ARTICLE:

INDONESIA: THE CONTROVERSY OVER THE BILL CONCERNING LAWFUL INTERCEPTION

By **Dr Edmon Makarim**, S.Kom., S.H., LL.M.[1]

Introduction

Recently, the Indonesian government has introduced a controversial Bill concerning lawful interception. The Bill regulates the interception of communications, and refers to a number of basic principles (relevancy, validity, secrecy and proportionality). The main legal provisions include (i) approval by a judge to authorize the interception (only suitable for qualified or certain types of crime, etc), (ii) interception procedures; (iii) building a national gateway for interception, (iv) reporting, registering or certification of interception devices, (v) a secrecy guarantee for the results of interception, (vi) e-system provider and/or operator liability, (vii) supervision; (viii) sharing the cost between the operator and law enforcement agencies. The aim of this article is to put lawful interception into context in Indonesia in order to enlighten the perspective as to how the Bill could reform Indonesian law in a beneficial way.

The discussion concerning interception is not new in Indonesia. Discussions had taken place during the years around 1990 when a number of laws defined the need for interception of communications in the interests of preventing crime, such as Law number 5 of 1999 concerning Psychotropic (Law of Psychotropic),[2] Law number 22 of 1997 concerning Narcotics (Law of Narcotics),[3] Law number 31 of 1999 concerning Corruption Eradication (Law of Tipikor),[4] and revision for Law number 3 of 1989 on Telecommunications, which became Law number 36 of 1999 (Law of Telecommunications),[5] whereby the provisions on the interception of communications were one of the important issues, because it can violate the confidentiality of the information in the communication. Further discussions occurred in the twenty-first century, with the promulgation of Law number 30 of 2002 concerning Corruption Eradication Commission (Law of KPK) which authorized the KPK to intercept and record communications; when PERPU number 1 of 2002 concerning Terrorism Eradication (Law of Terrorism)[6] had passed, giving authority to

1 *The author thanks Wesky Putra Pratama, S.H. and Dionysius Damas Pradiptya, SH., both of which are Assistant Researchers at the Legal Research Institute for Technology Law, Faculty of Law University of Indonesia (FHUI), (Lembaga Kajian Hukum dan Teknologi/LKHT-FHUI), for their help with the English translation of this article.*

2 *Article 55 of the Law of Psychotropic states that other than those stipulated in Law No. 8 Year 1981 on the Law of Criminal Procedure (State Gazette Year 1981 Number 76, Additional State Gazette Number 3209), a Republic of Indonesia police investigator may: (a) conduct an investigation using covert techniques, (b) open or inspect every shipment of goods by mail or other communication devices that allegedly has links with a case involving substances that are part of the investigation, and (c) intercept telephone conversations and/or other electronic means of telecommunication by people that are suspects or where they discuss alleged problems associated with psychotropic crime. The period of interception may last for no longer than 30 (thirty) days. The use of such techniques can only be made on written orders of the Chief of the State Police of the Republic of Indonesia or his appointed officials.*

3 *Article 66(2) of Law Number 22 Year 1997 concerning narcotics provides that Republic of Indonesia State Police Officers who are assigned to investigate narcotics and criminal investigations, are authorized to intercept telephone conversations or other telecommunications equipment. The period of interception may last for no longer than 30 (thirty) days. This law was revised with the promulgation of Law number 35 Year 2009 concerning Narcotics.*

4 *Article 26 provides investigators with the authority to intercept communications.*

5 *Article 40 of the Telecommunications Act states that every person is prohibited from intercepting information transmitted through telecommunications networks in any form. The definition of interception is to install equipment or conduct activities on the enhancement of telecommunication networks for the purpose of obtaining information without authorization. The information possessed by a person is a personal right that must be protected so that intercepting information should not be conducted without lawful authority. Article 42(2) provides that for the purposes of the criminal justice process, telecommunication service providers can record information sent and/or received, and can provide information upon the written request of the Attorney General and/or the Chief of State Police of the Republic of Indonesia for certain offenses, or to investigators when investigating a specific crime in accordance with applicable law.*

6 *Article 31(1) provides that once there is sufficient evidence as intended in article 26(4), the investigator is entitled: (a) to open, examine, and confiscate letters and submissions by mail or other delivery service that has links with terrorist crimes that are being investigated; (b) intercepting telephone conversations or other communications equipment allegedly used to prepare, plan, and commit crimes of terrorism. Interception can only be on the orders of the Chief Court for a maximum period of 1 (one) year.*

investigators to intercept communications; when discussing law number 18 of 2003 concerning Advocates (Law of Advocates),[7] in which advocates sought immunity from interception, and in the year 2007 with Law number 21 of 2007 concerning Eradication of Human Trafficking (Law of Human Trafficking),[8] which also gives investigators the authority to intercept communications.

Debate and discussion continued in 2003 and 2006 at the time of filing a judicial review to the Constitutional Court in respect of article 12(1)(a) of Law number 30 of 2002[9] concerning the Corruption Eradication Commission (Law of KPK),[10] especially regarding the KPK's authority in the interception process, because there were no formal provisions for its implementation based on law. In some cases, it was alleged that interception was used by the KPK for the purposes of entrapment. Furthermore, Constitutional Court Decision Number 006/PUU-I/2003[11] (in which the petitioners were two of the Public Election Commissioners who had their communications intercepted by the KPK) and Number 012-016-019/PUU-IV/2006, set out a mandate to make changes to the law of KPK or to adjust the procedures for interception in its own laws and regulations. Below is a summary of the main points from the decision of the Constitutional Court.

1. That the decision of the Constitutional Court Number 006/PUU-I/2003, on its legal considerations when deciding the petition for article 12(1)(a) Law of Commission, stated, amongst other things, "... to prevent possible abuse of authority for wiretapping and recording, the Constitutional Court believes is necessary to stipulate a set of regulations governing the conditions and procedures for wiretapping and recording." [The word used in Indonesian is "penyadapan" which was originally translated into "wiretapping" rather than "interception"]. The legal considerations are in accordance with the provisions of article 32 of Law number 39 of 1999 concerning Human Rights which states "Independence and confidential correspondence relationships, including communication by electronic means must not be disturbed, except by order of a judge or other legitimate power in accordance with the provisions of legislation." In Decision Number 006/PUU-I/2003 it was made clear that the interception and recording of a conversation is a restriction of human rights, where such restrictions can only be carried out by legislation, as provided by article 28J(2) of the 1945 Constitution. The law further stipulated that it is necessary to consider, among other things, who is authorized to issue orders to intercept and record conversations, and whether the order can only be issued after the beginning of sufficient evidence is obtained, which means that the purpose is to refine evidence, or whether the purpose was to obtain sufficient evidence from the beginning. In accordance with the requirements of article 28J(2) of the 1945 Constitution, it must be regulated by law in order to avoid the misuse of authority that violate human rights.

2. That based on the description above, and after reading the postulates submitted by the petitioner in accordance to the petition to review for article 12(1)(a) of Law of KPK, there are no "different constitutional reasons" in the postulates, so the petitioner's petition regarding the unconstitutionality of article 12(1)(a) of Law of KPK is not reasonable.

3. That although the petitioner's petition was not reasonable enough, article 12(1)(a) of Law of KPK concerned restrictions on human rights, thus in accordance with article 28J(2) of the 1945 Constitution, the terms and procedures for interception should be determine by law, whether

7 *Article 19(2) of Law number 18 of 2003 concerning advocates states that the advocate has the right to confidentiality with clients, including the protection of files and documents against the seizure or inspection and protection against the interception of communications of the advocate's electronic communications.*

8 *Article 31(1) of the Law of Human Trafficking provides that where there is sufficient evidence, authorized investigators may intercept telephone or other communications equipment allegedly used for preparing, planning, and committed the crime of trafficking in persons, and section (2) states that interception may only be conducted with the written permission of the court chairman for a maximum period of 1 (one) year.*

9 *'In conducting its duty for inquiry, investigation, and prosecution as intended in article 16(e), the Coruption Eradication Commission is authorized to intercept and record conversations'.*

10 *Article 12(1)(a): In conducting its duty for inquiry, investigation, and prosecution as intended in article 16(e), the Coruption Eradication Commission is authorized to intercept and record conversations.*

11 *Case Number 006/PUU-I/2003 page 104: "to prevent the possibility for abuse of authority for wiretapping and recording the Constitutional Court believes is necessary to stipulate a set of regulations governing the conditions and procedures for wiretapping and recording in question." Later in a dissenting opinion by Judge Constitution Maruarar Siahaan, SH, at page 116-117: "The presence of a super body, which with extraordinary powers, can be given the authority to record telephone conversations of people who are alleged to be corrupt, but there must be a clear oversight in the laws and regulations governing the minimum requirements that must be met in such a way that did not result in arbitrariness. Although this was seen as a threat to human rights, in our opinion, it is sufficient just to recommended the government a regulation which gives a clearer limits and juridical conditions for such extraordinary authority."*

by amending the Law of "KPK" or by introducing new laws.

In 2010, the legal issues on the interception of communications was debated again, because the activities of the KPK's policies on interception was presented and played in the Constitutional Court, which was open to the public and free to broadcast. This is because two Commissioners of the KPK (who were suspected of abuse of their power by the Indonesian police) petitioned for the constitutional examination of article 32(1)(c) of the Law of KPK, which states that when the Chairman of the Corruption Eradication Commission (KPK Chairman) became a suspect in committing a criminal offense, they shall be suspended from their position as chairman.

This case was a cause célèbre, because of the presentation and playing of calls in the Constitutional Court between an accused and his lawyer that were intercepted by KPK. The interception results that were played in court were neither appropriate nor proportional. A great deal of discussion took place in the media, and has had an effect on the drafting of the Bill relating to Lawful Interception, which had actually been drafted by the government before the case. Because of the mistrust of the law enforcement agencies (judges, police, prosecutors, and lawyers) and because of the public interest, some argue that it is not necessary to regulate the interception of communications, because any such regulation will weaken the authority of the KPK. This argument is founded by the belief that in fact, interception is the most effective way in dealing with cases of corruption. On the other hand, others express the need for regulation by law, because any restriction on human rights should be regulated by law. There is also an argument that interception under KPK should not require permission of a judge, because it will endanger the secrecy in conducting interceptions, and the court infrastructure itself seems not ready to handle the task. It is considered that interception of communications by KPK can be adequately regulated by self regulation.

The concern over the interception of communications lead to a judicial review of article 31 of Indonesian Law number 11 of 2008 concerning Information and Electronic Transaction (UU-ITE), which served as the foundation for the establishment of the government draft regulation concerning lawful interception.[12] The applicant claimed that article 31 was an unconstitutional provision because it gave a mandate to the government to write regulations that regulate things that should be established by law. Sections (1) to (4) of article 31 are set out below:

(1) A Person is prohibited from intentionally and without right or unlawful conduct to carry out interception or wiretapping of Electronic Information and/or Electronic Records in certain Computers and/or Electronic System of other Persons.

(2) A Person is prohibited from intentionally and without right or unlawful conduct from intercepting the transmission of nonpublic Electronic Information and/or Electronic Records from, to, and in certain Computers and/or Electronic Systems of other Persons, whether or not causing alteration, deletion, and/or termination of Electronic Information and/or Electronic Records in transmission.

(3) Interception intended by section (1) and section (2) shall be interception carried out in the scope of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institutions as stated by laws.

(4) Further provisions on procedures for interception as intended by section (3) shall be regulated by Government Regulation.

The meaning of interception

The original words used in the Indonesian Law for Corruption explicitly cites the word "wiretapping" in brackets beside the Indonesian word "penyadapan". The term "penyadapan" had already been used as a generic word in the Indonesian language in the context of obtaining access to the content of communications, and actually refers to the

12 *In the Indonesia hierarchy of laws, government Regulation (Peraturan Pemerintah, lower level provisions) should be derived from relevant Laws, the upper level. It is common in Indonesian drafting that the detailed mechanism of the legal norms which are set in the law are the subject of a detailed government Regulation. From this point of view, there is no need for a special law concerning interception, because it can be regulated by a government Regulation because article 31 of ITE only refers to the mechanism and procedures between law enforcement agencies.*

13 *In the context of the Indonesian legal system, the interpretation of any conduct is considered as unlawful conduct if the conduct is substantially against the law.*

interception activities in telecommunication networks.[14] The use of the term 'wiretapping' originated from conducting surveillance over physical wires. *The Oxford English Dictionary* (electronic version, v.4) refers to interception at 1.a as 'The action of intercepting; seizing or stopping (a person or thing) in the way; the fact of being intercepted or stopped; an instance of this.' Thus 'interception' covers both physical things (such as letters) and digital data.

To be valid, intercepted evidence must fulfilled pre requisite requirements such as a legitimate interest, based on a warrant (lawfully obtained), relevant, proportional, confidential and valid in order to have admissibility in legal proceedings.

General principles for interception

Consistent with the Universal Declaration of Human Rights (Declaration), the Indonesian Constitution incorporates many articles about the protection of human rights, particularly about freedom of communication and privacy.[15] Furthermore, the protection of human rights are also described in Law No. 39 year 1999 concerning Human Rights. (For which, see article 28F, 28G(1) and article 28J of the Constitution of Republic of Indonesia 1945[16] and article 32 of Law of Human Rights). Article 28J of the Constitution (similar to articles 28 to 30 of the Declaration) expressly provide that the human rights set out may only be limited for the sole purpose of securing recognition and respect of the rights and freedoms of others and meeting such requirements as morality and public order in a democratic society. It should be noted that parallel with the freedom of communication between the parties in the context of private communications, the confidentiality of information should also be protected. Intercepting without the law right to listen (eavesdropping), and any form of wiretapping or interception should be prohibited by law, with the exception that such activities can take place within the law to protect the public interest.

It is necessary to observe that prior to the passing of the Law of ITE, the legal provisions for the interception of communications were provided under the Law of Telecommunication. The telecommunication law differentiates the interception process and the recording information as two different things, as stipulated in article 40 and article 41:

> Article 40
>
> Every person is prohibited from conducting wiretapping of information that is transmitted through telecommunications networks in any form.
>
> Article 41
>
> In order to prove the truth, the use of telecommunications facilities at the request by users of telecommunications services, the providers are obliged to record the use of telecommunications facilities used by the users, and to record the information in accordance with laws and regulations.

The provisions of article 40 clearly states that wiretapping is prohibited.[17] The only conduct that is permitted is set out in article 42, where recording is based on a request from a law enforcement agency. Therefore, law enforcement agents are not permitted to intercept or record without authority. The need to cooperate with communication operators is set out in article 43, which provides that any action must not violate the obligations of the providers and aims to keep the confidentiality of the information in communication:

> Article 42
>
> (1) Providers of telecommunications services shall keep confidential information that is sent and/or received by customers of telecommunications services through telecommunications networks

14 *See the elucidation of article 26 of the Law of Corruption, which provides: "Kewenangan penyidik dalam Pasal ini termasuk wewenang untuk melakukan penyadapan (wiretaping)", translated as "The authority of the investigator in this Article, including the authority to conduct wiretaps (wiretapping)".*

15 *The Indonesian Constitution does not use the word 'privacy' as the terminology, but it uses the words 'personal dignity' and 'personal life'.*

16 *Article 28F Constitution of the Republic of Indonesia (NRI) 1945: "Every person has the right to communicate and obtain information for personal development and social environment, and the right to seek, obtain, possess, store, process and convey information using all types of channels available. (Second amendment); and article 28G (1), "Everyone is entitled to the protection of personal self, family, honour, dignity and property under its power, and is entitled to a sense of security and protection from the threat of fear to do or not do something that is right" (second amendment), and article 28J(1) of the Constitution of NR 1945, "Everyone must respect the human rights of others in an orderly society, nation and the state"; and section (2) "In carrying out the rights and liberties, every person shall be subject to restrictions set forth by laws with a view solely to ensure the recognition and respect for rights and freedoms of others to meet the demands of justice according to considerations of morality, religious values, security and public order in a democratic society". (Altered in the second amendment of the 1945 Constitution).*

17 *The word "wiretapping" is used here instead of "interception", because it was officially used as the terminology by the Telecommunication Law and other existing laws before the Law of ITE was promulgated.*

and/or telecommunication services.

(2) For the purposes of the criminal justice process, telecommunication service providers may record the information sent and/or received by telecommunication service providers and provide the information as needed, by:

a. Written request from General Attorney and/or the Chief of Indonesian Police for specific criminal acts;

b. Request from investigators for specific criminal acts in accordance with applicable law.

(3) The provisions on request and granting procedures to record the information as intended by section (2) shall be regulated by Government Regulation.

Article 43

Recorded information given by providers to users of telecommunication services as intended by article 41 and for the interest of the criminal justice process as intended by article 42 section (2) did not violate the provisions of article 40.

The procedures to request and the granting of an order to record information are set out in article 87, article 88, and article 89 of Government Regulation number 52 of 2000 concerning the provision of telecommunication providers:

Article 87

For the purposes of the criminal justice process, telecommunication service providers may record the information that is sent and/or received by telecommunication service providers and may provide the necessary information by:

a. Written request from General Attorney or Chief of Indonesian Police for specific criminal acts;

b. Request from investigators for specific criminal acts in accordance with applicable laws and regulations.

Article 88

The request for recording the information as intended by article 87 submitted in writing and legitimate to telecommunication service providers with a copy to the Minister.

Article 89

(1) A written request to record the information as intended by article 88 must contain at least:

a. Objects that were recorded;

b. Recording period; and

c. Period of time to report the results.

(2) Providers must meet the request to record the information as intended by section (1) no longer than 24 hours after the request being received.

(3) In case the recording was not technically possible, the telecommunication service providers as intended by section (2) are required to notify the General Attorney, Chief of Indonesia Police, and/or Investigators.

(4) Notification as intended by section (3) shall be submitted no later than 6 (six) hours after the request as intended by section (1) being received.

(5) The result of recording the information as intended by section (2) conveyed in confidentially to the General Attorney or Chief of Indonesia Police and or Investigators.

In 2006, Ministerial Regulation 11/PER/M.KOMINFO/02/2006 of 2006 was issued by the Minister of Communications and Information concerning the Procedures for Tapping in order to enable the authorities to obtain a direct access to the operator to enable the authorities to conduct interception

directly.[18] In terms, the provisions in this Regulation could be said to be an umbrella for the law enforcement agencies to conduct legitimate acts of interception by remote conduct through their own equipment, but the provisions of the Regulation contradicted the requirements of the Telecommunication Law, as outlined above, which distinguishes between interception and recording. This Regulation was susceptible to judicial review, because the Minister does not have the authority to make a regulation which conflicts with the law. It could be seen as a mechanism to lend legality to the interception of communications by the Minister:

Article 1(7). Penyadapan Informasi adalah mendengarkan, mencatat, atau merekam suatu pembicaraan yang dilakukan oleh Aparat Penegak Hukum dengan memasang alat atau perangkat tambahan pada jaringan telekomunikasi tanpa sepengetahuan orang yang melakukan pembicaraan atau komunikasi tersebut.

Article 1(7) of Ministerial Regulation number 11 of 2006 states that the purpose of the wiretapping (as a surveillance activity) was to listen, record, or note a conversation conducted by law enforcement agents by installing addition tools or devices on the telecommunication networks without the knowledge of the person who makes the conversation or communication itself. However, the act of interception in any form is prohibited by article 40 of the Law of Telecommunications.

Article 1(8). Penegak Hukum adalah aparat yang diberi kewenangan untuk melakukan penyadapan informasi berdasarkan undang-undang yang memerlukan adanya tindakan penyadapan informasi.

Article 1(8) provides for the scope to initiate interception measures that are narrower than the provisions provided for in article 42(2)(a) of the Law of Telecommunication, which not only provides specific criminal acts that give authority to the investigators under the law, but also allows the General Attorney and Chief of Indonesian Police to ask for a conversation to be recorded within the scope of specific criminal acts which attracted imprisonment of 5 (five) years and over, for life or death sentence.

Article 1 (9). Penyadapan informasi secara sah (Lawful Interception) adalah kegiatan penyadapan informasi yang dilakukan oleh aparat penegak hukum untuk kepentingan penegakan hukum yang dikendalikan dan hasilnya dikirimkan ke Pusat Pemantauan (Monitoring Center) milik aparat penegak hukum.

Article 1(9) provides that lawful interception means the interception of information activities conducted by law enforcement agents for the purposes of law enforcement that are controlled and the results sent to the Monitoring Center that belong to the law enforcement agencies. In contrast, the provisions in the Law of Telecommunications only provides authority to request the operator for help with the recording, and there is no authority to intercept remotely.

Article 3: Penyadapan terhadap informasi secara sah (lawful interception) dilaksanakan dengan tujuan untuk keperluan penyelidikan, penyidikan, penuntutan dan peradilan terhadap suatu peristiwa tindak pidana.

Article 3 of the Regulation provides for lawful interception in order to fulfill the purposes of inquiry, investigation, prosecution, and trial for criminal acts, while the provisions of article 42(2) of the Law of Telecommunications provides for lawful interception in order to fulfill the purposes of investigation, prosecution, and trial. Article 42 does not mention the inquiry stage. It is clear that article 42 does not allow interception at the inquiry stage, but only at the investigation stage and beyond.

The Regulation also provides for the devices and equipment to be used in accordance with international standards (Chapter IV), a valid technical mechanism (Chapter V), the existence of the center for monitoring (Chapter VI), the monitoring team (Chapter VII), the requirement to guarantee confidentiality (Chapter VIII) and the sharing of costs between the operator and law enforcement agencies (Chapter IX). The most interesting aspect of this Regulation is that the interception may by conducted from a single gate that can be exploited jointly by all

18 *In many legal provisions of laws, the word "wiretapping" was common terminology (especially based on the Telecommunication Law), until Ministry Regulation (No.11 Years 2006 concerning Lawful Interception) used two words in one sentence in article 1(9) and the word "interception" has become the new terminology. The Law of ITE also saw the same change. The definition of interception is now broader than "wiretapping".*

law enforcement agencies, as reflected in article 13, in that the Monitoring Centre serves as communications gateway for law enforcement agencies to conduct lawful interception.

The most important issue that should be underlined was whether the Minister had the authority to remove the prohibition on the interception provisions in the Law of Telecommunications. From the legal point of view, it is debatable whether the Regulation serves to provide for lawful interception.

In practice, the telecommunication operators want to reduce the cost of assisting law enforcement agencies, but the operators are in a difficult position because they are vulnerable to an action in tort from their users, based on the provisions of article 1365 of the Indonesia Civil Code, where the operator assists in enabling an enforcement agency to commit unlawful acts by facilitating access to their own network.

Ideally, the retrieval of electronic information should only be recognized by the court if the evidence had been lawfully obtained, and the law enforcement agencies should ensure the integrity of the data. But law enforcement agencies need an opportunity that can allow them to perform remote interception. There is no legal basis in the Law of Telecommunications for this. Remote interception can only be considered legitimate if it is carried out under the provisions of the Law of ITE.

Analysis on the interception provisions of recent laws and regulations

Observing how interception is listed and arranged in Indonesian laws, there is a diversity of provision. Below is a summary of the present position in Indonesia:

a. Wiretapping or interception is an activity that is prohibited unless conducted for the interest of law enforcement, while interception that is conducted in the interests of national security are not covered.[19]

b. The authority for interception is granted in respect of a specific criminal acts, not for all categories of crime.

c. Although some of the laws state that interception can be conducted in the inquiry stages, most of the laws provide that it must be conducted after obtaining sufficient evidence.

d. There is a diversity in the maximum period of conducting interception (from 1 month, 3 months to 1 year). That is, there are many different provisions in different laws concerning the period of interception. One law provides for 1 month, but other laws provide for 3 months, and another law sets out a period of up to 1 year.

e. Interception in general requires a warrant from a judge because it is a form of forceful measures in obtaining access to and the recording of information (except for the KPK, which are not clearly regulated: it is debatable whether they need to obtain an interception warrant, but the legal provisions do not expressly exempt the requirement for judicial authority).

f. Interception that has been regulated requires the involvement of the telecommunication operators or telecommunication service providers to undertake the recording (for which see the Law of Telecommunications); however, remote interception by law enforcement agencies is not controlled by judicial authority.[20]

g. The obligations for procedures relating to the regulation of interception are included in the Law of Telecommunications[21] and in the Law of ITE. In the context of telecommunications, Ministerial Regulation number 11 of 2006 provides for the direct interception of communications to be conducted by law enforcement agencies, and for such activities to be funnelled through the

19 *Article 40 of the Law of Telecommunication: "Every person is prohibited from conducting wiretapping of information that transmitted through telecommunications networks in any form".*

20 *Article 41 Law of Telecommunication: "In order to prove the truth, the use of telecommunications facilites at the request by users of telecommunications services, the providers are obliged to record the use of telecommunications facilites used by the users, and recording information in accordance with laws and regulations."*

21 *Article 42 Law of Telecommunications:*
(1) Providers of telecommunications services shall keep confidential information that is sent and/or received by customers of telecommunications services through telecommunications networks and/or telecommunication services.
(2) For the purposes of the criminal justice process, telecommunication service providers may record the information sent and/or received by telecommunication service providers and provide the informatin as needed, by:
a. Written request from General Attorney and/or the Chief of State Police of the Republic of Indonesia for specific criminal acts;
b. Request from investigators for spesific criminal acts in accordance with applicable law.
(3) The provisions on request and granting procedures to record the information as intended by section (2) shall be regulated by Government Regulation.

gateway and monitoring center.

h. Any interception should be conducted with a view to provide for the protection of privacy and the integrity of data, as has been mandated by the Law of ITE.[22]

Whether it is necessary to have a special law to regulate interception

By considering the essence of the decision by the Constitutional Court in 2006, it could be seen that the mandate has been executed by the existence of Law of ITE, which provides that interception is an activity that is prohibited unless conducted by law enforcement agents for the purposes of law enforcement. Furthermore, the Law of ITE has been delegated the technical implementation in the form of government Regulation, and the presence of Ministerial Regulation number 11 of 2006 cannot necessarily be said to conflict with the mandate.

However, the legality of Ministerial Regulation number 11 of 2006 is weak, because it is contrary to the norms outlined in the Law of Telecommunications. It can be said that the Ministerial Regulation does not have a power in the form of a set of umbrella provisions, because the state administration has no authority to waive the norms of the law. The consequence it that evidence adduced in legal proceedings that come from actions undertaken under the authority of the Ministerial Regulation will not necessarily be admissible, and it gives an opportunity to the wronged party to initiate legal action against the relevant law enforcement agency.

The introduction of article 31 of the Law of ITE and the government draft Regulation Concerning Interception for law enforcement agents (lawful interception) should be considered as a better alternative to provide for the legitimacy of interception. However, at the time of writing, a petitioner for a constitutional review of article 31(4) of Law ITE has made some changes, because the Constitutional Court declared, by Decision No.5/PUU-VIII/2010 dated 2 February 2011, that the provision of article 31(4) of Law No.11 year 2008 on Electronic Information and Transaction Act (law-ITE) concerning the provision of detailed provisions on interception in relation to the government Regulation, is unconstitutional. Therefore, article 31(4) no longer has binding legal force. As a consequence, it is necessary to consider concentrating the legislative effort to provide for the regulation of interception by means of a law (Undang-undang).

Furthermore, regarding Indonesian Law number 1 of 2006 concerning Mutual Legal Cooperation in Criminal Matters (Law of MLA), this law clearly provides for the cooperation between states to exchange electronic information or electronic records (or both) for the purpose of proving a crime. But it becomes a significant issue if interception is generally carried out under the auspices of judicial oversight in other states across the globe, but Indonesia has no judicial oversight at all. It could be said that the global standard for criminal procedure should be considered as the best practice in criminal procedure. In general, interception should only be conducted under the auspices of judicial oversight.

The KPK's Commissioners do not want to be required to obtain a warrant from a judge to conduct interception of communications. It is claimed that such a requirement acts as a barrier to interception. The KPK commissioners are of the opinion that it is sufficient that they regulate regulate their own procedures internally, via the Chairman. The KPK has the authority to conduct interception and to record, but there are no provisions regarding their procedures. There is no explicit requirements to request the authority of a judge to conduct an interception. In comparison, Constitutional Court decision for KPU case in 2004 (Case No.012-016-019/PUU-IV/2006) required the Commission to amend the Law of Corruption Eradication Commission or to make the new laws to specifically regulate the interception of communications. This is a controversial issue in Indonesia. The provisions concerning interception in the Corruption Law remain, and there is no revision or a proposal revision at the time of writing.

22 *Article 43 Law of ITE*
(1) In addition to Investigators of the State Police of the Republic of Indonesia, certain Civil Service Officials within the Government whose scope of duites and responsibilites is in the field of Information Technology and Electronic Transactions shall be granted special authority as investigators as inteded by the Law of Criminal Procedure to make investigation of criminal acts of Information Technology and Electronic Transactions.
(2) Investigation of Information Technology and Electronic Transactions as intended by section (1) shall be made with due regard to privacy protection secrecy, smooth public services, data integrity, or data entrirety in accordance with provisons of laws and regulations.
(3) Searchs and/or seizures of electronic systems suspiciously involved in criminal acts must be carried out with the permission of the local chief justice of the district court.
(4) In carrying out search and/or seizures as intended by section (3), investigators are required to maintain the public service interests.

Conclusion

From the foregoing, a number of conclusions can be drawn. First, interception remains a prohibited act because its violates human rights (inviolability of communication), particularly violation of privacy in communications. The interception of communications can only be carried out in order to protect the wider legal interest in accordance with the law. Therefore, interception should be based on the law, that in turn should eliminate the opportunity of law enforcement agents to abuse their power.

The regulation of interception should include provisions for the control of intercepting oral communication in private spaces (surveillance and monitoring such as bugging) which is not regulated.

A concern of law enforcement agencies should be to ensure that the evidence obtained as a result of interception and surveliance is admissible in legal proceedings. This implies that all such activities should be conducted within the law and under judicial oversight.

Indonesia might benefit from the existence of the National Interception Center. The Centre functions as a gateway that is necessary in order to protect and to balance the interests between the telecommunication providers and the law enforcement agencies in the implementation of good electronic governance in the interests of protecting the public interest. The National Interception Center has the capability to make the interception process by law enforcement agents become more efficient and effective by accommodating all the information and communications technology in the future.

Finally, the government Draft Regulation has the capability of making the interception of communications became more civilized, and in accordance with the best practices from other nation states. This is important in the context of mutual legal assistance in criminal law, especially when electronic evidence must be admissible for it to be effective, which is in turn based on the integrated criminal justice system which is accepted as a common norm in democratic nation states. At the very least, the government Draft Regulation Draft is capable of making the face of the criminal justice system better for the future.

Dr Edmon Makarim is a Lecturer and Researcher in Cyber Law (Telematics Law) and Intellectual Property Rights, at the Faculty of Law, University of Indonesia (FHUI), and a Senior Researcher for the Legal Research Institute for Technology Law, Lembaga Kajian Hukum dan Teknologi (LKHT-FHUI).

http://staff.ui.ac.id/edmon

edmon@ui.ac.id

