ELSAM Research Report Summary

The Law on Electronic Information and Transaction is a threat to the freedom of opinion and freedom of expression; it is urgent to revise

A. Introduction

The rising number of Internet users, including the increasingly universal use of the technology in daily life, has resulted in a number of social, economic and political impacts. This situation has resulted in a new development, which is commonly understood by all stakeholders, about the importance of regulating the Internet. To the present, the biggest challenge in formulating regulations about the use of Internet technology is that legal and social consequences and sanctions are always one step behind the technological innovation. Thus, the Internet needs comprehensive regulations to prevent loss of function, and at the same time maintain efficiency and interoperability. Besides, regulation is also important to set out human rights principles to facilitate the protection of the rights of users, and formulating the responsibilities of all stakeholders.[1]

The contents of Law No. 11 of 2008, which is expected to be the guideline of all the needs mentioned above, in fact show the converse, as it is full with limitations to human rights, appearing in a number of prohibitions. These stipulations, especially those in the article pertaining to the criminal act of libel and defamation, namely Article 27(3) UU ITE, have resulted in scores of people being criminalised. Besides, the lack of regulation on Internet content has resulted in arbitrary blocking and filtering of the Internet. One can call it arbitrary as Indonesia as yet lacks regulation about a transparent and accountable procedure to block Internet content. This act is in essence a form of limitation to human rights, especially the right to obtain information, freedom of opinion and freedom of expression. The Minister of Communications and Information Regulation No. 19 of 2014 on the Handling of Negative Internet Content, intended by the government to respond to the lack of regulation, has in fact resulted in its own polemics. In addition to substantial issues in the material, formally, the regulation is also problematic for limiting human rights outside legislation, which is in opposition of Article 28J(2) of the 1945 Constitution, and various other regulations.

In light of the issues, especially the two main issues in the implementation of UU ITE: the massive use of the libel/defamation article, and lack of clear regulation about Internet content, ELSAM has concluded a study in order to find solutions to these two issues. This solution is intended to ensure integration of the principles of human rights protection in all policies about the utilisation of information technology. In reference to Resolution 20/8 of the United Nations Human Rights Council, protection of rights of persons while off line should also apply while they are on line. This protection is relevant to the right of freedom of expression, which applies regardless of the medium chosen. This is regulated in Article 19 of

[1] See Joanna Kulesza, *International Internet Law*, (London: Routledge, 2012).

the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights, which Indonesia has ratified through Law No. 12 of 2005.

B. Criminalisation of libel: a 'sneaky' rule creating a chilling effect for the freedom of opinion and freedom of expression

Interestingly one would not find any stipulations on the crime of libel or defamation when one reads the Academic Paper or the initial drafts of the Electronic Information and Transaction Bill. In the initial draft, prohibitions only specifically apply to computer crimes, pornography/pornographic acts and gambling. The phrase on the crimes of libel and defamation only appeared in a working meeting between the Special Committee on the Electronic Information and Transaction Bill and the government (Ministry of Information and Communication and Ministry of Law and Human Rights), on 29 June 2007. This meeting resulted in an agreement to add a criminal sanction to libel in the set of prohibitions. All fractions in the parliament were in agreement to the suggestion, as recorded in their final comments in the last session enacting the bill into law.

The second aspect to note is the harsh criminal sanctions to acts prohibited by UU ITE, including the crime of libel. In the bill, when suggested by the government to the parliament, the threatened sanction was not as harsh as it is now. The idea to raise the sanction was promoted by the police, in a hearing with the Special Committee. The police based their assertion on the requirement of an objective reason for detaining (which in Article 21 of the Criminal Administrative Code is stated that the objective reason for a detaining is a threatened sanction of more than 5 years of prison). Without the detaining, according to the police, the investigators will find it difficult to investigate cases related to the use of Internet technology. Thus, the police requested that all acts criminalised in UU ITE be threatened with sanctions of more than 5 years.

As a result, five years after the enactment of UU ITE, almost a hundred persons have to face the law, due to accusations of libel/defamation through electronic media. Not a few of them were detained, due to the harsh threatened sanction. Another surprising finding is the tendency to use Article 27(3) of UU ITE as a tool for revenge, due to the ease of which of having a person detained based on this stipulation. Furthermore, in a number of cases, there are imbalanced power relations between the complainant and the defendant. In general, the complainants are people wielding political power (heads of regions, bureaucrats), economic power (business persons) or those having strong social influence. The defendants, in turn, are mostly lacking power, and thus find difficult to obtain adequate access to justice. Besides the rising number of victims of the law, the media through which the victims committed their 'crimes' also become more varied: not only cellular phone messages, e-mails and videos, but almost all social media platforms.

This situation is caused, among many causes, by uncertainty of the elements of Article 27 (3) of UU ITE. Several elements such as "distributing", "transmitting", "allowing access", "libel and defamation" are not explained further, resulting in multiple interpretations leading to legal uncertainty. One element with vague definition and resulting in massive implication to

the implementation of article is the element of “distributing and/or transmitting”. The lack of explanation of how the distribution is done, and its purpose, results in the context of information dissemination and/or electronic transactions becoming very broad. Anything that is distributed electronically, regarded to have insulted a particular party, regardless of whether the distribution is done privately or public consumption, can be classified as “distributing and/or transmitting”.

As a result, electronic information intended for limited consumption (by two parties, by sending via private e-mail, Blackberry Messenger (BBM), and short message service (SMS)) can be classified as defamation. The onus for the definition of “libel and/or defamation” is placed on the subjective judgment of the victim, contributing to the massive abuse of this provision. An example is the criminalisation of a woman who was undergoing a divorce process, changing her marital status on Facebook from “single” to “married” with her new partner. Feeling hurt over her action, her soon to be former husband reported the woman on charges of defamation, and managed to have her detained for four months.

When the formulation of the legal norm is examined, Article 27(3) seeks to generalise the crime of defamation. The Criminal Code classifies various forms of the genus of defamation in one chapter, which consists of various species of the offense as set forth in Articles 310 to 320 of the Criminal Code. This generalisation results in the formulation in Article 27(3) of UU ITE being excessively broad and vague, resulting in easy abuse of the article. The limited explanation of Article 27(3) also leads to the use of the article being completely dependent the on understanding and preference of law enforcement officers. In practice, sometimes perpetrators of defamation through the electronic media are arrested not for violating Article 27(3) of UU ITE, but Article 310 of the Criminal Code instead. There are also cases that are subject to double jeopardy, where law enforcement officials accuse the defendant of violating Article 310 of the Criminal Code, after failing to prove a violation of Article 27(3) of UU ITE.

In the evidentiary process, Article 27(3) UU ITE is even more inconsistent to the evidentiary elements of Article 310 or Article 311 of the Criminal Code. In Article 27(3), the evidence is to focus on the spreading of electronic information, not on whether an element has libellous content or not. The parameter assessing whether a content is libellous or not is often overlooked in the process, despite the element having a major position in the relevant article. The absence of the obligation to prove the element of libel in the crime results in obscuration of the variations of defamation contained in Chapter XVI of the Penal Code. It has to be kept in mind that in these offenses are gradations of the material acts, which although quite similar, have differentiating elements.

Thus, the existence of Article 27(3) of UU ITE is in fact biased towards curbing freedom of opinion and expression, and not the original goal of maintaining the reputation of others. The ease of which one is reported on charges of defamation, as well as the tendency of law enforcement officers to make arrests and detention, has caused a chilling effect on the right to freedom of opinion and expression. Not infrequently, these restraints also lead to violation of other human rights, especially when one has to undergo detention.

C. The vacuum of law leading to arbitrary Internet content blocking has disrupted the freedom of expression and right to information

Recently, the Trust+ Positif program managed by Ministry of Communication and Information instructed Internet service providers to block Vimeo, a video sharing site classified as negative. Vimeo's placement in the negative list is supported by the argument that Vimeo contains a lot of pornographic content. As with the previous blocking moves by the ministry, the blocking of Vimeo immediately sparked controversy in the community, accusing of the ministry of taking rash action. The Ministry of Communication and Information is considered not to have performed in-depth studies of Vimeo's content, and not take into consideration of the negative implications of the blocking of Vimeo. While several Web sites made to circulate pornographic content are actually left alone by the ministry, Vimeo, which is widely used by Internet users to share copyrighted visual works, is blocked. The society argues that the benefit obtained through Vimeo actually outweigh the costs. Vimeo is an effective medium for sharing, with thousands of types of content therein. Pornographic content is only one negative content, compared to the thousands of positive and beneficial content. Thus, the blocking of Vimeo is considered as a solution that is not proportional to the problem trying to be solved.

During the process of discussing the Electronic Information and Transaction Bill (RUU ITE), the issue of blocking is considered to be closely related to the process of law enforcement, in the event of a commitment of an act prohibited by UU ITE. According to law enforcement officials, if the blocking is not done, the offender may alter or destroy evidence of crime. That is, the blocking action is interpreted as seizure of the evidence of a crime. In practice, the blocking of Internet content conducted by Internet service providers, at the behest of the Ministry of Communication and Information through the Trust+ Positive program, is directed against content assessed to have negative potentials according to the understanding of the government. The problem is that UU ITE does not clearly regulate the categorisation of content that should be blocked, for whatever reason, by which state institution, through what procedures, and what complaints mechanisms are available and recovery procedure provided.

Blocking of Internet content is allowed to be done by the state, as a form of restriction on the right to freedom of expression that is indeed allowed to be limited. However, the restriction must refer to the rules and principles of the restriction as set forth by the Constitution and international human rights law. Referring to Rundle and Bridling (2008), when a state takes action to block Internet content, the following aspects must be considered:

No.	Aspect	Explanation
1	Purpose	The earliest step to be taken in blocking and/or is to formulate the goal of the implementation of these measures.
2	Official statement of the action to be taken	Motivated by the purpose in number 1, the government must release a statement that it feels the need to take action in the form of filtering or blocking a certain content.
3	Specific	This aspect accommodates the need that the state ensures that

	explanation of the blocking/ filtering to be done	everyone is able to understand the law and can check that the restrictive measures are not taken arbitrarily.
4	Justification of screening measures	In this section, the aspects that justify the limiting action are laid out. In this context, both international law, national law, conventions that are widely accepted by society, and values and norms can serve as the basis for justification. Examples include national security, public order, public health or morals as stipulated in the provision of Article 19(3) of the International Covenant on Civil and Political Rights.
5	Elaboration of the problem happening and mechanisms for implementing such restrictions	In this aspect, the implementation procedure selected by the government in number 2 should be described thoroughly. This aspect is a form of transparency to the public in order to encourage monitoring to prevent abuses by the government. For example, explaining that when a Web site is blocked, Internet users will receive a message: i) showing why the filtering/blocking is occurring and the legal basis for the action, and ii) including a description of how Internet users can report problems and receive messages.

The practice in several countries shows that whenever there is a blocking of a particular Web page or site, the government will initially provide a warning. If not followed, the government, through competent authorities will block the Web pages or sites concerned, specifying clearly that the page in question is blocked, description of the reasons behind the blocking, and providing appeal mechanisms that can be taken by the content owner in case of an objection to the action. Several experts propose a judicial mechanism as a forum for content owners or service providers to be able to appeal the action taken by the government. Also being developed is an online mediation and arbitration practice, familiarly known as Online Dispute Resolution (ODR). The alternative remedy is similar to the existing dispute resolution mechanisms known to the public, only that the institution is specifically entrusted to resolve disputes online. As is common with the practice of mediation and arbitration in general, dispute resolution with this method tends to be faster and better able to accommodate the needs of the parties.

In general, the legal framework of blocking can be divided into two types: *first*, normative rules about the types of content that are prohibited and *second*, types of control mechanisms to be applied. However, wherever possible blocking of content is positioned as the last resort, after going through the stage of notification of the presence of illegal content. This notification is done either to the owner or content provider and the user of the Internet. Prohibited content can be marked and it is up to the Internet users to decide whether to continue to see the content or not.

Such a mechanism will encourage the intellectual development and maturation of Internet users in dealing with a wide range of Internet content, especially in determining which content is good and which is not. Such a mechanism also aims to avoid blocking the wrong targets, given the blocking mechanism used in the present continues to be based on keywords. In this mechanism, Internet content containing prohibited keywords are automatically inaccessible to the user. In fact, some of the Internet content containing the keywords does not actually possess negative aspects. On the other hand, some of the actually negative content does not use these keywords.

D. Conclusion and Recommendations

Law No. 11 of 2008 on Electronic Information and Transaction (UU ITE) is the legal instrument regulating all aspects of information technology and communications in Indonesia. It contains stipulations on electronic information and documents, electronic transaction, implementation of electronic certification, intellectual property rights and personal protection, wiretapping, criminal and administrative sanctions, and various other aspects related to the actors and objects in the field of information technology and communications. The regulations posed in UU ITE seem to be a mishmash of various legal norms, whose regulation could have been done in separate legal instruments. As a consequence, the aspects of regulation in UU ITE lack coherence between one article and another. To add to the problem, the many aspects that the law intends to regulate result in lack of in-depth understanding of the legal norms; mostly touching only the surface.

Due to the situation, at least two crucial problems arise with regard to the content of UU ITE. First, as a legislation that purports to be the basis for regulating the utilisation of Internet technology, UU ITE has failed to be a comprehensive guideline for the traffic of Internet content. The stipulations in UU ITE tend to focus on the criminalisation of material acts. Issues such as criminalisation of negative content have not been accommodated by the law, despite the pressing need for them. As a result, technical/ministerial regulations arise, which should not bear the burden of such level of legal norms.

Second, in the articles related to criminalisation, whose regulation is based on the awareness that the Internet cannot be separated from the potential of criminal acts, because the Internet facilitates traffic of human activities as in real life, as a result, the policy makers seem to have miscalculated the impacts of the formulations of legal norms when implemented in practice. This miscalculation later results in irregularities such as the harsh sanctions, duplication of crime, resulting in a flexible use of criminal sanctions that in turn results in suppression of the freedom of opinion and freedom of expression of citizens. It is ironic that while the law was created to uphold and protect human rights, it ends up violating human rights itself. In light of the conditions, ELSAM considers it important to immediately amend UU ITE, due to the following considerations:

1. A change of paradigm in policy making, which places the right to access the Internet as a part of human rights, and thus all principles of human rights protection must also be referred to in creating policies related to the Internet.

2. In the context of criminalisation, it is important to review all articles related to criminalisation, and remove all duplications of criminal violations in UU ITE, as they have been regulated in the Criminal Code. It is also important to consider the suggestion to remove the criminalisation of libel and/or defamation.

3. In relation to the practice of Internet content blocking, many parties have regarded this practice to be inherently flawed, as it has always resulted in greater impacts than the intended goals. In order to ensure the goal of protecting human rights, amendment to UU ITE has to specifically provide a space for content regulation that considers three elements to test: (i) the act of blocking content has to be regulated by a clear law, and can be accessed by everyone (the principles of predictability and transparency); (ii) the act has to be in fulfilment of one goal regulated in Article 19(3) ICCPR, namely to protect the rights and reputation of another party; national security or public order, or public health and morals (the principle of legitimacy); and (iii) the act has to prove that there is an urgency and done minimally (mechanism of the last resort) to reach the main goal (the principles of importance and proportionality). Besides, the authority to perform all these acts must be awarded to a body independent from political and commercial interests or institutions that do not have the authority, being impartial and not discriminative. There should also be protection from misuse, including possibility of complaint and restitution to misuse of blocking.

4. Along with the strengthening of the Indonesian Internet Governance Forum, it should follow that decision makers use the multi stakeholder approach in the process of decision making. In the model, not all decisions related to the Internet should be taken by a single party/authority, but all stakeholders, such as the government, business sector (service provider), technical groups, civil society organisations, including Internet users, should be involved.

Institute for Policy Research and Advocacy (ELSAM)
Jl. Siaga II No.31, Pejaten Barat, Pasar Minggu, Jakarta Selatan 12510
Tel. +62 21 7972662, 79192564, Fax. +62 21 79192519
e-mail: office@elsam.or.id, Web page: www.elsam.or.id, twitter: @elsamnews