RULES OF GOVERNMENT SECRECY IN THE LAW OF ARCHIVES IN INDONESIA

Brian Amy Prastyo[1]

Abstract

Every government operates secrecy as one of mechanism to protect the state, the people, and the assets from threats. There is lack of clarity of rules for the secrecy system in Indonesia. Ultimately, there is no uniform conception among government officials, because each agency makes its own policy and system. This condition brings disadvantage to society, because there is no clear guidance on this subject and it will not be able to push the government to act more responsible in managing the information. The rules about "closed archives" in Law No. 43 of 2009 about Archives and the term of "security classification" that mentioned in Government Regulation No. 28 of 2012 about the Implementation of Law No. 43 of 2009 about Archives, do not help at all in solving that problems. To get the accountability in the management of closed archive, the government does not have any other option than establishing a set of rules that describe a clear secrecy system. The secrecy concept can be framed within the concept of records life cycle, in order to be more adjustable to the existing system.

Keywords: *information law, government secrecy, freedom of information, national archives, security classification*

I Introduction

Secrecy was used to be seen as individual matter. Later, this conception was applied also in organization. The rationale for the application of secrecy in organization, according to Fred H. Cate was because organization works almost similar to individual. He said, "organization like individuals, often require privacy for independence and integrity (organizational autonomy). Organizational autonomy includes the need for one organization to keep secrets from another".[2]

Generally, there are three basic elements in every secrecy system. First, every secrecy system at least consists of three primary actors, the one who own the information, the one who keep the information, and the one who does not have the authority to know the information. Second, every actor is tied with rights and responsibility. For example, the one who own the informa-

[1] Brian Amy Prastyo teaches cyberspace law in University of Indonesia. Critics and supports for this article can be sent to brian [at] masber [dot] com

[2] Fred H. Cate,(1997). *Privacy in Information Age,* Brookings Institution, p.21.

tion has the right to get a guarantee from the one who held the information, that the information will not be disclosed to anyone. The one who held secret information also has the right to deny every request to disclose the information, if the requester is not authorized to know the information. Third, every secrecy system must have particular object. For example, secrecy in banking area can only be applied in document related to banking activities.

There can be three kinds of secrecy system. First, theory of full secrecy. This theory determines that the one, who hold secret information, in any circumstances, whether ordinary or extraordinary, must keep that secret even if it has to sacrifice other interest which may be bigger than the interest that is protected by that secrecy. Second, theory of relative secrecy. This theory determines that the one who hold secret information can or must disclose the secret, if there is bigger interest call for it.[3]

Every government operates secrecy as one of mechanism to protect the state, the people, and the assets from threats. In some countries, the procedure and responsibility for all related stakeholders regarding the protection of government secrecy is regulated in a sui generis law of government secrecy. However in Indonesia, the legal system about government secrecy is still unclear, because Indonesia does not have legal definition of government secrecy and the effort to promulgate a sui generis law about it has not been succeeded yet. There are several possible problematic outcomes out of this situation for Indonesia, such as the difficulties to determine what kind of information that can be classified as secret, difficulties to measure how much secret information that kept and managed by the government personnels or contractors, and difficulties to assess whether the government secrecy has been misused for the benefit of personal or vested group.

Although Indonesia does not have a sui generis law on government secrecy, several laws have provisions that served as the rules of government secrecy; and the one that presented in this article is Law No. 43 of 2009 about Archives that contain provisions about "closed archives". In this article, I propose a scheme about how the Indonesian National Archives can manage their "closed archives" as a part of the state secret.

II. Lack of Clarity of the Rules of Government Secrecy in Indonesia

The popular name for the government's secret information in Indonesia is *State Secret*. Generally, state secret is defined as something that has to be kept secret for the sake of national interest,[4] but the problem is that in legal context there is no exact meaning of the term 'national interest'. That term factually is not mentioned and defined in any law in Indonesia.

Although there is an unclear legal provision on secrecy, people usually refers to KUHP or Kitab Undang-Undang Hukum Pidana (Law of the Penal Code) as the basis to punish person who disclose state secret. KUHP does not mention the term "state secret" at all and there is no specific chapter governing that matters. In that law there is one chapter that titled "disclosure of

[3] Ko Tjay Sing, (1978). *Rahasia Pekerjaan Dokter dan Advokat [Secrecy in the Work of Doctor and Lawyer]*, Gramedia, p.10.

[4] Tim Penyusun Kamus Pusat Pembinaan dan Pengembangan Bahasa,(1994). *Kamus Besar Bahasa Indonesia [General Dictionary on Indonesia Language]*, 2nd ed., Balai pustaka.

secrecy", but it only regulates the penal sanction for the disclosure of official secret, disclosure of employment secret, and disclosure of trade secret.

Secrecy is mentioned in article 113 KUHP (Law of the Penal Code) as an attribute of letters, maps, plans, pictures, or items that is related to the defense and security of Indonesia against attack from the outside, that must not be known by unauthorized person. In 1991 there is a case in *Pengadilan Negeri Bandung* (lower court) that related to this article. On their legal analysis, the judge said that,

"the term 'defense' and the term 'security' of Indonesia against attack from the outside as the fourth element of article 113 (1) of the Law of the Penal Code are actually military terms, therefore according to our opinion, the meaning of the terms must be construe in accordance with the meaning that commonly used by the military corps".[5]

That judge interpretation seems in contradiction with *Pedoman Pokok Pengamanan Pemberitaan Sandi* (Main Guidance of the Security of Encrypted Messages). It is because the Guidance says that the meaning and classification of state secret is generally similar with the provisions in Law No. 43 of 1999 on State Employee.[6] This law is only regulating non military employee and explicitly recognize something that is called official secrecy (*rahasia jabatan*). Therefore, if the meaning of state secret must be construe under this law, then there can be two consequences. First, state secret can also be seen from non military perspective. Second, state secret is similar with official secret.

That conflict of opinion shows that it is not clear whether state secret only applied in government's military domain or can be in civilian domain. The distinction between state secret and official secret is also unclear. The concept of official secret which is the secret that only apply for state employees who hold "trusted state position"[7] is seem not applicable in Indonesia. The law No. 43 of 1999 does not determine explicitly, first, what are the trusted state positions, and second, who can hold that position. Consequently, there is a generalization that all employees have authority on official secrecy.

Despite of the lack of legal basis for the definition of state secret, *Lembaga Sandi Negara* (State Encryption Agency) acknowledges four levels of secret information, Top Secret (*Sangat Rahasia*), Secret (*Rahasia*), Confidential (*Rahasia Dinas*), and Restricted (*Terbatas*). The information is classified based on the content, which mainly can be divided into two categories, strategic information and tactical information.[8] However, there is no law that describes that classification basis more detail.

This lack of clear legal basis for state secrecy creates an extensive range of discretion among government officials. In the end, the interpretation of state secret is different from one agency to another. Not only that, the parameter and the limitation to establish something as state secret also vary because it depends on, "the preference of thought and policy of the leader in each agency".[9] In addition to that, Lembaga Sandi Negara (State Encryption

[5] Bandung Court Decision (Putusan No. 04/Pid/B/1991/PN Bdg, 23 Maret 1991).

[6] Lembaga Sandi Negara,(2002). *Berita Rahasia dan Klasifikasinya [Secret Information and Its Classification]*" , p.2.

[7] Ko, *supra* p.19.

[8] Lembaga Sandi Negara, *supra* p.8.

[9] Departemen Pertahanan Republik Indonesia,(2000). *Naskah Akademik Rancangan Undang-Undang tentang Rahasia Negara Republik Indonesia* [Academic Draft of State Secret of Republik Indonesia

Agency) also mentions that,

"the meaning of state secret among government officials, officially does not have similarity because there is no law or regulation that can be used as guidance; therefore it is very difficult to gain a common perception about state secret".[10]

Conclusively it can be say that until now there is no formal conception of state secret in Indonesia.

III. The Relation of the Rules of Closed Archives with Government Secrecy

Indonesia already had a sui generis law about national archives since 1971. In 2009 that law was amended by the Law No. 43 of 2009 about Archives. This law stated that the head of each agency of archives has the authority to declare that certain static archives be closed for public access (article 66.5). There are four type of agency of archives which are mentioned explicitly in this law, namely Indonesia National Archives (as the agency of archives in the national level), Provincial Archives (as the agency of archives in the provincial level), Municipal Archives (as the agency of archives in the city or town municipal level), and University Archives (as the agency of archives in the university).

There is a serious problem in this law. Article 62.2 of this 2009 Archives Law provided the basis norm for the discretion to determine certain static archives be closed for public access. That provision serves as a legal norm for classifying certain archives as secret. There are at least three problems raised by that provision. First, considering that there are multiple type of agency of archives, does this provision mean that there are also multiple type of secrets, for example: national secret, provincial secret, municipal secret, or university secret? If that provision should be interpreted that there are multiple secrets, then which of those secrets that can be considered as state secret or government secret? Second, classifying certain archives as secret is a serious threat to the principle of freedom of information, but why does this article not expressly giving the criteria of the information or circumstances that can be used as the basis for classifying certain archives as secret? How can this classifying authority be executed appropriately if the exact laws and regulations that needed to implement this article has not been promulgated yet? Third, in this article of 62.2, the criteria for classifying is not mentioned specifically, but why does in article 62.3 the criteria for declassifying is mentioned? How the relevan stakeholders can appropriately declassify certain archives while they don't have any guidance on the criteria of classification? Furthermore, the criteria for declassifying the closed archives in article 62.3 obviously shows that closed archives is not always a state or government secret. One of the clue is that the article 62.3 stated that the protection of the intellectual property and unfair trade competition – the subject matter which belongs to private interest and not state or governmental interest – can be considered as the basis for declassifying the closed archives.

In 2012, the Indonesian government promulgated Government Regula-

Bill], Jakarta, Januari 2000, p. 1.

[10] Lembaga Sandi Negara, *supra* p. 9.

tion No. 28 of 2012 about the Implementation of Law No. 43 of 2009 about Archives. This technical rules does not help at all in solving problems related to the article 62.2 of the 2009 Archives Law. It mentioned the term of 'security classification' in article 38, but it does not explains what kind of archives that can be classified as open or closed.

Considering this circumstances, rules about the type and scope of closed archives are needed, so that the head of agency of archives can execute their authority appropriately and the rights of the citizen to have as much freedom of information can be guaranteed. The Law No. 14 of 2008 about Disclosure of Public Information is not sufficient, because it has several substantial errors on its provisions about 'Public Information Exempted from Disclosure'. Therefore, a sui generis law on government secrecy should be seriously considered for that purpose.

IV. Scheme for Managing Closed Archives as Government Secrecy

To inspire the rule making process on this issue, I would like to propose a scheme on how to manage a close archives as government secrecy. The management scheme of closed archives will be constructed using the concept of life cycle. This concept assumes that every record progresses through three phases; creation, use and maintenance, and disposition.

A. Creation

To successfully manage records creation, an organization needs program such as directives management, forms management, and reports management.[11] Directives provide clear, standardized instructions on the organization's policies and procedures. Forms are used to collect information for repetitive and standardized organization uses and are a major organization's document used for gathering, processing, and distributing information. Reports management can reduce complexity by providing only essential information to those who really need it.

In this creation phase, secrecy can be limited by regulating the kind of information that can be classified as secret. Before doing that, it is very important to define the justification first. The author proposes this rationale: that disemination of certain information may create harmful effects to particular person or to the national security interest.

Nonetheless, considering that secrecy is often used to hide the bad conduct of government officials, it is very important to define first what information should not be classified as secret. The United States determines information that (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or (4) prevent or delay the release of information that does not require protection in the interest of the national security, can not be classified as secret.[12] Indonesia can adopt that as a model.

Information that can be classified as secret is information that related

[11] Zulkifli Amsyah,(1996). *Manajemen Kearsipan [Management of Archives]*, Gramedia Pustaka Utama, p.6.

[12] Executive Order 12958 § 1.7.

to, 1) military activities, 2) intelligence activities, 3) diplomatic activities, 4) science and technology activities that related to national security, 5) cryptology activities. It is very important to note that not all information in those categories of activities is worth to be protected by secrecy.

Not all military information can be classified as secret. However, there are several information that is very important to be protected by secrecy, such as the site and timing of a planned attack, military tactics and strategy, the location of naval vessels, the supply of ammunition, and the number of troops.[13] In wartime, secrecy concerning such matters is essential to the ability to surprise an opponent and reduces the opponent's ability to plan a successful attack. Disclosure of a planned invasion site, for example, enables the opponent to strengthen the defense at the point of attack and to plan a surprise counteroffensive.

Intelligence operations fall into two categories, information gathering and covert operations. The first category consists of the collection and analysis of information about other nations and their activities. Much information gathering today involves the use of satellites, interception of messages, and abstracting information from open sources such as political reports, but undercover agents and confidential sources continue to be employed. A specific need for secrecy in the field of intelligence usually related with four kinds of information: (1) the identity of agents and sources; (2) information relating to methods and capabilities; (3) reports from intelligence agents; and (4) intelligence information provided by allied nations.[14] Disclosure of the identity of agents and sources impairs the ability of agents to gather intelligence, dries up sources, and may endanger the lives of those named. Disclosure of methods and capabilities alerts foreign nations to the need for countermeasures and tends to frustrate intelligence operations. Disclosure of the techniques employed to transfer information out of a country, for example, may preclude further use of those techniques; disclosure of information relating to technical collection systems may render the systems worthless. Disclosure of the reports of intelligence agents may give clues to the identity of agents and sources or of methods and capabilities.

Secrecy is very important in diplomatic negotiations, because the disclosure of negotiating strategy and goals may impair the capability of negotiating the most favorable terms. A negotiating party that discloses its minimum demands usually will get nothing more than the minimum.[15] In some instances, secrecy is intended to preserve the capacity for surprise and to avoid warning those against whom the agreement is directed.

Scientific and technological information can be divided into three broad categories: (1) information with exclusively military applications; (2) information with both military and civilian applications; and (3) information with no known military applications.[16] The first category includes information about the design and capabilities of weapons systems and research directed towards developing new systems. Much of this information is governmental in origin and available, directly or indirectly, only from government sources. Weapons tests, for example, are conducted by the government, and the re-

[13] Benjamin S. Duval,(1986).Jr., *The Occasions Of Secrecy*, 47 U. Pitt. L. Rev. p.579, 592.
[14] *Id.*, p.598.
[15] *Id.,* p. 616.
[16] *Id.,* p.604.

sults can enter the public domain only if they are released, leaked, or stolen. Restrictions on the dissemination of dual use technology sometimes are justified on grounds unrelated to military considerations, such as the costs of research and put competing products on the market more rapidly than otherwise would be possible. Conversely, nondisclosure enables companies to maintain a competitive advantage in international competition. Secrecy may also inhibit the spread of some types of weapons to less developed nations.

Cryptology includes both signal security (ways of keeping messages secret) and signal intelligence (ways of intercepting messages). Cryptologic information includes information relating to intercepting messages, to constructing codes, and to breaking codes.[17] Restrictions on disclosure of cryptologic information are designed both to protect the security of government communications and to preserve the ability to gather intelligence by intercepting messages and breaking the codes of other nations.

With regard to this creation phase, one of the important things is to establish a suitable implementing agency. If the ministries are chosen as the implementing agency, there are pros and cons. The pros is that the ministries are the parties who usually produce and control the information. The cons is that often that authority is used for improper purpose, such as to hide corruption activities. If the court is chosen, then the pros is that its decision will have more power to related parties. This will make the secrecy classification's rule more concrete than the one in the statute. However, there are several cons. First, Indonesia does not implement precedent; therefore it is likely that former court's decision will only have small effect on future cases. Second, court is passive institution. It waits for cases. In Indonesia the culture of settling cases through court is still undeveloped. Therefore, the law may not have a good progress, because there may be not enough case in this matter. Nevertheless, comparing those two models of implementing agency the author thinks that the final authority to enforce the rules should be assigned to the ministries.

B. Use and Maintenance

Records remain in the maintenance and use stage until they become inactive. In conventional practice, an active record need to be stored in a record keeping system that permits retrieval and protects them from loss or damage.[18] The benefit of managing the maintenance and use stage is that record loss is minimized and retrieval time is shortened.

In this phase of life cycle, secrecy can be limited by regulating the procedure of safeguarding the secret information. Using the United States' system as a model, this procedure can be consisting of two activities. First, establishing general restriction on access. It means that a person may have access to classified information if (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee; (2) the person has signed an approved nondisclosure agreement; and (3) the person has a need-to-know the information. Classified information may not be removed from official premises without proper authorization. Second, establishing distribution control. It means that the person who distributes classified infor-

[17] Simon Singh,(1999). *The Code Book: The Evolution of Secrecy From Mary, Queen of Scots to Quantum Cryptography,* Double Day, p.8.

[18] Sedarmayanti,(1990). *Tata Kearsipan Dengan Memanfaatkan Teknologi Modern [Management of Archives with the Help of Modern Technology]*, Yayasan Bina Administrasi, p.30.

mation must ensure that it is distributed only to organizations or individuals eligible for access and with a need-to-know the information.

C. Disposition

In this phase, records retention schedules are written to establish policy on the retention and disposition of records. Records retention ensures that records are retained for the required period; records disposal ensures that records are removed to lowcost storage or destroyed once they become inactive or their value declines. Disposition results in disposal of records, or if they have historical value they are transferred to archival storage.[19] The records management organization is responsible for setting retention schedules and making appropriate storage available for inactive and archival records. Records management also monitors and/or executes the destruction of records once their retention periods have expired. In this disposition phase, secrecy can be limited by regulating the procedure of declassifying secret information.

Using the United States' system as the model, this procedure may includes seven areas: 1) authority of declassification, 2) transferred records, 3) automatic declassification, 4) systematic declassification review, 5) mandatory declassification review, 6) processing request and reviews, and 7) declassification database. Furthermore, within the Indonesia National Archives, a professional unit can be set up to conduct following activities: 1) to hold classification activity to the minimum necessary to protect the national security, 2) to ensure the safeguarding of classified national security information in both Government and industry in a cost-effective and efficient manner, 3) to promote declassification and public access to information as soon as national security considerations permit.

V. Conclusion

There is lack of clarity of rules for the secrecy system in Indonesia. The existing statutes are only determining penal provisions, but they do not include material provisions. Ultimately, there is no uniform conception among government officials, because each agency makes its own policy and system. This condition brings disadvantage to society, because there is no clear guidance on this subject and it will not be able to push the government to act more responsible in managing the information.

To get the accountability in the management of closed archive, the government does not have any other option than establishing a set of rules that describe a clear secrecy system. The secrecy concept can be framed within the concept of records life cycle. Therefore, it can be more adjustable to the existing system.

With a clear rule of law on secrecy, the problem of uncertainty in government secrecy law can be solved. Furthermore, the society can have more chance to criticize what information can be classified as secret, which can have the authority to classify, or know how much the classified and declassi-

[19] Arsip Nasional RI,(1998). *Penyusutan Arsip [Disposal of Archives]*, ANRI, Proyek Pembinaan Kearsipan, p.13.

fied information in the government. Finally, this law on government secrecy will push the government to be more accountable in the management of dynamic archive, so that it will comply with democratic values.

Bibliography

Books and Articles

Amsyah, Zulkifli,(2006). *Manajemen Kearsipan* [Management of Archives], Gramedia Pustaka Utama.

Arsip Nasional RI,(1998). *Manajemen Arsip Inaktif* [Management of Inactive Records], Proyek Pembinaan Kearsipan

Arsip Nasional RI.(1998). *Pengantar Manajemen Arsip* [Introduction to Management of Archives], Proyek Pembinaan Kearsipan

Arsip Nasional RI,(1998). *Penyusutan Arsip* [Disposal of Archives], Jakarta, ANRI, Proyek Pembinaan Kearsipan.

Basuki, Sulistyo,(1999). *Manajemen Arsip Dinamis: Sebuah Pengantar* [Records Management: An Introduction]

Cate, Fred H,(1997). *Privacy in Information Age,* Brookings Institution.

Departemen Pertahanan Republik Indonesia,(2000). *Naskah Akademik Rancangan Undang-Undang tentang Rahasia Negara Republik Indonesia* [Academic Draft of State Secret of Republik Indonesia Bill],Jakarta.

Dmitrieva, Irina,(2003). *Stealing Information: Application Of A Criminal Anti-Theft Statute To Leaks Of Confidential Government Information*, 55 Fla. L. Rev. 1043

Duval, Jr., Benjamin S,(1986). *The Occasions Of Secrecy*, 47 U. Pitt. L. Rev. 579

Ellis, Judith(Ed.),(1993).*Keeping Archives,* 2nd Ed. Australia, Thorpe.

Halstuk, Martin E,(2002). *Policy Of Secrecy-Pattern Of Deception: What Federalist Leaders Thought About A Public Right To Know, 1794-98*, 7 Comm. L. & Pol'y 5.

Karin, Marcy Lynn,(2002). *Out Of Sight, But Not Out Of Mind: How Executive Order 13,233 Expands Executive Privilege While Simultaneously Preventing Access To Presidential Records*, 55 Stan. L. Rev. 529

Ko, Tjay Sing,(1978). *Rahasia Pekerjaan Dokter dan Advokat* [Secrecy in the Work of Doctor and Lawyer], Gramedia

Lay, Wahyu., *Sartini, Kearsipan* [Archives], Angkasa, 1995.

Lee, Edward,(2003). *The Public's Domain: The Evolution Of Legal Restraints On The Government's Power To Control Public Access Through Secrecy Or Intellectual Property, 55 Hastings L.J. 91*.

Lembaga Sandi Negara,(2008). *Berita Rahasia dan Klasifikasinya* [Secret Information and Its Classification]

Roeslosz, MAP Meilink,(1973). *Dari Arsip Tertutup Sampai Arsip Terbuka* [From Closed Archives to Open Archives], Jakarta, Bhatara.

Sedarmayanti,(1990). *Tata Kearsipan Dengan Memanfaatkan Teknologi Modern* [Management of Archives with the Help of Modern Technology], Yayasan Bina Administrasi

Sims, John Cary,(1993). *Triangulating The Boundaries Of Pentagon Papers*, 2 Wm. & Mary Bill Rts. J. 341

Singh, Simon,(1999). *The Code Book: The Evolution of Secrecy From Mary, Queen of Scots to Quantum Cryptography*, Double Day.

Sprehe, J. Timothy,(2002). *New Controls On Access To Government Information*, Internet Connection

Suparyati, Tuginem, Pudji Rahayu,(2002). *Tata Usaha dan Kearsipan* [Administration and Archives], Kanisius.

Tim Penyusun Kamus Pusat Pembinaan dan Pengembangan Bahasa,(1994). Kamus Besar Bahasa Indonesia [General Dictionary on Indonesia Language], 2nd ed., Balai pustaka.

Wijaya AW,(1986). *Administrasi Kearsipan: Suatu Pengantar* [Archives' Administration: An Introduction], Rajawali.

Wiriadiharja, H. Muftie,(1987). *Beberapa Masalah Kearsipan Di Indonesia* [Several Problems of Archives Management in Indonesia], Balai Pustaka.

Website

"Indonesia Belum Memiliki Batasan Rahasia Negara [Indonesia Do Not Have Limitation on State Secret Yet]",available at http://www.hukumonline.com.

Report of The Commission on Protecting and Reducing Government Secrecy, http://www.access.gpo.gov/int, last visited August 9, 2004.