Legal Framework Publication of State Secrets via Cyberspace in Indonesia

Yasir Adi Pratama

Universitas Brawijaya, Indonesia
E-mail: yasiradipratama@gmail.com

Abstract

The issue of publishing information and electronic data that fall under the category of state secrets via cyberspace remains unregulated in Indonesia, leading to a complex debate between the state's secrecy and the public's right to access information. This tension has been further intensified by the Fourth Industrial Revolution and the widespread availability of information, making it difficult to distinguish between state secrets and public information. As a result, individuals or entities who disseminate state secrets through cyberspace may not be held accountable unless specific regulations are established. This study adopts a normative juridical approach with a legal and conceptual framework to examine the intersection of state secrets and the publication of information through cyberspace, examining relevant provisions from existing laws and regulations. The study's findings may provide the legal vacuum concerning the criminalization of individuals who have published information or electronic information that may be categorized as state secrets through cyberspace.

A. Introduction

The current era of digitalization, with its transition to the fourth industrial revolution or the Internet of Things (IoT), demands that everything is connected to the internet or cyberspace. This includes the dissemination of information, which may potentially be categorized as state secrets. Advancements in information technology have revolutionized nearly every aspect of existence. On the one hand, computer technology offers the opportunity to access information, engage in work, participate in politics and democratic processes, and provides various other advantages. However, on the flip side, information technology has the potential to encroach upon the tangible real-life issues that society has been grappling with for an extended period. Netizens may perceive this as a challenge that needs to be addressed before it continues to...
evolve within the realms of cyberspace. Indonesia, as a sovereign state based on Article 28E paragraph (3) of the 1945 Constitution of the Republic of Indonesia, recognizes the right to freedom of expression and the right to obtain and disseminate information using all available channels, as stated in Article 28F of the same constitution.

The existence of cyber law is crucial in addressing cybercrime, particularly in the context of electronic information publication through cyberspace. In Indonesia, cyber law is regulated under the Electronic Information and Transactions Law (ITE Law). However, in its practical implementation, the UU ITE, which is intended to control and regulate to prevent cybercrime in the cyberspace realm, has fallen short. The 2008 ITE Law has not been able to effectively restrict the actions of individuals in their online interactions, especially when such actions originate from outside Indonesian territory. Additionally, key principles such as legal certainty, utility, prudence, and good faith, which were the intended objectives of ITE Law, remain unfulfilled.

To date, there is no specific regulation in the form of legislation that governs the categorization of information as state secrets in Indonesia. The draft state secrets bill is currently under consideration by the Indonesian House of Representatives. Therefore, it is possible for individuals or legal entities to publish information that may be categorized as state secrets without facing legal consequences, particularly if such publication occurs outside of Indonesia.

Unauthorized disclosure of state secrets, such as those made by the non-profit website Wikileaks created by Julian Assange, which operates without regard to national borders, constitutes a violation of state secrets. Wikileaks received information about corruption in the Kenyan government and leaked videos about the wars in Afghanistan and Iraq, as well as classified documents related to the United States military. The question arises as to whether Wikileaks publication of this information can be classified as the disclosure of state secrets of Kenya or the United States.

The classic argument for transparency in government is that the people have a right to know, as argued by Thomas Emerson. According to Dennis Thompson, the same argument can be made for state secrecy. Moreover, cyberspace is considered a neutral territory for all users, providing unrestricted freedom of expression beyond conventional geographical boundaries. Therefore, discussing the topic of state secrets being published through cyberspace in Indonesia is an interesting area of research. The problem formulation that can be deduced is as follows: (1) What is the regulatory framework governing state secrets in Indonesia? and (2) What are the legal consequences for individuals who disclose state secrets via cyberspace in Indonesia?

This research will use normative analytical descriptive research methods by reviewing regulations which governing state secrets in Indonesia. Data would be collected mainly from national legal instruments, as well as scholar books and journals. The novelty of this research

---

lies in the emphasize on state secrets which published online and legal consequences for individuals who disclose state secrets via cyberspace in Indonesia.

B. Discussion

1. Regulatory Framework Governing State Secrets in Indonesia

Indonesia, as a legal state governed by the principles set forth in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, also strives to maintain a delicate balance between the rights of the public (citizens) and those of the state (government), given its democratic nature. The specific regulation regarding state secrets has not been fulfilled to date due to the non-enactment of the State Secrets Bill in the Indonesian House of Representatives. This has resulted in uncertainty as to which information can be categorized as state secrets, particularly in the current era of IoT (the fourth industrial revolution) where it is highly likely that a vast amount of information is published in cyberspace. It is essential to emphasize that every individual is entitled to freedom of opinion and the right to access information.

The notion of freedom of expression and access to information contradicts the regulation regarding state secrets. Hence, the House of Representatives has not yet ratified the State Secrets Bill. This viewpoint is based on the assumption that a democratic government should not withhold information from its citizens, who are the rightful owners of the state. Between state secrets and transparency, sometimes secrets prevail, although there is a right to information and transparency. The information released upon request does not necessarily guarantee transparency or cooperation from the institution, as it is not automatically released but must be requested with the requisite knowledge.

Indonesia has issued Law No. 14 of 2008 on Public Information Disclosure (PID Law) in order to ensure the right of citizens to access information. With the enactment of the PI Law, the public can implement control mechanisms in responding to policies issued by the government in the implementation of state affairs. PID Law regarding information categorized as secrets is referred to as "exempted information" as stipulated in Article 2 (4) of PID Law, which states that:

"Exempted Information is categorized as secret in accordance with the Law, propriety, and public interest based on testing the consequences that arise if certain information is given to the public, and after carefully considering that withholding Public Information can protect greater interests than disclosing it or vice versa."

Based on the above article, it can be interpreted that information that can be categorized as secret must be regulated by law, propriety, and public interest that have been carefully considered.

The PID Law has further regulated in detail the types of exempted information from the obligation to be disclosed to the public in Article 17 of the PID Law, which consists of:

---

12 The enactment of Law Number 14 of 2008 on Public Information Disclosure was carried out during the Plenary Session of the House of Representatives on April 3, 2008.
“(a) Public information that, if disclosed, can hinder law enforcement processes; (b) Public information that, if disclosed, can interfere with the protection of intellectual property rights and protection against unfair competition; (c) Public information that, if disclosed, can endanger national defense and security; (d) Public information that, if disclosed, can reveal Indonesia’s natural wealth; (e) Public information that, if disclosed, can harm national economic resilience; (f) Public information that, if disclosed, can harm foreign relations; (g) Public information that, if disclosed, can reveal personal authentic deeds; (h) Public information that, if disclosed, can reveal personal secrets; (i) Memoranda or letters between public bodies that are confidential in nature except by decision of the Information Commission or court; and (j) Information that cannot be disclosed based on the law.”

In addition to the PID Law, Indonesia has issued other laws that categorize information as secret, namely the State Intelligence Law No. 17 of 2011 (State Intelligence Law) which regulates intelligence secrets, the Indonesian National Army Law No. 34 of 2004 (TNI Law) which regulates military secrets, the Banking Law No. 10 of 1998 amending Banking Law No. 7 of 1992 (Banking Law) which regulates bank secrets, and the Archives Law No. 43 of 2009 (Archives Law) which regulates closed archives.

The State Intelligence Law regulates intelligence secrets in Article 25 paragraph (1) which states that intelligence secrets are part of state secrets, and in detail regulated in Article 25 paragraph (2) which is mostly similar to the exempted information regulated in PID Law, only adding in the field of state intelligence. Because intelligence secrets are part of state secrets, indirectly information that can be classified as state secrets has been regulated in the State Intelligence Law.

In the TNI Law, which regulates military secrets, it is explained that military secrets are part of the TNI soldier’s oath to be held firmly even if the TNI soldier has been honorably or dishonorably discharged. The limits of military secrets are regulated in the Explanation of Article 35 of the TNI Law. The TNI Law does not explicitly explain that military secrets are part of state secrets, but if we look at the Explanation of Article 35 of the TNI Law, then military secrets are included in state secrets because they are the same as those regulated in Article 25 paragraph (2) letter a of the State Intelligence Law, namely all information that endangers national defense and security.

The Banking Law regulates bank secrets, which refers to all information related to customer information, deposits, and storage, and also requires banks to maintain the confidentiality of such information. Based on those provisions, bank secrets is applied only

---

14 According to Article 25 paragraph (2) of Law No. 17 of 2011 on State Intelligence, intelligence secrets are categorized as follows: (a) Endangering national defense and security; (b) Disclosing natural resources of Indonesia that are classified as confidential; (c) Harming national economic resilience; (d) Harming foreign policy interests and foreign relations; (e) Disclosing memoranda or letters that need to be kept confidential according to their nature; (f) Endangering the state intelligence system; (g) Endangering access, agents, and sources related to the implementation of intelligence functions; (h) Endangering the safety of state intelligence personnel; or (i) Disclosing plans and implementations related to the implementation of intelligence functions.

15 Article 35 Law No. 34 of 2004 on the Indonesian National Army (TNI Law).

16 Article 37 Law No. 34 of 2004 on the Indonesian National Army (TNI Law).

17 The military secret is everything related to military duties that if falls into unauthorized hands will harm the state in the defense sector.

18 Article 1 number 28 Law No. 10 of 1998 amending Law No. 7 of 1992 on Banking (Banking Law).

to and limited to information regarding depositors and their deposits. Therefore, any information unrelated to depositors and their deposits is not considered bank secrets.\(^{20}\)

The Archive Law regulates closed archives as stipulated in Article 44 of the Archive Law where the creator of the archive can restrict access to the archive for reasons provided for in paragraph (1) on those article.\(^{21}\) Based on the provisions of the Archive Law regarding closed archives, it is similar to exempted information as regulated in the PID Law, where the creator of the archive is obligated to maintain the confidentiality of the closed archive.\(^{22}\)

The above regulations regarding various secrets information can be concluded that although Indonesia does not yet have a specific law on state secrets, there are already various regulations that classify certain information as state secrets.

### 2. The Legal Consequences for Individuals Who Disclose State Secrets via Cyberspace in Indonesia

The advancement of information and communication technology (ICT) towards the era of IoT is inseparable from cyberspace. Cyberspace can be defined as the connection of various computer systems that can be accessed remotely, allowing for massive data exchange.\(^{23}\) Based on the Black Law Dictionary, cyberspace is “the realm where computer communications and simulations are used on the internet”. With this definition, it can be briefly interpreted as the internet world where various computers or other electronic devices are massively connected and can access the internet.

The development of cyberspace today allows many people to connect and access various information published in the world of the internet, not only through news websites, but also through social media. With the vast amount of information being published, it is possible that various information categorized as state secrets may still be published by individuals, whether they are journalists or individuals. The dissemination or spread of illegal information on the internet does not mean that it is a human right to communicate, as the internet is not only a communication medium between parties but also a global communication medium that can be accessed by all parties. Therefore, the internet is not a law-free medium, as it is subject to the law above its creators, users, and those who operate it as public infrastructure for communication and information, both nationally and globally.\(^{24}\)

The specific regulation on state secrets should have been implemented in Indonesia, considering the rapid development of cyberspace, to balance between state secrecy and public freedom to access information. There is a tension between the government's openness and its efforts to maintain national security, in which state secrets are used as a reason to achieve transparent governance.\(^{25}\) The existence of such regulations is expected to establish clear boundaries between information that can be categorized as state secrets and those that are not.

---


\(^{21}\) The reasons for opening archives to the public may include: a. impeding law enforcement processes; b. disrupting the protection of intellectual property rights and protection from unfair competition; c. endangering national defense and security; d. revealing Indonesia's natural resources that fall under protected secrecy; e. damaging national economic resilience; f. harming foreign policy interests and foreign relations; g. revealing authentic acts that are personal in nature; h. revealing personal secrets; and i. revealing memoranda or letters that require secrecy based on their nature.

\(^{22}\) Law No. 43 of 2009 on Archives Law.


Steven Aftergood has identified three clear boundaries for determining what can be considered a state secret: (1) genuine national security secrecy; (2) bureaucratic secrecy to avoid errors; and (3) political secrecy to avoid errors in policy.\textsuperscript{26} If state secrets are not clearly categorized, government activities will deviate from their intended purpose of protecting national security, but instead become a basis for a corrupt bureaucracy that ultimately undermines accountable government performance.\textsuperscript{27}

Although there is no specific regulation on state secrets in Indonesia, regulations on the crime of state secret information can be found in the Indonesian Criminal Code Book (KUHP) and other specific regulations such as the PID Law, State Intelligence Law, TNI Law, Banking Law, and Archives Law. The KUHP, which regulates the criminalization of state secret information related to national security, is stipulated in Articles 112 to 116 of the KUHP, as follows:

a. Article 112 of KUHP which stated that:

> “Whoever intentionally announces letters, news, or information that he knows must be kept confidential for the interests of the state, or intentionally informs or provides it to foreign countries, shall be punished with imprisonment for a maximum of seven years.”

Based on that article, individuals who publish letters, news, or information that is secret for national security purposes with the threat of imprisonment for a maximum of 7 (seven) years.

d. Article 113 of KUHP which stated that:

> “(1) Whoever intentionally discloses, informs or hands over to unauthorized persons documents, maps, plans, drawings or secret objects related to the defense or security of Indonesia against external attacks, in whole or in part, which are in their possession or of which they know the contents, forms or arrangements of the objects, shall be punished with imprisonment for a maximum of four years; (2) If the documents or objects are in the possession of the offender, or their knowledge of it is due to their search, the penalty may be increased by one-third.”

Based on that article, individuals who publish confidential letters, maps, plans, drawings, or objects related to Indonesia's defense or security against external attacks, with a maximum imprisonment penalty of 4 (four) years.

c. Article 114 of KUHP which stated that:

> “Whoever, due to their fault (negligence), causes secret documents or objects as referred to in Article 113 to become their duty to keep or place, and their form or arrangement or all or part of them are known to the public or are controlled or known by unauthorized persons, is subject to a maximum imprisonment of one year and six months or a maximum of one year of detention or a maximum fine of four thousand and five hundred Indonesian rupiahs.”

Based on that article, individuals who made dissemination of secret letters due to negligence, the maximum penalty is imprisonment for up to 1 year or detention for up to 1 year with a fine.


\textsuperscript{27} \textit{Loc. Cit}.
d. Article 115 of KUHP which stated that:

“Whoever sees or reads secret documents or objects as referred to in Article 113, in whole or in part, while it is known or reasonably suspected that the objects are not intended for him to know, as well as making or instructing the making of copies or summaries in any letters or language, making or instructing the making of models or images, or if not delivering the objects to judicial, police or government officials, in the event that the objects come into his possession, is threatened with imprisonment for a maximum of three years.”

Based on that article, individuals who acknowledge the contents of secret letters that should not be known, the maximum penalty is imprisonment for up to 3 years.

e. Article 116 of KUHP which stated that:

“Conspiracy to commit crimes as referred to in Articles 113 and 115 is punishable by imprisonment for a maximum of one year.”

Based on that article, individuals had conspiracy to commit a crime, the maximum penalty is imprisonment for up to 1 year.

The criminalization of information that can be categorized as state secrets is also regulated in Article 54 of the PID Law\(^28\) which regulates individuals who without authorization access and/or obtain and/or provide information that is secret with a threat of imprisonment for a maximum of 2 (two) years up to a maximum of 3 (three) years depending on the classification of the exempted information.

The State Intelligence Law also regulates the criminalization of intelligence secrets in Article 44\(^29\) which states that a person who intentionally steals, discloses or leaks state secrets is punishable by up to 10 (ten) years in prison, and Article 45\(^30\) which regulates the negligence of a person resulting in the leakage of state secrets with a maximum penalty of 7 (seven) years in prison. This applies not only to ordinary individuals or legal entities, but also to intelligence personnel, who face the same penalties\(^31\).

The Banking Law regulates the criminalization of bank secrecy in Article 47 paragraph (2) of the Banking Law\(^32\), which only applies to legal subjects such as members of the board of commissioners, directors, bank employees, or affiliated parties who disclose confidential

\(^28\) Article 54 of Law Number 14 of 2008 on Public Information Disclosure states that: “(1) Any person who intentionally and without right accesses and/or obtains and/or discloses information that is exempted as regulated in Article 17 letter a, letter b, letter d, letter f, letter g, letter h, letter i, and letter j shall be punished with a maximum imprisonment of 2 (two) years and a fine of up to Rp10,000,000.00 (ten million Indonesian Rupiah); (2) Any person who intentionally and without right accesses and/or obtains and/or discloses information that is exempted as regulated in Article 17 letter c and letter e, shall be punished with a maximum imprisonment of 3 (three) years and a fine of up to Rp20,000,000.00 (twenty million Rupiah).”

\(^29\) Article 44 of Law Number 17 of 2011 on State Intelligence regulates the punishment for the disclosure of intelligence secrets, which stipulates that any person who intentionally steals, discloses, and/or leaks Intelligence Secrets as referred to in Article 26 shall be punished with imprisonment for a maximum of 10 (ten) years and/or a maximum fine of Rp500,000,000 (five hundred million Rupiah).

\(^30\) Article 45 of Law Number 17 of 2011 on State Intelligence regulates the punishment for negligence resulting in the leakage of Intelligence Secrets, which stipulates that any person who, due to negligence, causes the leakage of Intelligence Secrets as referred to in Article 26 shall be punished with imprisonment for a maximum of 7 (seven) years and/or a maximum fine of Rp300,000,000 (three hundred million Rupiah).


\(^32\) Article 47 of Law Number 10 of 1998 on Amendment to Law No. 7 of 1992 on Banking states that: “Members of the Board of Commissioners, Board of Directors, bank employees, or other affiliated parties who intentionally disclose information that is required to be kept confidential under Article 40 shall be punished with imprisonment for at least 2 (two) years and a fine of at leastRp4,000,000,000.00 (four billion rupiah) and up to Rp8,000,000,000.00 (eight billion rupiah).”
information with a maximum penalty of 2 (two) years of imprisonment. The Archives Law also regulates the criminalization of closed archive secrecy in Article 85 of the Archives Law\textsuperscript{33}, which applies to individuals who fail to maintain the confidentiality of closed archives with a maximum penalty of 5 (five) years of imprisonment.

The existing legal regulations that govern the criminalization of information that can be categorized as state secrets have not specifically accommodated rules regarding the publication of state secrets through cyberspace. The provision in the KUHP that comes closest to the publication of state secrets is the act of announcing information from letters, news, or statements that should be kept confidential for the interests of the state. However, the drawback of this provision in the KUHP is that it does not address the situation where such information is in the form of electronic information that is published through cyberspace. Therefore, there is a need for more comprehensive legal provisions to address the issue of the publication of state secrets through cyberspace.

The Personal Data Protection Law (PDP Law)\textsuperscript{34}, the newly enacted regulation by the Indonesian government, there are penal provisions as stipulated in Article 67(2) of the PDP Law, which govern the prohibitions as set forth in Article 65(2) of the PDP Law. It states that “anyone who intentionally and unlawfully discloses personal data that does not belong to them shall be subject to a maximum imprisonment of 4 (four) years and/or a fine of up to IDR 4,000,000,000.00 (four billion Indonesian Rupiah)”. However, the PDP Law does not specifically regulate the criminalization of individuals who publish certain information or electronic information via cyberspace. It solely addresses the criminalization of individuals who disclose personal data that does not belong to them.

In the Electronic Information and Transactions Law (ITE Law), which is the country's main tool in combating cybercrime, there are provisions that regulate the punishment for electronic information that is categorized as secrets under Article 48 paragraph (3) of the ITE Law\textsuperscript{35}, which carries out criminal acts in accordance with Article 32 paragraph (3) of the ITE Law\textsuperscript{36} for acts that cause secrets electronic information to be accessed by the public. However, these provisions are limited to electronic information owned by others or by the public, and there are no provisions regarding electronic information that is categorized as state secrets and owned by a particular country, especially Indonesia.

The absence of specific regulations governing individuals responsible for the publication of information or electronic information that can be categorized as state secrets through cyberspace creates a legal vacuum regarding the criminalization of such individuals responsible for the publication of state secrets through cyberspace in Indonesia. Owing to the legal vacuum concerning the criminalization of individuals who have published information or electronic information that may be categorized as state secrets through cyberspace, such individuals cannot be subject to criminal prosecution or held accountable in the eyes of the law.

\textsuperscript{33} Article 85 of Law Number 43 of 2009 on Archives regulates the criminal sanctions against the secrecy of closed archives, which stipulates that: "Any person who intentionally fails to maintain the confidentiality of closed archives as referred to in Article 44 paragraph (2) shall be punished with imprisonment for up to 5 (five) years or a fine of up to Rp250,000,000.00 (two hundred and fifty million rupiah)."

\textsuperscript{34} Law Number 27 Year 2022 on Personal Data Protection.

\textsuperscript{35} Article 48 paragraph (3) of the Law Number 11 Year 2008 on Electronic Information and Transactions states that: "Anyone who fulfills the elements as referred to in Article 32 paragraph (3) shall be punished with imprisonment for a maximum of 10 (ten) years and/or a fine of up to Rp5,000,000,000.00 (five billion rupiah)."

\textsuperscript{36} Article 32 paragraph (3) of the Law Number 11 Year 2008 on Electronic Information and Transactions states that: "Any person who intentionally and without authority or unlawfully alters, adds, reduces, transmits, damages, deletes, moves, or hides someone else's or public electronic information and/or electronic documents in any way, which results in the disclosure of confidential electronic information and/or electronic documents that can be accessed by the public with data integrity that is not as it should be."
C. Conclusion

The regulations consisting of the PID Law, the State Intelligence Law, Banking Law, TNI Law, the Archives Law, and the KUHP which regulate various types of classified information can be concluded that although Indonesia has not yet had a specific law on state secrets, there are various regulations which categorize information as state secrets. However, the aforementioned regulations do not specifically accommodate rules regarding the publication of state secrets through cyberspace. The provision closest to the publication of state secrets in the KUHP is the announcement of information from letters, news, or statements that must be kept confidential for the sake of the state. Nevertheless, the shortcoming of this provision is that there is no provision if such information is in the form of electronic information that is published through cyberspace.

In ITE Law, which is the frontline of Indonesia in tackling cybercrimes through cyberspace, there is a provision that regulates criminal sanctions in Article 48 paragraph (3) ITE Law that is in accordance with Article 32 paragraph (3) ITE Law, for acts that cause the disclosure of electronic information classified as secret to be accessible to the public. However, this provision is limited to electronic information belonging to other individuals or the public and does not include electronic information containing state secrets held by a country, particularly Indonesia. The absence of the specific regulations governing individuals responsible for the publication of information or electronic information which can be categorized as state secrets through cyberspace results in a legal vacuum concerning the criminalization of such individuals responsible for the publication of state secrets through cyberspace in Indonesia. Owing to the legal vacuum concerning the criminalization of individuals who have published information or electronic information that may be categorized as state secrets through cyberspace, therefore such individuals cannot be subject to criminal prosecution or held accountable in the eyes of the law.

D. Suggestion

As a sovereign country over its territory, including cyberspace, Indonesia should have detailed boundaries regarding information that can be categorized as state secrets, especially electronic information in cyberspace. It is highly possible that state secrets can be disclosed by individuals or legal entities. Therefore, to achieve this, Indonesia requires specific regulations or laws that govern the publication of information or electronic information categorized as state secrets through cyberspace.

This legal framework for the protection of state secrets in cyberspace, including provisions for the criminalization of those who disclose state secrets through cyberspace. This legal framework should be comprehensive and encompass various laws and regulations related to national security, including the KUHP, PID Law, the State Intelligence Law, TNI Law, Banking Law, and Archives Law. It is also recommended that the government of Indonesia strengthens its efforts to raise awareness among the public about the importance of protecting state secrets in cyberspace. This could include educational campaigns, workshops, and training programs to help individuals and organizations understand the risks associated with cyber espionage and the importance of cybersecurity.
References

A. Book

B. Journal
C. Regulation

Constitution of the Republic of Indonesia Year 1945.

Law Number 1 Year 1946 concerning Criminal Law Regulations.

Law Number 10 Year 1998 concerning Amendments to Law Number 7 Year 1992 concerning Banking.

Law Number 34 Year 2004 concerning the Indonesian National Army.

Law Number 14 Year 2008 concerning Public Information Disclosure.

Law Number 11 Year 2008 concerning Electronic Information and Transactions.

Law Number 43 Year 2009 concerning Archives.

Law Number 17 Year 2011 concerning State Intelligence.