessity (Fadli, 2022) .

At the national level, Indonesia has regulations spread across 16 laws, including the ITE Law (Article 31), Telecommunications Law (Article 40), and KPK Law, which authorise wiretapping for law enforcement purposes with a judge's permission. The Draft Criminal Procedure Code (RKUHAP) tightens this mechanism by requiring written requests from investigators and prosecutors, except in emergencies such as national security threats. However, this fragmentation of rules creates risks of abuse of power and inconsistencies in practice (Maria Tzanou, 2021b) .

Australia, through the Telecommunications (Interception and Access) Act 1979, limits wiretapping to intelligence and national security purposes, with strict oversight by an independent body. This difference in approach was seen in the case of Australia's wiretapping of Indonesia (2013), which was deemed a breach of the diplomatic code of conduct although not categorised as an international criminal offence. Indonesia responded with diplomatic measures, including the recall of its ambassador and an evaluation of bilateral cooperation (Christopher Slobogin ., 2021)

The legal implications of wiretapping include violations of privacy rights and potential damage to international relations. Wiretapping without a clear legal basis can damage public trust and the image of the perpetrating state. In Indonesia, the absence of a specific law on wiretapping makes oversight mechanisms weak, so the ICJR recommends the establishment of a Wiretapping Bill to unify the scattered rules (Maria Tzanou, 2021a) .

International law recognises lawful interception as a form of legal wiretapping, but with strict conditions: (1) national security purposes, (2) court approval, and (3) time restrictions. In Indonesia, its implementation still faces technical challenges, such as the lack of trained human resources and adequate infrastructure. Privacy International's report emphasises the importance of transparency and accountability in the use of wiretapping technology (Muhammad Evan Aryasuta ., 2024)

A comparison with Germany shows that the country has a Federal Constitutional Court that actively cancels unconstitutional wiretapping regulations, while Indonesia does not have a similar institution. In fact, Constitutional Court Decision No. 5/PUU-VIII/2010 has mandated the establishment of a Wiretapping Law to protect privacy rights (Ladito R. Bagaskoro, 2023) .

Thus, harmonisation of wiretapping regulations is required at both the national and international levels. Indonesia needs to adopt a human rights-based model of independent oversight, while multilateral diplomacy should be strengthened to formulate ethical standards for inter-state tapping. Without these steps, the practice of wiretapping risks becoming a repressive tool that compromises individual human rights and state sovereignty.

The Impact of Wiretapping on Human Rights and Interstate Relations

Wiretapping potentially violates the right to privacy as part of human rights guaranteed by international instruments such as Article 12 of the Universal Declaration of Human Rights (UDHR) 1948 and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) 1966. These activities cause psychological discomfort, threaten individual dignity, and reduce citizens' sense of security, especially when conducted without a clear legal basis. In Indonesia, the ITE Law and Telecommunications Law authorise wiretapping for law enforcement, but regulatory fragmentation risks creating loopholes for abuse of power (Jawahir Thontowi ., 2020)

In the international context, the case of Australia's wiretapping of Indonesia (2013) is a clear example of the political-diplomatic impact. This action was deemed to violate the principle of non-intervention in the 1961 Vienna Convention, although it was not categorised as an international criminal offence. The Indonesian government responded by temporarily withdrawing its Ambassador from Canberra and evaluating military and intelligence cooperation, demonstrating how this practice undermines bilateral trust (Tim Lindsey, 2024) .

The impact of human rights is not only limited to individuals, but also extends to national security. Wiretapping of high-ranking state officials, such as the President and ministers, can leak strategic information that jeopardises sovereignty. On the other hand, weak oversight at the national level - such as the absence of a specific law on wiretapping in Indonesia - exacerbates the risk of privacy violations. In fact, Constitutional Court Decision No. 5/PUU-VIII/2010 has mandated the establishment of specific regulations to ensure proportionality (Laura K. Donohue, 2023) .

Diplomacy is a key instrument in resolving cross-border wiretapping disputes. Following the 2013 scandal, Indonesia and Australia developed a joint code of conduct to prevent a recurrence of similar incidents, although Australia refused to formally apologise . This approach shows that wiretapping is more often resolved through political channels than international law, given the complexity of proof and the sensitivity of bilateral relations (Fiona de Londras ., 2024)

Wiretapping has also fuelled a global discourse on the balance between security and privacy. Organisations such as Privacy International emphasise the importance of transparency and accountability in the use of wiretapping technology to prevent the state from acting arbitrarily. In Germany, the constitutional court has actively overturned unconstitutional wiretapping regulations, while Indonesia is still grappling with a fragmented legal framework (Anggara ., 2020)

As such, wiretapping creates a dilemma between security needs and human rights protection. Harmonising national regulations - such as the passing of the Wiretapping Bill - and strengthening independent oversight mechanisms are critical solutions to mitigate the negative impacts. Meanwhile, proactive diplomacy and the

establishment of international norms remain necessary to maintain stable relations between countries in the digital era.

An Ideal Wiretap Monitoring Model

Wiretapping as a law enforcement instrument requires an oversight model that integrates human rights compliance, institutional accountability and operational effectiveness. First, the legal framework should be clear and centralised, replacing the regulatory fragmentation that exists in Indonesia. A specific Wiretapping Law needs to be passed to establish the legitimate purpose (such as the prevention of terrorism or corruption), the procedure for applying for a licence, and time and scope limitations. This instrument should align with international standards such as the ICCPR and the 2001 Budapest Convention on cybercrime, while ensuring the principles of proportionality and *necessity* underpin every action (Institute for Criminal Justice Reform (ICJR), 2021) .

Second, an independent oversight body outside the executive structure must be established to prevent conflicts of interest. Such a commission - similar to the *Independent Commissioner's Office* in Hong Kong - should have full authority to audit applications for licences, monitor implementation and evaluate the results of wiretapping. Its membership should include human rights experts, civil society representatives and technology experts to ensure objectivity. This mechanism can reduce the risk of abuse of power by intelligence or law enforcement agencies (Rahman, 2021) .

Third, court approval is an absolute requirement for any wiretapping, except in emergencies that threaten life or national security. Specialised courts - such as the *Foreign Intelligence Surveillance Court* in the US - should be established with judges competent in technology and human rights. Applications for permission must be accompanied by detailed *probable cause*, including identification of the target, duration, and specific reasons why other methods are inadequate. In emergencies, wiretapping may be conducted without prior authorisation, but must be reported to the court within 24 hours for verification (David Gray, 2022) .

Fourth, strict time limits are needed to prevent wiretapping from becoming a tool of mass surveillance. The maximum wiretap authorisation is valid for 30 days, with the option to extend once upon re-evaluation. Data obtained outside this period or irrelevant to the investigation must be automatically destroyed by the system, accompanied by a certification of deletion from the supervisory agency. This mechanism prevents the indiscriminate storage of data that could potentially be misused for political purposes (Graham Greenleaf, 2020) .

Fifth, the security of intercepted data must be guaranteed through encryption protocols and *access log* systems. Data should only be stored on isolated servers with access limited to investigators directly working on the case. Any opening or transfer of data must be digitally recorded, enabling tracking in the event of a leak.

Telecommunications service providers are also required to implement *end-to-end encryption* for dedicated wiretap channels, preventing hacking by unauthorised parties (Peter Parycek ., 2022)

Sixth, regular audits by independent oversight bodies are key to accountability. A minimum of 20% of wiretapping cases should be randomly audited each month, including an examination of licence documents, recorded communications, and compliance with the original purpose. Audit results are reported to parliament and the public in redacted form-without divulging sensitive information-to ensure transparency. Any breaches of procedure found should be dealt with firmly, ranging from administrative to criminal sanctions (Shlomi Dolev et al., 2021) .

Seventh, public complaint mechanisms need to be accessible easily and quickly. People who feel they are victims of illegal wiretapping can report to the Ombudsman or a specialised human rights court. Reports must be verified within 14 working days, with fines for false reporters to prevent abuse of the system. If proven valid, the oversight body should recommend compensation and restoration of the victim's good name.

Eighth, human resource capacity building cannot be ignored (Joseph A. Cannataci, 2020) . Wiretap operators are required to undergo annual training on professional ethics, human rights law, and technological developments. Certification of technical competence-such as the use of ISO-standardised wiretapping equipment-is a prerequisite for reducing operational errors. Violations of the code of conduct, such as unauthorised wiretapping, should result in licence revocation and criminal prosecution (Bivitri Susanti, 2021) .

Ninth, limited transparency is needed to build public trust. Annual reports detailing wiretapping statistics-number of requests, approvals, and denials-should be published, even with redactions that do not reveal active intelligence operations. This documentation helps the public assess the agency's performance while encouraging improved regulation (Lalu Wira Pria Suhartana ., 2023)

Tenth, international cooperation should be regulated through bilateral or multilateral agreements. The Australia-Indonesia wiretapping case (2013) shows the need for explicit agreements prohibiting the wiretapping of strategic officials. *Mutual Legal Assistance* (MLA) mechanisms need to be strengthened to ensure that cross-border wiretapping is only carried out for serious crimes, with the written consent of the relevant country (Mosgan Situmorang ., 2021)

Eleventh, standardisation of wiretapping technology by a neutral institution such as Kominfo is a must. The tools used must be certified and tested regularly to prevent data manipulation. The prohibition of the use of illegal *spyware* (e.g. Pegasus) must be followed by severe criminal sanctions, both for producers and users (Agnieszka Grzelak, 2025) .

Twelfth, the separation of authority between institutions prevents overlapping authority. Polri may only wiretap for general crimes, KPK for corruption, and BIN for foreign intelligence. Data exchange between agencies requires written permission from the court, ensuring the *need-to-know* principle is maintained (Mirna et al., 2023) .

Thirteenth, a constitutional review by the Constitutional Court every five years is needed to adapt the Wiretapping Law to the times. This process involves academics, human rights NGOs, and legal practitioners, with Constitutional Court Decision No. 5/PUU-VIII/2010 on privacy protection as the main reference (Jonathon W. Penney, 2022).

Finally, proportional sanctions should be applied to violators. Abuse of wiretapping authority is subject to a criminal penalty of 5-15 years in prison and a fine of up to Rp10 billion. Officials proven to have leaked wiretap data for personal or political gain must be sacked and barred from holding public office. This model creates a system that respects human rights without compromising national security, while addressing the complexity of challenges in the digital era (Ika Riswanti Putranti et al., 2023) .

Thus, wiretapping is an important instrument in law enforcement and state security, but its implementation must be within clear legal corridors and uphold human rights, especially the right to privacy. At the international level, wiretapping is strictly regulated through various human rights instruments such as the UDHR and ICCPR, as well as the principles of non-intervention in the Vienna Convention, although in practice there are still gaps and ambiguities, especially in the context of transnational crime and global security. At the national level, Indonesia faces challenges in the form of regulatory fragmentation, weak oversight, and the absence of a specific law that comprehensively regulates wiretapping, potentially leading to abuse of power and human rights violations.

The Australian wiretapping case against Indonesia clearly demonstrates the serious impact of wiretapping on relations between countries, ranging from diplomatic rifts, loss of trust, to disruption of strategic cooperation. In addition, wiretapping conducted without strict oversight mechanisms can threaten the privacy rights of citizens and public officials, as well as reduce the legitimacy of the state in the eyes of the public and the international community. Therefore, the ideal wiretapping oversight should prioritise the principles of legality, proportionality, accountability and transparency, by involving independent oversight institutions, court approval mechanisms, periodic audits and strict sanctions for violations.

Harmonisation of national regulations with international standards is absolutely necessary, both through the enactment of a comprehensive wiretapping law and the strengthening of cross-agency monitoring mechanisms. In addition, international cooperation and diplomacy must continue to be promoted to prevent the misuse of wiretapping that can damage the order of relations between countries. Thus,

wiretapping can remain an effective law enforcement tool without compromising fundamental rights and state sovereignty.

Conclusion

Wiretapping is basically prohibited in international and national law because it potentially violates the right to privacy guaranteed in various human rights instruments such as UDHR 1948, ICCPR 1966, and Vienna Convention 1961, as well as in the Indonesian constitution and laws. However, there are expressly regulated exceptions, where wiretapping is allowed in certain circumstances that threaten state order and security, such as in the handling of criminal acts of terrorism, corruption, narcotics, and transnational crimes, provided that it is carried out by authorised institutions and follows clear and strict legal procedures.

In practice, supervision of wiretapping in Indonesia still faces challenges due to regulatory fragmentation and the absence of a special law that regulates wiretapping mechanisms and procedures in an integrated manner. This has the potential to lead to violations of privacy rights and abuse of authority by law enforcement officials. Therefore, the establishment of a comprehensive wiretapping law and the strengthening of independent oversight institutions are urgent needs to ensure that every wiretapping action takes place legally, proportionally and accountably.

At the level of interstate relations, wiretapping practices such as those between Australia and Indonesia are seen more as violations of the diplomatic code of ethics than international crimes, so their resolution tends to be pursued through diplomacy and negotiations. Thus, harmonising national wiretapping arrangements with international standards, as well as strengthening oversight mechanisms and protecting human rights, are key to preventing privacy violations and maintaining trust in international relations.

References

Agnieszka Grzelak. (2025). EU Criminal Law and Electronic Surveillance: The Pegasus System and the Legal Challenges It Poses. *European Journal of Law and Technology*, 1-18. https://doi.org/10.14311/EJLT.2025.02.01

Andrew Roberts. (2023). The Role of Courts in Surveillance Oversight: Comparative Insights. *Journal of Comparative Law*,*18* (2), 200-225. https://doi.org/10.1080/17441056.2023.2210458

Anggara. (2020). *Reorganising Wiretapping in the Criminal Justice System*. ICJR. https://icjr.or.id/wp-content/uploads/2021/07/Mengatur-Ulang-Penyadapan-dalam-Sistem-Peradilan-Pidana_Edisi-Revisi.pdf

Anna Johnston. (2022). The Impact of International Treaties on Domestic Surveillance Laws. *International Review of Law, Computers & Technology*,36 (2), 150-170. https://doi.org/10.1080/13600869.2022.2038476

Bivitri Susanti. (2021). Indonesia's Legal Framework for Electronic Surveillance: Challenges and Reform. *Indonesian Journal of International Law*,*19* (2), 201-220. https://doi.org/10.17304/ijil.vol19.2.2021.5

Christopher Slobogin. (2021). *Privacy, Due Process and the Competing Interests in Government Surveillance*. Oxford University Press. https://doi.org/10.1093/oso/9780190940816.001.0001

Daniel J. Solove. (2023). *Surveillance, Privacy and Public Trust*. Cambridge University Press. https://doi.org/10.1017/9781108762341

David Gray. (2022). Legal Frameworks for Governmental Surveillance: A Comparative Analysis. *International Journal of Law, Crime and Justice*,*70* , 101-112. https://doi.org/10.1016/j.ijlcj.2022.101812

Fadli. (2022). *Reconstruction of Wiretapping Authority Regulation in the Framework of Law Enforcement in Indonesia* [Sultan Agung Islamic University]. http://repository.unissula.ac.id/30936/1/10302000396.pdf

Fiona de Londras. (2024). National Security, Surveillance and Human Rights: A Comparative Study. *Human Rights Law Review*,*24* (1), 45-70. https://doi.org/10.1093/hrlr/ngad021

Graham Greenleaf. (2020). Cross-Border Data Interception and International Law. *International Data Privacy Law*,*10* (4), 299-312. https://doi.org/10.1093/idpl/ipaa013

Ika Riswanti Putranti, Marten Hanura, Safrida Alivia Sri Ananda, & Gawinda Nura Nabila. (2023). Cyber Resilience Revisited: Law and International Relations. *Journal of Law, Policy and Globalisation*, *126*, 98–110.

Institute for Criminal Justice Reform (ICJR). (2021). Reconciling the Legal Arrangement of Wiretapping in Indonesia. *ICJR Policy Brief.* https://icjr.or.id/mendamaikan-pengaturan-hukum-penyadapan-di-indonesia/

Jawahir Thontowi. (2020). Wiretapping in International Law and its Implications for National Law. *Ius Quia Iustum Law Journal*, *22*(2), 183–202.

Jonathon W. Penney. (2022). *Digital Surveillance and Privacy in the Global South*. MIT Press. https://doi.org/10.7551/mitpress/13834.001.0001

Joseph A. Cannataci. (2020). International Law and the Right to Privacy in the Digital Age. *Human Rights Law Review*,*20* (1), 1-25. https://doi.org/10.1093/hrlr/ngz043

Jukka Lohse & Jari Viitanen. (2020). The Intelligence Process in Finland: Legal Norms and Oversight. *Scandinavian Journal of Military Studies*,*3* (1), 19-35. https://doi.org/10.31374/sjms.55

Ladito R. Bagaskoro. (2023). *Development of Criminal Law in Indonesia*. PP OTODA. https://ppotoda.org/wp-content/uploads/2023/11/Ebook_PerkembanganHukumPidanadiIndonesia_organized.pdf

Lalu Wira Pria Suhartana. (2023). *International Law and Indonesia's National Interest*. University of Mataram.

https://eprints.unram.ac.id/24337/1/Hukum%20Internasional%20dan%20Kepentingan%20Nasional%20Indonesia.pdf

Laura K. Donohue. (2023). Oversight and Accountability in Surveillance: International Best Practices. *Law and Contemporary Problems*, *86*(1), 115–140.

Lee, S. (2022). The Influence of Social Media on Ethical Norms in Interpersonal Communication. *Media Ethics Review*, *15*(1), 67–83.

Maria Tzanou. (2021a). Privacy and Surveillance: Comparative Legal Approaches in the Digital Age. *Computer Law & Security Review*,*41* , 105567. https://doi.org/10.1016/j.clsr.2021.105567

Maria Tzanou. (2021b). Regulating State Surveillance: International Standards and National Implementation. *Computer Law & Security Review*,*41* , 105-120. https://doi.org/10.1016/j.clsr.2021.105567

Marko Milanovic. (2022). The European Court of Human Rights and Secret Surveillance. *European Journal of International Law*,*33* (3), 765-789. https://doi.org/10.1093/ejil/chac045

Mirna, D., Sandjojo, A., & Rumata, V. (2023). Enhancing Better Policies in Indonesia Cyber Security Management: Comparative Analysis of Lawful Interception. *Journal of Management and Public Services*, *12*(2), 123–137.

Mosgan Situmorang. (2021). Harmonisation of National Law in the Field of Corruption with the United Nations Convention Against Corruption. *RechtsVinding Journal*, *3*(3), 329–346.

Muhammad Evan Aryasuta. (2024). *Wiretapping Practices against Corruption Offenders in the Perspective of National and International Law* [UIN Syarif Hidayatullah Jakarta]. https://repository.uinjkt.ac.id/dspace/bitstream/123456789/78818/1/11190480000075_Muhammad%20Evan%20Aryasuta%20ILMU%20HUKUM.pdf

Paul Schwartz. (2021). The Regulation of Wiretapping and Electronic Surveillance in Europe and the United States. *Columbia Journal of Transnational Law*, *59*(2), 321–367.

Peter Parycek. (2022). *Lawful Interception: Privacy, Security and Surveillance*. Springer. https://doi.org/10.1007/978-3-030-85713-6

Rahman, A. (2021). Ethics and Responsibility in Social Media Use among Youth. *Youth & Society*, *53*(6), 1120–1135.

Rothstein, H. R., Sutton, A. J., & Borenstein, M. (2006). *Publication Bias in Meta-Analysis: Prevention, Assessment and Adjustments*. John Wiley & Sons.

Shlomi Dolev, Oded Margalit, Benny Pinkas, & Alexander Schwarzmann. (2021). Lawful Interception in WebRTC Peer-To-Peer Communication. *Cyber Security Cryptography and Machine Learning*, 153-170. https://doi.org/10.1007/978-3-030-78120-2_11

Sinta Dewi Rosadi. (2020). Wiretapping, Privacy, and Law: The Indonesian Experience. *Journal of Law & Development*,*50* (3), 321-340. https://doi.org/10.21143/jhp.vol50.no3.2020.321-340

Stency Mariya Mark. (2024). Shielding Privacy in the Surveillance Era: A Comparative Study of India, USA and South Africa. *Revista Direito, Estado e Tecnologia*,6 (2), 45-68. https://doi.org/10.26512/rdet.v6i2.51916

Tim Lindsey. (2024). Oversight Mechanisms for Surveillance in the Asia-Pacific: Lessons for Indonesia. *Asia-Pacific Law Review*,*32* (1), 55-80. https://doi.org/10.1080/10192557.2024.1001234