International Journal of Social Research and Development
www.socialsciencejournal.net
Online ISSN: 2664-8709, Print ISSN: 2664-8695
Received: 12-06-2025, Accepted: 13-07-2025, Published: 28-07-2025
Volume 7, Issue 2, 2025, Page No. 36-38

Constitutional law and surveillance of public officials: Blancing national interests, privacy, and accountability

Ninik Agustini, Ria Tri Vinata
Faculty of Law, Wijaya Kusuma Surabaya, University, Dukuh Kupang, Surabaya, Indonesia

Abstract
Cybercrime threatens individual security through unauthorized access to personal assets. It involves identity theft, data breaches (information resource theft), account hijacking, and the distribution of viruses embedded in files, websites, and critical codes. It may also encompass acts of defamation, slander, and reputational harm. Similarly, industrial espionage and the hostage-taking of critical information resources have become increasingly prevalent. These phenomena have caused public concern due to the erosion of privacy and the looming threat of asset loss and intellectual property theft. Personal data protection has become a crucial preventive measure in response to the growing threat to personal data security. This study used a normative juridical method to systematically and normatively explore and analyze the legal aspects of specific issues or topics. The method emphasizes an in-depth examination of legal norms derived from various sources, such as legislation, court decisions, and legal literature. Therefore, this study concludes that constitutional law is essential to solve cybercrime by regulating state authority, protecting constitutional rights, formulating legal frameworks, coordinating interagency, and safeguarding cyber sovereignty. Constitutional Law ensures that responses to cybercrime are carried out under the principles of the rule of law and democracy, while simultaneously protecting national interests and citizens' rights.

Keywords: Cybercrime, surveillance, constitutional law

Introduction
Information technology and electronic transactions have become essential in daily life, influencing sectors such as government and business. While they offer many advantages, they also have serious risks due to new forms of criminal activity, widely known as cybercrime, which threatens privacy, security, and public trust (Suhariyanto, 2013, p. 108) [7].

The fast growth of information and communication technology (ICT) is like a double-edged sword. It helps improve human life and progress, but it also makes it easier for people to conduct criminal activities through digital networks and online, known as cybercrime. These crimes are carried out through internet-based computer networks, where computer and communication systems are used as tools to get personal benefit at the expense of others. Cybercrime represents the dark side of technological progress, negatively impacting virtually every aspect of modern life (Arief, 2006, p. 1) [3].

Both cybercrime and cyber warfare pose significant threats to individual security, particularly through unauthorized access to personal assets. Prominent incidents include identity and data theft (targeting information resources), account hijacking, the distribution of viruses within the files and websites, manipulation of critical codes, slander, defamation, and character assassination. In addition, industrial espionage and the hostage taking of critical information resources are becoming increasingly common. These incidents have caused widespread public concern due to the loss of personal privacy and the growing risk of losing valuable assets and wealth.

Cyberspace may also be used as a political tool to disseminate fake news intended for political provocation or economic manipulation. The interconnected nature of the internet enables hostile actions aimed at disabling or destroying the resources of opposing nations without the need for physical proximity. This threat landscape must be taken seriously, as perpetrators may come from various backgrounds and collaborate despite differing agendas (Soewardi, 2013) [6].

Building on the points discussed earlier, the Indonesian government recognizes the urgent need to protect national and citizen interests in the digital space. In response, it has introduced several regulations, including Law No. 27 of 2022 on Personal Data Protection (PDP Law), which establishes a legal framework for storing, transferring, and using personal data in cyberspace. Indonesia's efforts to strengthen data protection and raise public awareness of cybersecurity play a crucial role in mitigating risks and ensuring the country's sustainable development of information technology (Kennedy, 2024) [4].

Beyond data theft and online fraud, unauthorized surveillance also constitutes a form of cybercrime especially when it violates established legal norms and human rights. Wiretapping conducted without proper legal authority or oversight may be deemed unconstitutional as it contravenes the principle of legality. Constitutional Law regulates the authority of state institutions, including those legally empowered to conduct surveillance activities—such as the police, public prosecutors, or intelligence agencies, as stipulated in Law No. 11 of 2008 on Electronic Information and Transactions and the Intelligence Law.

In addition to data theft and online fraud, unauthorized surveillance represents a serious form of cybercrime, particularly when it infringes upon established legal norms and fundamental human rights. Wiretapping used without proper legal authorization or oversight may be considered unconstitutional because it breaks the principle of legality. Constitutional Law governs the authority of state institutions, including those legally permitted to conduct surveillance, such as the police, public prosecutors, and intelligence agencies as outlined in Law No. 11 of 2008 on Electronic Information and Transactions and the Intelligence Law.

Therefore, examining the implications of information technology on constitutional law on cybersecurity and data privacy is important to ensure that legal frameworks remain responsive to the challenges brought by technological advancement. This study aims to examine the constitutional and regulatory foundations of surveillance, focusing specifically on the scope and limitations of state authority as outlined in Constitutional Law.

Method

This study adopts a normative juridical approach to systematically and normatively explore and analyze the legal aspects of a particular issue or topic. This method used examination of legal norms found in various sources, including statutes, court decisions, and legal literature (Kristiawanto, 2022) [5].

The normative legal approach is the primary method for investigating cybercrime in Indonesia, examining relevant legal norms through literature reviews and statutory analysis. This approach aims to provide an in-depth understanding of the legal framework for personal data protection, particularly the extent to which the constitution supports it. The analysis of personal data protection laws plays an important role in evaluating the substance of existing regulations. This study aims to identify whether these laws either align with or deviate from the constitutional principles that serve as the foundation for personal data protection (Sunggono, 2019) [9].

Discussion

Regulations on Surveillance in Cyberspace

Surveillance issues, whether at the national or international level, often involve distinct motives. However, the core objective remains the same: to obtain information about an individual without their knowledge. One of the most common motives is to collect evidence related to criminal acts. Nevertheless, this does not mean that any party can conduct surveillance on such grounds, as unauthorized surveillance may lead to public unrest and disrupt social order.

The issue of surveillance contributes to an atmosphere of discomfort and insecurity among citizens. It signals a loss of protection against arbitrary control, a threat to the right to privacy, and a violation of human dignity. These developments raise serious concerns about the erosion of constitutional rights.

As a sovereign nation, Indonesia is not immune to threats from cybercrime. One notable example was the surveillance conducted by Australia targeting Indonesian officials. The incident involved the wiretapping of then-President Susilo Bambang Yudhoyono, First Lady Ani Yudhoyono, and several senior government officials. The operation began with the Defense Signals Directorate (DSD), Australia's intelligence agency, collecting mobile phone numbers of high ranking Indonesian officials, particularly in the fields of defense, security, social affairs, politics, and economics. Initially, the only number obtained was that of Bali Police Chief, Inspector General Sutisna.

As a result, the surveillance network was expanded through Australian Embassy and Consulate General. In 2009, prior to Indonesia's presidential election, the DSD intercepted additional phone communications involving multiple Indonesian officials. This operation was later exposed by Edward Snowden, a former member of the U.S. National Security Agency (NSA), who also leaked classified documents involving intelligence practices by allied countries. These countries formed an intelligence alliance known as SIGINT or the "Five Eyes" (TEMPO, 2018) [10].

Australia neither confirmed nor denied the wiretapping activities when questioned by Indonesian authorities. This lack of response led then-President Yudhoyono to temporarily recall Indonesia's ambassador to Canberra until diplomatic relations were normalized. The relationship between Indonesia and Australia, a two Pacific neighbours with a long history of cooperation and trade had recently been in high tensions over several issues, including human rights, terrorism, and asylum seekers (The Guardian, 2013) [11].

Within Indonesia's Constitutional Law framework, surveillance activities must be regulated through a system of checks and balances, including judicial approval or parliamentary oversight. This mechanism is essential to prevent the abuse of executive power. Any violation of this oversight may render surveillance practices unconstitutional (Sumariyastuti, 2019) [8].

In the context of international law, particularly under international human rights instruments, surveillance is generally considered a prohibited act under several legal frameworks. Article 12 of the Universal Declaration of Human Rights (UDHR) 1948 states:

"N*o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honour and reputation. Everyone has the right to protection of the law against such interference attacks*."

This study emphasizes that no individual may be subjected to arbitrary interference in personal, family, home affairs, or their correspondence. Moreover, any attack on one's honor and reputation is prohibited. Every person is entitled to legal protection against such interference or assaults (Thontowi, 2015) [12].

The Relationship Between Constitutional Law and Cybercrime

Constitutional Law has an important connection with cybercrime. Although HTN mainly focuses on the structure, function, and relationships of state institutions, as well as the relationship between the state and its citizens, it also provides the legal foundation to deal with cyber threats. This includes protecting national security, defending citizens' rights, and creating laws that follow the principles of a democratic legal system. This connection can be seen in several ways, such as the government's role in protecting cybersecurity, upholding constitutional rights, supporting cooperation among institutions, and defending the country's digital sovereignty.

Cybercrime increases, including hacking critical infrastructure, stealing data, or spreading false information. Constitutional Law becomes more important in guiding how the state should respond legally and responsibly. One example is the cyberattack on Indonesia's National Data Center (NDC) in 2024, which showed the urgent need for strong, clear constitutional rules to protect national interests. The crucial point is the legal authority given to the state to ensure national security. Article 30(1) of the 1945 Constitution states that national defense and security are the responsibility of the Indonesian Armed Forces and the National Police. Cybercrimes like ransomware attacks or election system hacks threaten the country's stability. These crimes require quick and coordinated responses from institutions such as National Cyber and Crypto Agency (NCCA), the Ministry of Communication and Information (MCI), and the police.

Constitutional Law ensures that these powers are exercised in accordance with the division of responsibilities among institutions, preventing overlap and ensuring accountability through legislative oversight by the House of Representatives. Moreover, HTN provides the legal foundation for the formulation of policies and regulations, such as the Electronic Information and Transactions Law (ITE Law) and the Personal Data Protection Law (Law No. 27 of 2022), which are intended to address cybercrime while complying with the legislative procedures outlined in Article 20 of the 1945 Constitution.

Another important aspect of constitutional law regarding cybercrime is its role in protecting citizens' rights guaranteed by the 1945 Constitution. These rights include the right to privacy (Article 28G) and the freedom of expression (Article 28E(3)). Cybercrimes such as data theft, doxing, or unlawful surveillance often breaks these rights, imposing a constitutional obligation on the state to ensure protection. Constitutional law ensures that laws such as the Personal Data Protection Law protect against these crimes and follow democratic values and the rule of law, as mentioned in Article 1(3) of the Constitution. For example, voter data was leaked from the General Election Commission in 2023. This raised constitutional concerns about the state's responsibility in protecting citizens' data and how law enforcement can act without limiting other rights, such as the right to free expression. Constitutional law gives a legal guide to balance the protection of rights with the need for public safety.

The connection between constitutional law and cybercrime also extends to interagency coordination and the defense of cyber sovereignty. Constitutional law governs the relationships among the executive, legislative, and judicial branches and independent institutions such as the National Cyber and Crypto Agency. Fighting cybercrime requires well-defined collaboration among institutions such as the National Cyber and Crypto Agency for cyber threat prevention, the police for law enforcement, and the Ministry of Communication and Information for digital content regulation. Constitutional law ensures this cooperation works effectively, with each agency staying within its legal role.

On an international level, cybercrimes involving transnational actors such as hacking by foreign groups raise issues of cyber sovereignty. Article 11 of the 1945 Constitution, which governs foreign relations, provides the legal foundation for Indonesia to take diplomatic steps or cooperate under international legal frameworks, such as the *Budapest Convention on Cybercrime*, although Indonesia has not yet ratified it. Such cases highlight that constitutional law is relevant at the domestic level and plays an important role in the global context.

Therefore, Constitutional Law provides a foundational legal framework in response to cybercrime by regulating state authority, protecting citizens' rights, guiding legislation, enabling inter-agency coordination, and safeguarding cyber sovereignty. However, challenges such as the lack of specific cybersecurity legislation, overlapping institutional mandates, and the often ambiguous implementation of the ITE Law indicate the need to strengthen constitutional law - based legal framework.

The drafting of Cybersecurity and Cyber Resilience Law currently under deliberation in Indonesia is expected to clarify the roles of state institutions and enhance the national response to cyber threats, while remaining grounded in constitutional principles. Therefore, Constitutional Law is relevant and essential in ensuring that cybercrime is addressed effectively, democratically, and in accordance with the rule of law.

Conclusion

Constitutional Law is a branch of law that governs the structure of the state, the relationships between state institutions, and the relationship between the state and its citizens, all based on constitutional principles. Protecting personal data has become increasingly important in addressing the risks of data misuse, cyberattacks, and potential human rights violations. This concept is implemented through various national and international data protection laws to safeguard individuals' personal information from unauthorized access and misuse. Constitutional Law is closely connected to cybercrime through the regulation of state authority, the protection of constitutional rights, the formation of legal frameworks, interagency coordination, and the defense of cyber sovereignty. It ensures that the state's response to cybercrime adheres to the principles of the rule of law and democracy, while also protecting national interests and citizens' rights.

References

1. Abdumalikov G. Profound Importance of Cyber Security in the Field of Business. Int J Hum Comput Stud,2022:4(2):43–6.
2. Ajufo GK, Qutieshat A. An Examination of the Human Factors in Cybersecurity: Future Direction for Nigerian Banks. Indones J Inf Syst (IJIS),2023:6(1):1–16.
3. Arief BN. Tindak Pidana Mayantara Perkembangan Kajian Cyber crime di Indonesia. Jakarta: Rajawali Pres, 2006.
4. Kennedy A. Perlindungan Data Pribadi Dalam Dunia Siber Di Indonesia Ditinjau Berdasarkan Hukum Tata Negara. Hukum Din Ekselensia,2024:6(2):82–98.
5. Kristiawanto. Memahami Penelitian Hukum Normatif. Jakarta: Prenada, 2022.
6. Soewardi BA. Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. Media Inf Ditjen Pothan Kemhan, 2013, 31–5.
7. Suhariyanto B. Tindak Pidana Teknologi Informasi (Cyber crime) Urgensi Pengaturan dan Celah Hukumnya. Depok: Raja Grafindo Persada, 2013.
8. Sumariyastuti SHD. Penyadapan Dalam Perspektif Hak Asasi Manusia. Yurispruden,2019:2(2):135–53.
9. Sunggono B. Metodologi Penelitian Hukum. Depok: Rajawali Pers, 2019.
10. Tempo. Australia Has Been Spying on Indonesia Since 1950 [Internet], 2018. [cited 2025 May 14]. Available from: https://en.tempo.co/read/526400/australia-has-been-spying-on-indonesia-since-1950
11. The Guardian. Australia's spy agencies targeted Indonesian president's mobile phone [Internet], 2013. [cited 2025 May 14]. Available from: https://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone
12. Thontowi J. Penyadapan dalam Hukum Internasional dan Implikasinya terhadap Hubungan Diplomatik Indonesia dengan Australia. J Huk Ius Quia Iustum,2015:2(22):183–202.