SAFENET Position Paper

Analysis of the Regulation of the Minister of Communication and Informatics (PM Kominfo/MR) No. 5 of 2020 concerning Private Electronic System Operators

Part 1:
Introduction

In the midst of the Covid-19 pandemic, on November 24, 2020, the Government through the Minister of Communication and Informatics of the Republic of Indonesia (hereinafter abbreviated as Kominfo), promulgated Regulation of the Minister of Communication and Informatics No. 5 of 2020 concerning the Private Electronic System Operators (hereinafter abbreviated as PM Kominfo/MR 5/2020).[1]

The provisions of PM Kominfo/MR 5/2020 have only one consideration, namely: "that in order to meet regulatory needs in the operation of the electronic system in the private sphere, as well as to implement the provisions of Article 5 paragraph (3), Article 6 paragraph (4), Article 97 paragraph (5), Article 98 paragraph (4), and Article 101 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, it is necessary to stipulate a Regulation of the Minister of Communication and Informatics concerning the Private Electronic System Operators."

This is certainly shocking that in the midst of public pressure of immediate completion of the discussion and ratification of the Personal Data Protection Bill, it turns out that the government instead regulates more technically related electronic systems in the private sphere. For this is the private sphere, of course, there will be legal consequences as well as problems that are very likely to occur, especially the impact that arises from not only the aspects of rules that do not comply with standards, legal theory or principles, but also from basic problems of freedom and human rights, in particular, in the realm of digital or online.

On the other hand, the legal politics of regulating the electronic systems operators still leaves basic problems that so easily threaten the assurance of freedom of opinion and expression in Indonesia. Moreover, institutionally in the state institutional system, a more independent governance arrangement to supervise and account for the operation of the electronic system has not been formulated in an integrated manner, with complete mechanism, including accommodating complaints or objections regarding the possibility of abuse of authority of institutions and individuals with an interest in power.

We know that the private sphere is a fundamental part of human rights, which under international human rights law has its own regulations, especially the right to privacy (privacy rights). Protection of

[1] Stipulated in Jakarta, on November 16, 2021 by the Minister of Communication and Informatics, Johnny Gerard Plate, State Gazette of the Republic of Indonesia Year 2020 Number 1376.

personal rights itself has such a broad dimension or scope and cannot be simplified as a right that is easily limited, even though its position is as derogable rights (qualification of rights that can be limited). The right to internet access is a human right (internet rights). Often it is also called the right to access digital technology (digital rights). The two have become very close in human life in this century, that is why the UN Human Rights Council has stated in its resolution.[2]

Thus, this PM Kominfo/MR 5/2020 needs to be studied and placed within the framework of legal analysis, especially the policies related to digital rights as an important part of human rights in the midst of a digital society, and at the same time analyzing more deeply its position as one of the rules in hierarchy of laws and regulations.

Based on these, this position paper is intended to answer two things:
How are the arrangements for the electronic system operation related to the private sphere in the legal system, especially in the framework of human rights law and statutory law?

Does the regulation in PM Kominfo/MR 5/2020 comply with human rights law standards and guarantees freedom of expression, as well as what impact it will have?

[2] Human Rights Council, Thirty-Second Session, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, A//HRC/32/L.20, 27 June 2016.

Part 2:
Right to Privacy, Normalization and Restrictions: Theoretical Approach

---

The right to privacy as a human right

Privacy in the digital era is a fundamental part of human rights development, providing a framework that helps to measure better standards, particularly in protecting the rights of persons (privacy rights). This is because human rights provide a global consensus on which to develop the rules and principles on the conditions for human development itself, including in the objectives of guiding the legal system, government policies, the work of non-governmental organizations, as well as for learning in higher education.

Violation of human rights in such context is a denial of the opportunity to gain the core human well-being. No exception, in terms of protecting the right to privacy as one of these rights. Article 12 of the 1948 Universal Declaration of Human Rights (UDHR) states the following:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Although Article 12 (above) clearly aims to protect against invasion of privacy such as breaking into someone's house and stealing their email, with such rapid development of technology, it is necessary to develop ideas about the right to privacy in this digital age. Storing and sharing personal information, for example, is a process that deserves serious consideration. It supports other basic rights such as freedom of speech and freedom to associate.

The United Nations has stated, "the same rights that people have offline must also be protected online." In 2013, the United Nations adopted a resolution to reaffirm and outline the right to privacy in the digital age, calling for governments to be transparent and proactive in addressing two major privacy vulnerabilities, namely those relating to the surveillance and misuse of personal data.

Surveillance in a vulnerable situation is a form of surveillance action that actually "hinders the free functioning of civil society," or the vulnerability of digital communications to surveillance to do so. It can be ascertained that if information and electronic transactions, for example, are vulnerable to excessive surveillance, it is estimated that a number of human rights violations will occur.

On the one hand, there is the responsibility of the government to exercise oversight that can enable a corrupt government bureaucracy to exercise power more efficiently and more effectively, or also to supervise companies that are also involved in corruption.

On the other hand, the dangers of non-government surveillance are equally alarming. Indeed, it can empower individuals or governments to monitor, prevent or avoid certain conflicts that can create potential for violence. For business entities, it can also concentrate knowledge in the hands of a few influential people and allow commercial entities to influence consumer behavior.

However, this should be clear and more careful in its limitations. Because in practice there are indeed spyware practices that were exploited in the civil war in Syria, and in that context it can be a very powerful weapon in all lines of information. However, the basic principle is how communication and information technology cannot easily be abused by political and commercial actors.

Meanwhile, the second vulnerability is about the misuse of personal data. Exposing personal data can result in system destruction and even damage to reputation with major repercussions. Misuse of personal data is, of course, a violation of rights. Personal data can be collected digitally, biometrically, genetically, and through video and other media. The type of data that is collected, and what is done with it, affects more than just the right to be protected from what is known as "arbitrary interference with ... [one's] correspondence".

This is linked to other basic rights protected by UDHR, such as the right to a fair trial, if communication between the accused and his lawyer is disclosed. In fact, this must be protected. Likewise, the rights to freedom to gather and freedom to associate are indeed rights or freedoms that can be limited, but the restrictions should not actually eliminate the position of guaranteeing these basic rights or freedoms.

The right to be free from discrimination can be violated when linked or proxy data (eg algorithms displaying individual profiles, voting behavior, religion) is collected and used to block access to information or access to certain information. And this, of course, is contrary to the freedom which should have been guaranteed.

Like algorithmic data in practice, efforts to influence consumer behavior are not a mere violation of rights, but can erode systems that defend other rights protections. Although human rights are mostly individual rights, they in turn also need collective systems (such as privacy and data use standards) to be upheld while guaranteeing protection for all.

Regulation of right to privacy in the Indonesian statutory system

Legislation hierarchy theory

The regulation of right to privacy, including restrictions, is a form of regulation which of course has consequences for disturbing the basic rights of citizens. In statutory theory, the provisions regulating the rights and limitations of the basic rights of citizens should be regulated in legal products that require the consent of the people or citizens, in this context the approval of the people's representatives or parliament. Especially if the regulation contains certain legal sanctions, it is not sufficient that it is regulated in the provisions of the executive legal product alone.

Based on Law No. 12 of 2011 which was later amended by Law No. 15 of 2019, shows that in the order of or hierarchy of Ministerial Regulations, it is regulated in the Elucidation of article 8, paragraph (1) of Law Number 12 of 2011 concerning the Formation of Legislation. (hereinafter abbreviated as UU 12/2011).

Article 8 paragraph (1) of Law 12/2011 states,

> Types of Legislation other than those referred to in Article 7 paragraph (1) include regulations stipulated by the People's Consultative Assembly, the House of Representatives, the Regional Representative Council, the Supreme Court, the Constitutional Court, the Supreme Audit Agency, the Judicial Commission, Bank Indonesia, the Minister, bodies, institutions, or commissions that are at the same level as established by law or the government at the behest of the law, the Provincial People's Representative Council, the Governor, the Regency/City Regional People's Representative Council, the Regent/Mayor, the Village Head or equivalent.

Meanwhile, Article 8 paragraph (2):

> Legislation as referred to in paragraph (1) is recognized for its existence and has binding legal force as long as it is ordered by a higher level of statutory regulations or is established based on authority.

Whereas in the Elucidation of Article 8 Paragraph (1),

> What is meant by "Ministerial Regulation" is a regulation stipulated by a minister based on content in the framework of carrying out certain affairs in government.

And the Elucidation of Article 8 Paragraph (2),

> What is meant by "competent authority" is the administration of government in accordance with the provisions of the Legislation.

If the substance of PM Kominfo/MR 5/2020 includes the regulation of digital rights, including restrictions, given that it relates to privacy rights, then clearly, (1) the substance or content actually exceeds the limits given in Law 12/2011, because the content of the Permenkominfo should be limited to the framework of 'administering certain government affairs'. (2) it is a concrete form of arbitrariness in the formation of laws and impact on the potential for legalized violations of basic rights or human rights.

Norming theory

Hans Kelsen stated that the authority to form norms needs to be considered. The authority to determine what should be in a legal provision derives from the norm. According to Kelsen, the analysis is based on the norm validity principle as an objective assessment mechanism for human behavior. According to him, a norm is said to be valid if it is formed by the competent authority to form the norm. This authority is obtained from other norms of a higher position.[3]

[3] Hans Kelsen, *Teori Hukum Murni: Dasar-Dasar Ilmu Hukum Normatif* (translated from The Pure Theory of Law).

This is very important to understand in the practice, what authority forms PM Kominfo/MR 5/2020, what is the basis for the rules, and based on what legislation the mandate is obtained. Such questions need to be considered as a form of understanding the authority known as attribution.

Three-part test theory

The foundation for international law regarding freedom of expression is based on Article 19 of the Universal Declaration of Human Rights (UDHR, 1948) and Article 19 of the International Covenant on Civil and Political Rights (hereinafter referred to as ICCPR, 1966). The ICCPR has become Indonesian law after the Indonesian government ratified it through Law no. 12 of 2005.

Substantively, Article 19 states:

(1) Everyone has the right to have an opinion without interference.
(2) Everyone has the right to freedom of expression; This right includes freedom to seek, receive and impart any information and thoughts, regardless of restrictions orally, in writing, or in printed form, artwork or through other media of his choice.
(3) The exercise of the rights contained in paragraph 2 of this article creates special obligations and responsibilities. As such may be subject to certain restrictions, but this can only be done in accordance with the law and to the extent necessary to: (a) Respect the rights or reputation of others; (b) Protect national security or public order or public health or morals.

General Comment No. 34, Paragraph 3 explicitly states, "that the exercise of the right to freedom of expression is accompanied by special duties and responsibilities. For this reason, there are limited areas with respect to the limitations of permissible rights in order to respect the rights or good names of others or for the protection of national security or public order, or public health or morals. However, when the State party imposes restrictions, the exercise of freedom of expression is not allowed to make the right itself disappear. "The Committee reminds" that the relationship between rights and limitations and between norms and exclusions must not cause the situation to reverse."

Enforcement of the limitation of expression, among others, refers to a three-stage test, which is goal-oriented to test the legitimate aim, in accordance with existing laws, is necessary and proportional. The concrete scope related to legitimate purposes will depend on the stipulated provisions, for example those related to the interests of public safety, national security, public health, and so on. This test is also based on the existence of national laws, with the indicator that these laws must be clear, open and transparent that are known to all citizens to enable them to understand their behavior and understand about prohibited acts or actions. Vague and broad laws, for example on national security objectives, do not fit the indicators of clear laws.

Permissible Limitations: Standard and Mechanism

In the development of the law, there is a number of doctrines developed by experts in human rights law which are then adopted in authoritative interpretation as a reference in interpreting international human rights law instruments, specifically related to the restrictions permitted by Article 19 paragraph 3 of the ICCPR, ratified by Law no. 12 of 2005.

The criteria for limiting freedom of expression and the right to information as stipulated in Article 19 paragraph (3) of the ICCPR (which has been ratified by Law No. 12 of 2005), are based on several detailed legal interpretations,

1. *Prescribed by Law*. This is interpreted through 4 things, (i) There are no restrictions on human rights, except by expressing them in the generally applicable national law which is consistent with the ICCPR and enforced for a limited period of time. (ii) Laws that are issued limiting human rights must not be arbitrary or without justifiable reasons; (iii) Legal rules aimed at restricting must be clear and accessible to all parties. (iv) Adequate arrangements must also be provided or regulated in these provisions, including when there is an abusive and illegal regulatory obligation, or a consequence of the implementation of such restriction of rights.

2. *Legitimated Aim*. The interpretation of this is related to the restrictions that must fulfill one of the stated objectives stated in the text of human rights legal instruments (legitimate aim). In particular, it refers to article 19 paragraph (3) of the ICCPR.

3. *Necessary*. The limitation measure must be necessary to achieve the necessary aims, this can be tested from, (i) Is the proposed limitation proportional to the objective? Is it the least necessary constraint to meet the goal? (ii) Is there a primary public interest in providing information? (iii) Does the limitation "may not jeopardize the right itself"? As noted in General Comment 34, that the reason of 'necessary' "must be appropriate to achieve their protective function."

Such restrictions are possible, because freedom of expression is not an absolute right, and there are a number of situations in which derogable rights are limited. However, the process of restricting freedom of expression (or other human rights) cannot be carried out without justification on the basis of sufficient reasons.

With this standard, restrictions on rights or freedoms are made possible by law, to the extent that they meet the requirements,

(1) Must comply with international human rights law standards, a three-part test, including the doctrine of related restrictions, especially article 19 paragraph (3) of the ICCPR, one of which refers to the principles of Syracusa.

(2) With regard to the blocking in general, it is necessary to take into account developments from the experience of other countries, in particular referring to the Council of Europe (EU), which has recommended that public authorities should not carry out acts of public blocking, denying public access to information on the Internet, regardless of the limits. The United Nations and three other specific mandates on freedom of expression explain that "blocking of entire websites, IP addresses, ports, network protocols, or types of use (such as social networks) is an extreme measure - analogous to a newspaper ban or broadcasters (in the context of Indonesian law, called bredel pers) - which can only be justified according to international standards.

Part 3:

Legal Review

PM Kominfo/MR 5/2020 concerning Private Electronic System Operators, was stipulated on November 16, 2020 and promulgated on November 24, 2020, through the State Gazette of the Republic of Indonesia No. 1376.

PM Kominfo/MR 5/2020 consists of 7 Chapters, 49 articles. The details can be seen in the following table,

Chapter	Name of Chapter	Article
Chapter I	General requirements	Article 1
Chapter II	Registration of Private Electronic System Operators	Article 2-8
Chapter III	Management and Moderation of Electronic Information and/or Electronic Documents	Article 9-12
Chapter IV	Request for Termination of Access to Electronic Information and/or Prohibited Electronic Documents	Article 13-20
Chapter V	Granting Access to Electronic and/or Electronic Systems for the Purpose of Supervision and Criminal Law Enforcement	Article 21-46
Chapter VI	Transitional Provisions	Article 47
Chapter VII	Closing	Article 48-49

Relation with PP 71/2019

To understand this Permenkominfo, it is necessary to look at the basis of the mandate given, so that it is known why this regulation is at the Ministerial level. In the single Considering section, it states:

> "... that in order to meet regulatory requirements in the operation of electronic system in a private sphere, as well as to implement the provisions of Article 5 paragraph (3), Article 6 paragraph (4), Article 97 paragraph (5), Article 98 paragraph (4), and Article

101 Regulation Government Number 71 of 2019 concerning Electronic Systems and Transactions, it is necessary to stipulate a Regulation of the Minister of Communication and Informatics concerning Private Electronic System Operators; "

Articles	Reference to Government Regulation (PP) Number 71 of 2019
Article 5 paragraph (3)	The provisions regarding the obligations of the Electronic System Operator as referred to in paragraph (1) and paragraph (2) shall be regulated by a Ministerial Regulation.
Article 6 paragraph (4)	(4) Further provisions regarding Electronic System Operator registration as referred to in paragraph (3) shall refer to the norms, standards, procedures and criteria stipulated by a Ministerial Regulation.
Article 97 paragraph (5)	Provisions regarding the procedure for application for termination of access as referred to in paragraph (1) to paragraph (4) shall be regulated in a Ministerial Regulation.
Article 98 paragraph (4)	Further provisions regarding the implementation of the obligation to terminate Access as referred to in paragraph (1) shall be regulated in a Ministerial Regulation.
Article 101	Further provisions regarding the procedure for the imposition of administrative sanctions and for filing objections to the imposition of administrative sanctions are regulated in a Ministerial Regulation.

By examining the details in PP 71/2019, it is known that the Permenkominfo is aimed at implementing the "order" of Government Regulations into ministerial-level operational rules, which are explicitly written down the legal formation with/in the Permenkominfo.

Hierarchically, the *lex superiori derogate lex inferiori* law principle applies, that is, the rules below may not even contradict higher rules. From this point of view, let us observe the coherence of the statutory regulations.

Request for Termination of Access

The provisions in the Permenkominfo need to be considered in relation to the protection of digital rights for individuals and the public at large. How could it not be, in the regulation of PM Kominfo/MR 5/2020 there are 65 keywords of "Termination of Access", both interpreted as access blocking and take down. This signifies at least two things,

(i) the potential for limiting rights or freedoms is high, and very likely to interfere with the interests of electronic system administrators in the private sphere, especially if not for legitimate and disproportionate reasons;
(ii) the standard of limitation, especially in the issue of termination of access, needs to be examined in depth to what extent it guarantees protection of rights, including whether or not there is an adequate mechanism for complaints (this is called the grievance mechanism in access to justice for public services).

In addition, the most fundamental thing and a hindrance in encouraging the development of protection assurance for the private electronic systems operators (ESO) in the private sphere is that this PM Kominfo/MR instrument has emphasized a legal position that will force all ESOs, from various social media platforms, to provide online-based services, to submit to and accept domestic or local jurisdiction, both for content and use of content in daily practices.

In Chapter III, regarding the Governance and Moderation of Electronic Information and/or Electronic Documents, in particular the rules in Article 9 paragraph (3) and (4),

> Article 9 paragraph (3):
> Private ESO is obliged to ensure that: a. The Electronic System does not contain any prohibited Electronic Information and/or Electronic Documents; and b. The Electronic System does not facilitate the dissemination of prohibited Electronic Information and/or Electronic Documents.
>
> Article 9 paragraph (4):
> Electronic Information and/or Electronic Documents that are prohibited as referred to in paragraph (3) are classified as: a. violating statutory provisions; b. disturbing the public and disturbing public order; and c. notify the way or provide access to prohibited Electronic Information and/or Electronic Documents

The phrase 'prohibited' in these two articles actually has a very broad scope and its interpretation opens up space for debate, especially if there is a conflict of interest for State Institutions or law enforcement officials. For example, what is meant by "public disturbance", what is the standard or measure, who has the authority to determine it, and what if the public feels that it is not part of what is called "disturbing society".

In fact, such arrangement is more precisely regulated by restoring its provisions to restrictions on the basis of law, because it is to protect citizens' constitutional rights. For example, what if an individual uses his social media to raise solidarity in rejecting a government or corporate project, so that it makes some people nervous who happen to work in the government or corporation.

This is because the Law was formed through two institutions that administer power which have a 'check and balances' mechanism (the principle of balance), so that the destructive power of catchall interpretations can be prevented or limited. If not, then this flexible regulation in PM Kominfo/MR 5/2020 is an entry point for abuse of power or arbitrariness.

In addition, in relation to Chapter IV, Article 14, regarding the Request for Termination of Access, it is necessary to consider the restriction standards stipulated in Article 19 paragraph (3) of the ICCPR, including consideration of the General Comment of the Human Rights Committee, No. 34. These considerations are based on,

First, the Petitioner.

Parties that can request termination of access, as mentioned in Article 14 (1): “Requests for Termination of Access to Electronic Information and/or Electronic Documents that are prohibited

as referred to in Article 13 can be submitted by: a. Public; b. Ministries or Institutions; c. Law Enforcement Officials; and/or d. judiciary. " With this provision, the parties are very broad, even at the stage of petition, but it can be imagined that in practice there will be requests that will interfere with the activities of the ESO itself. Therefore, the qualifications need to be more explicit so as not to make it easy to cut off access to information or unilateral requests.

Second, the Nature of Urgency.

Moreover, the reason given by PM Kominfo/MR 5/2020 also recognizes the word 'urgent'. In Article 14 paragraph (3) it is stated, "The application referred to in paragraph (1) is urgent in terms of: a. terrorism; b. child pornography; or c. content that disturbs the public and disrupts public order. "

There are three things that need to be criticized regarding the nature of this urgency,

(i) insist that the basis is not explained, whose assessment is and the specific mechanism for regulating it. Without clarity on the meaning of urgency, it is possible to predict the potential for arbitrariness.
(ii) related to the issue of terrorism, in practice the provisions (especially the Criminal Act of Terrorism), institutions, and a comprehensive interpretation of legal issues related to terrorism must be connected. Why is that, this is due to the large and broad implications, including the protection of human rights, if in the end the institution or institution has the authority related to terrorism, for example without going through the coordination of the BNPT (National Counterterrorism Agency), then the practice will be very uncontrollable and will cause losses for many parties.
(iii) content that disturbs the public and disturbs public order, which is the same as the previous analysis, how is it standardized or in practice, including the mechanism for objecting to the meaning of "disturbing the public" or "disturbing public order".

If we refer to the Syracusa Principles, the assessment of public order issues as a basis for restrictions, including termination of access in the case of PM Kominfo/MR 5/2020, can be referred to in paragraphs 22-24, concerning Public Order (*ordre public*).

> 22. The expression "public order (*ordre public*)" as used in the Covenant can be defined as a set of rules which ensure the functioning of society or a set of basic principles upon which society is based. Respect for human rights is part of public order (*ordre public*).
>
> 23. Public order (*ordre public*) is defined in the context of certain human rights objectives which are limited on this basis.
>
> 24. State institutions responsible for the maintenance of public order (*ordre public*) must be subject to control in exercising their power through parliaments, courts or other competent independent bodies.

In the midst of such a relaxed arrangement and very easy or prone to abuse, it is necessary to criticize the large and dominant role or authority of the ministry in Permenkominfo, especially in relation to the public interest.

The Ministry's enormous authority, from the authority of regulators, executors, including appraisers and executors, will certainly accumulate a lot of crucial powers and facilitate arbitrariness. It can be imagined, if they are part of the government and could at any time assess and decide on access based on his political interests. It is inevitable, that there is a concern of Permenkominfo No. 5/2020 will be abused to silence groups that criticize the government. In terms of institutional architecture, there is no independent institution or body involved, for example, the possibility of exploring mandates or powers such as courts in the mechanism of terminating access, so that their monitoring and testing becomes more limited by intervening power with conflicts of interest.

It is important to safeguard the public interest, that the enforcement of PM Kominfo/MR 5/2020 is carried out with external and independent supervision, as well as the necessary, legitimate and proportional means of enforcement to achieve one goal of limitation as stipulated in Article 19 (3) of the ICCPR.

Legal Submission through Obligation to Register

Private ESO has an obligation to register. As stipulated in the Regulation of the Minister of Communication and Information Technology Number 36 of 2014 concerning Registration Procedures for Electronic System Operators (State Gazette of the Republic of Indonesia of 2014 Number 1432), it is declared invalid since the enactment of PM Kominfo/MR 5/2020.

It is stated in Article 2 (1), that "Every Private ESO is obliged to register." In paragraph (3) it states, "The obligation to register for Private ESO is carried out before the Electronic System begins to be used by Electronic System Users."

Interestingly, the process is also not long, because it requires 6 (six) months from the promulgation of PM Kominfo/MR 5/2020. In the Transitional provisions it is stated, "Article 47 Private ESO as regulated in this Ministerial Regulation is obliged to register within a period of no later than 6 (six) months after this Ministerial Regulation comes into effect." Such transitional provisions affirm the once-completed article, or einmalig.

In a number of articles, this registration has legal consequences, particularly with respect to a number of administrative sanctions. As stated in Article 45 paragraph (4) PM Kominfo/MR 5/2020,
"The administrative sanctions as intended ... are in the form of:

a) Written warning;
b) Temporary suspension;
c) Termination of Access; and/or
d) Revocation of Electronic System Operator Registration Certificate. "

The Issuance of Registration Certificate Article 6 (1) Registration certificate for Private ESO is issued by the Minister after the registration requirements as referred to in Article 2 to Article 5 are declared complete in accordance with this Ministerial Regulation and placed in the Private ESO list. And,

because of that, it is possible to revoke the ESO Registration Certificate. This is confirmed in Article 46 paragraph (4), which confirms administrative sanctions, in the form of revocation of Electronic System Operator Registration Certificate.

This shows that Permenkominfo No. 5/2020 requires each Private ESO to register and obtain an Identification certificate issued by the Ministry before the public in Indonesia starts accessing its services or content.

The basic problem is, what if the private ESO lives abroad, or is being run from abroad, while the registration process for legal purposes has not been actively carried out? There needs to be a critical reflection on the operation of Private ESO which is actually subject to obligation to register related to financial services, social media and content sharing platforms, cloud service providers, arts and so on.

Temporary or full termination of access to a site is clearly a general prohibition against the entire site, a disproportionate act, because it relates to the protection and guarantee of digital rights. Therefore, human rights and freedom are not absolute. Limitation is carried out by considering guarantees of protection of other human rights, and that is why it is known as the limitation permitted under Article 19 (3) of the ICCPR.

Part 4:
Private ESO and Human Rights Protection

Analysis of the Articles

In general, the right to privacy is guaranteed by article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights.

Article 12 of the Declaration, states,

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Meanwhile, article 17 of the Covenant, states,

(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
(2) Everyone has the right to the protection of the law against such interference or attacks.

Meanwhile, the provisions in PM Kominfo/MR 5/2020 contain contents that are potentially contradictory to the two articles, especially based on how to place personal data in the private ESO which is so easily accessible to the interests of the authorities which so far have two basic things, namely: (1) lack of independent supervision in obtaining access to personal data; (2) In practice, personal data is often misused, especially by bureaucratic law enforcement and law enforcement officials.

The following points become the basic problem,

(1) Defining and using personal data, including specific personal data. According to Article number 21 PM Kominfo/MR 5/2020, "Specific Personal Data" is health data and information, biometric data, genetic data, sexual life/orientation, political views, children's data, personal financial data, and/or other data in accordance with the provisions of the legislation. The term separation is related to possible interventions in opening or processing it for purposes that are truly legitimate, proportional and have clear provisions in law.

The problem is, to what extent the interpretation of "needs" or "level of urgency" is consistent with the implementation in the field. In addition, overly managing personal data relating to “health data and information, biometric data, genetic data, sexual life/orientation, political views, children's data, personal financial data,” constitutes a personal right as a fundamental part of human rights, which is too far interfered with by the state or other parties.

(2) In addition, based on Article 36 PM Kominfo/MR 5/2020, there are two paragraphs relating to this matter, especially in relation to the possibility of opening access to Content of Communication.

- Paragraph (3), "Private ESO provides access to Content of Communication requested by Law Enforcement Officials in the event that the request is formally submitted to Private ESO."
- Paragraph (4), “Request for access to Content of Communication as referred to in paragraph (3) must attach: a. the basis of the authority of the Law Enforcement Officials; b. the purpose and objectives and interests of the request; c. a specific description of the type of Electronic Data requested; d. a criminal act that is being investigated, prosecuted, or on trial; e. a letter of determination from the head of the district court in the area where the Law Enforcement Institution has the authority. "
- Paragraph (5), " Private ESO provides access to Specific Personal Data requested by Law Enforcement Officials in the event that the request is submitted based on the provisions referred to in paragraph (4)."

The basic problem with the provisions of article 36 is that it is clearly contrary to the right to “be illegally interfered with personal, family, home or correspondence problems, and every citizen has the right to legal protection against interference”, and is prone to abuse, considering the level of public distrust over the issue of rights restrictions in law enforcement practices so far, the mechanisms to be complied with, including the public mechanism for complaints about abuse of power over private ESO. The three-part test also has not been strictly regulated in the legal mechanism in PM Kominfo/MR 5/2020, so practically, this arrangement opens up space for violations of human rights, especially the right to privacy.

(3) As stated earlier, the potential or concern of Permenkominfo No. 5/2020 will be misused to silence groups that criticize the government in fact, is wide open, this is because in the institutional architecture, there is no independent institution or body that has been formed, involved, or balanced with the perspective of the obligation to protect human rights.

(4) If an independent institution is not yet available, including the procedural mechanism, then it is clear that a strict three-part test may not be used as a framework for limiting human rights, including access to personal data.

(5) Basically, Permenkominfo is a derivative legal product of PP 71/2019, and it is known that PM Kominfo/MR 5/2020 is intended to carry out the "order" of the Government Regulation into ministerial-level operational regulations. The problem is, is Ministerial level regulation can be justified in regulating these restrictions seen from its legal product or form, as regulated in relation to PM Kominfo/MR 5/2020 which contains 65 keywords of "Termination of Access", both interpreted as access blocking and take down. The simplest example of this problem is the question in the power of the interpretation of "disturbing the public". What is the standard or measure, the authority to determine it, and the mechanism if the public feels that it is not part of what is called "disturbing the public".

(6) The orientation of such regulation in PM Kominfo/MR 5/2020 is how to organize legislation and regulations if the core and basic provisions are not sufficiently single and intact to regulate, as associated with the plan for the Personal Data Protection Bill. Current regulations are still rife, and the scope of the responsibilities is still not clearly understood.

Impact on Freedom of Expression

The most likely impact is the potential for large limitations on rights or freedoms, coupled with the possibility of disturbing the interests of private electronic system operators, especially if not for legitimate and disproportionate reasons. Meanwhile, contrary to the situation, it is known that the standard restrictions, especially the termination of access, are actually limited in providing guarantees for protection of rights, including the absence of an adequate mechanism for complaints (grievance mechanism), for example for public services.

PM Kominfo/MR 5/2020 may force all ESOs from various social media platforms, online-based service providers, to submit and accept domestic or local jurisdiction, both for content and the use of content in daily practices. In this context, it is clear that the direction of policies and regulations through PM Kominfo/MR 5/2020 actually makes Indonesia a region that requires registration of private ESO and submits itself to the domestic/national legal system. The legal framework for such obligation weakens the position of protection of all social media platforms, applications and other online service providers, especially to accept domestic/national jurisdiction over user data content and policies and practices. Such legal framework becomes a repressive instrument that would contradict or even violate human rights.

It is realized that in its development, the responsibility of ESO is not only borne by the state, but also the responsibility of various types of companies in the digital access industry which actually plays an important role in protecting, but on the contrary, it fails to protect the freedom of expression of internet access users. Internet service providers and telecommunications providers face legal pressure and intimidation by the government to comply with censorship and surveillance. Whereas in the context of private ESO, this does not mean that this responsibility is also released, but it is also the same as the important role in protecting freedom of opinion and expression, including recognizing and encouraging responsibility for taking actions that guarantee respect for human rights.

Therefore, considering that PM Kominfo/MR 5/2020, in the midst of a regulation that is so relaxed and will be very easy or prone to abuse, it is necessary to criticize the large and dominant role or authority of the ministry, specifically related to the public interest. Even though it has been authorized to normalize, as a process of restoring rights or access to electronic systems that have been closed, the closure or actions of blocking access, closing accounts and/or deleting content are a form of action that has the potential to eliminate human right and freedom itself.

Part 5:
Conclusions and recommendations

Conclusions

In general, the provisions of PM Kominfo/MR 5/2020 are closely related to the provisions of the right to privacy guaranteed by article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights.

Moreover, the right to internet access is a human right (internet rights or also known as digital rights). It is also often called digital rights access. Both have become very close in human life in this century, as the UN Human Rights Council has stated in its resolution (vide: Human Rights Council, Thirty-Second Session, Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, A//HRC/32/L.20, 27 June 2016).

In PM Kominfo/MR 5/2020, a number of legal conceptual frameworks for 'termination of access' are recognized, and this is actually a form of limiting human rights. Therefore, the termination of access or such restrictions must refer to a number of elements which must be declared as a three-part test, namely, first, prescribed by the law; second, legitimate aim; third, necessary. Such matters should be strengthened in the instruments and interpretation guidelines so that they are not far from the framework or standards of international human rights law. As stated in the UN General Comment 34, that the reason of 'necessary', as one of the basic elements of judgment for limitation, must be connected with the objective to achieve the protection function, 'must be appropriate to achieve their protective function'.

The problem is, the provisions in PM Kominfo/MR 5/2020 do not confirm the extent to which the interpretation of the "need" or "level of urgency" is consistent with implementation in the field. Excessive regulation actually interferes with personal rights.

In addition, PM Kominfo/MR 5/2020 opens a chance of multi-interpretation, especially as it is not strictly regulated about three-part tests, restrictions on rights, compliance mechanisms, including a public mechanism for complaints of abuse of authority over private ESO. The three-part test itself has not been strictly regulated in the legal mechanism in PM Kominfo/MR 5/2020, so practically, this arrangement opens up space for violations of human rights, especially the right to privacy.

With such provisions, the tendency that Permenkominfo No. 5/2020 will be misused to silence groups that criticize the government, is wide open, this is because in the institutional architecture, no

independent institution or body has yet been formed, to balance the power and obligations of protecting human rights. Finally, it is necessary to look in detail about the power of the interpretation of "disturbing the public". What is the measure or standard, the authority to determine it, and the mechanism if the public feels that it is not part of what is called "disturbing the public".

In this conclusion, it needs to be reminded that in a country that declares itself the constitutional state of Indonesia, Article 1 paragraph (3) of the 1945 Constitution, the state actions should be based on law, following the provisions or legal standards that can be accounted for. The most basic thing in a democratic rule of law is to guarantee the freedom and uphold human rights. The concern is that running a government without procedures and legal substance is far below standard, then it also results in contradictions. Such anti-democratic model will give birth to a sign of unsupervised government, especially regarding restrictions on internet access, giving birth to what is called authoritarianism that uses digital power in order to control technology as a means of protecting its interests, or digital authoritarianism.

Recommendations

There are four main points to consider as recommendations,

(1) To arrange legislation and regulations when the core and basic provisions are not sufficiently single and intact in regulating, as associated with the plan on the Personal Data Protection Bill. Current regulations are still rife, and it is not clear that the scope of the responsibilities is understood. This means that it requires a more comprehensive and protective arrangement.

(2) In this regard, it is hoped that the progressive efforts of the personal data protection law can become a common ground in determining the direction of the changes, including affirming the principles, mechanisms, procedures, channels of complaints about the restrictions imposed, given the urgency of the scope and level it is also necessary to affirm the legislation.

(3) The government also needs to ensure the protection of privacy or personal rights, including within the scope of private PSE, so that the integrated rules related to the laws governing the protection of personal data can become the master regulation.

(4) It is also necessary to ensure public involvement in policy development or the formation of relevant laws and regulations, even though legal products are part of the authority of the executive pillar.

* * *