Research Article

The Problems Of Sending Spam E-Mails To People In Indonesia

Arus Reka Prasetia[1], Rozahi Istambul[2]

[1]reka.prasetia@widyatama.ac.id

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

ABSTRACT: The Internet is part of the development of technology, where the internet provides many impacts, both positive and negative. Currently, privacy issues on the internet have also become a complicated legal issue, this is due to quite several privacy-related issues, but not all countries in the world manage privacy issues on the internet. As a means of communicating the Internet has introduced e-mail that provides convenience and practicality. But in its development e-mail has an adverse impact on its users in the form of e-mail spam. In terms of its actions, sending spam e-mail is quite a disadvantage, even violate privacy. Some countries have also set it to one type of cybercrime (cybercrime). This article will discuss e-mail spam in Indonesia, how the legislation in Indonesia sees the action of this spam e-mail, is there any possibility of spam e-mail is criminalized as a cybercrime. The article will also look at how spam e-mails violate privacy and review and analyze internet privacy settings in Indonesia in relation to the criminalization of spam e-mail.

Keywords: Spam e-mail, Cybermedia, Cybercrime.

1. Preface

The internet has brought about enormous changing effects for humans. All human activities have turned into digital activities on the internet. As part of the convergence of telematics, there are three important elements, namely telecommunications, media, and informatics. The internet has become a different world from the physical world that has been known every day, where almost all matters related to violations or even crimes cannot be touched by the positive laws that apply in the physical world every day. For this reason, the world of the internet and all the activities involved in it are often referred to as cyberspace and the legal rules that govern it are called cyberlaw.

The use of e-mail as the convenience provided by the internet also has the opportunity for abuse, wherein the use of e-mail, spam e-mail is also known. Spam e-mail, referring to the definition of the word spam, is an e-mail that contains "junk" content or is irrelevant to the needs of its users (Anonymous, 2015, www.techterms.com). Sending large amounts of spam e-mails, of course, will cause inconvenience or even loss because not infrequently the content of spam e-mails contains links that direct e-mail recipients to click on certain links that contain dangerous content or can make the recipient of the e-mail a victim of crime cyber. In Indonesia, spam e-mail has also been a problem in using the internet for a long time. In fact, in 2019, based on the release of data from Kaspersky Lab, Indonesia is ranked seventh as the country that sends the most spam with a total of 3.1 percent (Andesma, 2020, www.techno.okezone.com).

In Indonesia, the act of spamming or sending spam e-mails is related to a violation of the privacy of internet users. Even though ethically on the internet (netiquette), spam e-mail is considered an unethical act, of course, netiquette has not been able to decisively reduce the spread of spam e-mail. This can be a weakness of cyberlaw enforcement in Indonesia, through the Law on Electronic Information and Transactions (UU ITE). Then the spam e-mail does not only talk about the problem of privacy violations on the internet but how then the spam e-mail can lead or mislead internet users to various content on the internet that is dangerous or will be able to harm e-mail recipients, both psychologically and materially, so that in this context it should be cyberlaw in Indonesia can regulate it strictly. In some countries, spamming has become a part of cybercrime, even in Australia, special regulations regarding spamming have been regulated in the Spam Act 2003. This happens because privacy is something that cyberlaw needs to protect as well. Privacy in this condition is also related to the understanding that every person on the internet also has the right not to be disturbed.

Although in some countries spam e-mail has been classified as a cybercrime, in Indonesia it has not been regulated in the relevant laws and regulations. For this reason, based on the above background, the focus of this article is on spam and cybercrime, which raises several problems, namely whether spam e-mail can be defined as cybercrime and how best to regulate spam e-mail in relation to privacy protection in criminal law cyber in Indonesia.

2. Research Methods

The approach used is the normative approach method, on the grounds that this research intends to analyze the legal doctrine and legal issues of spam e-mails to then provide a perspective on the norm system, whether it can be regulated in such legal norms, especially cyber-criminal law. This article uses a Comparative Approach to look at the settings for spam e-mail in several countries with related regulations.

Primary data becomes data obtained from laws and regulations regarding cyberspace, principles, as well as regulations regarding privacy on the internet and regulations regarding spam e-mail. Meanwhile, secondary data consists of related literature books and journals that discuss cybercrime and related regulations. Secondary data is also used to find references related to spam settings in several countries to find out why in those countries spam e-mail is considered a criminal activity and its relation to their privacy settings.

The data collection techniques in this article use several methods, namely an inventory of the data that is the reference source for this article. Then classify all the data and divide it into primary data and secondary data and systematize primary data and secondary data to suit the needs of this article.

The data analysis technique is carried out in this article using qualitative and quantitative descriptive analysis techniques, namely the author describes the primary data and looks for facts that support the description of the primary data which aims to provide an overview and describe the problems that exist then further analyzed with theories and explanations. explanation related to existing problems based on secondary data. The results of this analysis are then used to formulate a conclusion.

3. Spam E-mails as Cybercrime

Disturbing information in the form of subtle advertisements, information that becomes an entry point for cybercrimes, such as data falsification, fraud, and data theft (Alazab and Broadhurst, 2015: 2; Ozbasi, 2019). Basically, spam activity is relatively easy when you look at the definition, which is an action that is carried out repeatedly or repeatedly. This means that the sender of information who is said to be spamming (spammer) can be seen from two characteristics, namely deliberately sending spam to commit crimes or spam senders who do not know that they have committed spam.

Spam e-mail, apart from containing unnecessary or irrelevant information, it is not uncommon for spam e-mails to lead recipients to click on certain links or URLs (Unique Related Location), where when clicked, this URL link will lead to a particular website or the URL contains malware. or a virus that can damage the recipient's computer system or steal e-mail recipient data. These malware or virus inserts are usually in the form of messages in spam e-mails that are social or complex codes.

Before the development of technology that is getting faster and faster, especially the internet today, the scope of privacy is limited to the disturbance that is subjectively experienced by each privacy. For example, there is an unauthorized break into someone's home or interference with someone's private life. Nowadays, with the existence of the internet, the scope of privacy has become wider. Internet with ubiquitous and borderless nature makes the scope of privacy not only a matter of disturbing one's personal life, but also involves several other aspects, as stated by Lessig cited by Rosadi (2015: 2), namely (1) privacy as a concept that individuals do not want disturbed by others, (2) the concept that privacy is related to one's honor, (3) the concept that government authority must be limited, so that its actions will not interfere with the privacy of its citizens.

The concept of privacy conveyed by Lessig is then related to freedom of personal expression and avoiding misuse of personal data on the internet, which is still a problem in the context of legal rules related to privacy on the internet. One example of causes related to privacy on the internet is the break-in of private photos of several Hollywood artists on iCloud which causes private photos of these artists to spread on the internet. It is known that the perpetrator of the iCloud account breach broke into 572 accounts, including the artist's accounts (Jeremy and Diamond, 2016).

There is a traditional view that the issue of privacy is independent of the legal structure, so that privacy is naturally threatened by the rapid development of technology, so that here the law should intervene in privacy arrangements (Solove, 2003: 14). As one example of the case above, law is demanded to be more dynamic in technological developments so that the law can ensnare perpetrators of technology crimes, because technology cannot be merely a tool or instrument. As has been described by Cockfield and Pridmore (2007: 483) that to explain the synthesis between law and technology, there is a substantive theory which states that technological

development also contains various social, economic, and political values which will then give birth to power and authority to whom mastering these technological developments.

Today, the issue of privacy on the internet has also become a complicated legal issue, but not all countries in the world regulate privacy issues on the internet. It is noted that Sweden is the first country to regulate the protection of privacy and personal data since 1973 through the Sweden Data Act 1973, where to date there are 76 countries that specifically regulate privacy and protection of personal data in a statutory regulation in their country (Greenleaf, 2012).

In the European Union, since 1995, guidelines for privacy and protection of personal data have been drawn up that can be adopted by EU countries in "Directive 95/46/EC/of the Parliament and of the Council on the Protection of Individuals regarding the Processing of Personal Data and on the Free Movement of such Data. " The directive was formulated with the aim of protecting the basic rights and freedoms of everyone, the rights to privacy in relation to the processing of personal data.

In Indonesia, there are no laws and regulations that specifically regulate the protection of personal data and privacy, especially on the internet. Several laws and regulations related to this matter are still regulated sporadically, such as Article 1 Number 3 and Number 4 of the Law of the Republic of Indonesia Number 43 of 2009 concerning Archives which regulates and distinguishes dynamic and vital archives; Article 29 of Law of the Republic of Indonesia Number 36 of 1999 concerning Human Rights, which states that everyone has the right to protection of personal, family, honor, dignity and property rights; Article 40 of Law of the Republic of Indonesia Number 10 of 1998 concerning Banking, in which banks are required to keep confidential information about their depositing customers and their deposits, except for tax purposes, settlement of bank receivables, judicial interests, and criminal cases; up to Article 40 of Law of the Republic of Indonesia Number 36 of 1999 concerning Telecommunications, which states that every person is prohibited from engaging in wiretapping of information transmitted through telecommunications networks in any form.

Regarding privacy with cybercrime, which is a global phenomenon and is new to the realm of law, violation of privacy can also be said to be one of the new modes of cybercrime. Early in its development, the terminology for crimes using technological means was "computer crime" or computer related crime. Hamzah and Marsita (1987: 24) reveal that the emergence of computer crime cannot be separated from "The man behind the machine", that there are deliberate mistakes that lead to misuse of computers that are carried out illegally for the benefit of themselves or their group.

Sending spam e-mails can cause disruption to computer systems or data, because spam e-mails are usually in the form of phishing. Phishing itself in the 2001 Convention on Cybercrime is classified into Offences Against Confidentiality, Integrity and Availability of Computer Data and System in the mode of system disruption or computer data disruption. In general, there are 2 (two) objectives of sending spam (Chohwanandi, 2012: 2-3), among others (1) sending spam usually aims as a medium for publication and promotion for the products of companies sending spam e-mails, for example a certain company wants to sell their production goods, because if through advertising it will certainly generate quite expensive costs, so by using this method, the company will be able to send as many e-mails as possible to all e-mail owners in the world, (2) spam is usually used as a "bomb e-mail", where if someone has an enemy on the internet or corporate competition, it is usually done by means of an e-mail bomb so that the individual is bothered to receive unnecessary e-mails in large numbers and continuously. Spamming is also often used as a medium for spreading viruses and worms, where the character of these viruses and worms is to automatically distribute files to all e-mail owners, with the aim of getting as many victims as possible. Spam can get out of hand because most spam is not manually generated by human spammers. These spammers usually use computer programs called Autobots.

The two objectives of sending spam above have a main characteristic, namely sending unwanted messages or e-mails by the recipient. This is because sending spam does not pay attention to the privacy of the recipient, in the context of privacy violations (Prosser in Dewi (2009: 19)). This form of sending spam e-mail includes disturbing people's right to be alone, where the scope of the disturbance is not only physically but mentally, whether individual, private, or state.

In connection with the 2 (two) objectives of sending spam e-mails above, spam e-mail senders for business promotion purposes are adhering to the principle of building their own market (if we built it, they will come), so that many spam e-mail senders use bots to simplify the spamming process.

Several laws and regulations in various countries have regulated e-mail spam as a crime, such as in Canada which is regulated through several laws and regulations, including the Personal Information Protection and Electronic Documents Act (PIPEDA), Competition Act, Charter of Rights Freedoms, The Criminal Code and the Competition Act, Canadian Code of Practice for, and Consumer Protection in e-commerce. Meanwhile in Australia it is regulated in the Spam Act of 2003, Telecommunications Act of 1997, and Australia Parts IVA, V, and VC of the Trade Practices Act of 1974.

Based on the description above, to determine an act to be a cybercrime, there are several things that must be considered related to the criminalization of cybercrime (Widodo, 2013: 60-61), among others (1) criminalization is an effort that supports the ultimate goal of criminal policy to protect and welfare of the community, (2) the actions to be criminalized are truly criticized by the community, (3) it is necessary to take into account the advantages and disadvantages of criminalization, (4) efforts need to be made so that there is no over-criminalization which can have secondary effects on the interests of the community, (5) it is necessary to adjust the capacity of law enforcers and law enforcement.

4. Ideal Settings Regarding Spam E-mails as Cybercrime for Privacy Protection

As described above, cybercrime has given a new form of crime that the positive criminal law cannot reach. In terms of sending spam e-mails, several countries have also regulated the sending of spam e-mails as a form of cybercrime.

Prasetyo (2010: 45) explains that there are several reasons that can be the basis for an act to be criminalized, including (1) the existence of a victim, (2) criminalization is not solely aimed at retaliation, (3) must be based on the principle of the ratio principle, and (4) there is a social agreement. Furthermore, these reasons are discussed one by one based on the elements and modes of sending spam e-mails, which are as follows:

1. There were victims

In a criminal act, the victim is the main prerequisite for the existence of a crime. This is because the crime will inevitably cause harm in his actions, where this loss is experienced by the victim. In spam e-mails, there are losses experienced by spam e-mail recipients as victims, namely violated privacy, where the spam e-mail is not wanted by the recipient and there is phishing which can then retrieve personal data from the recipient of the spam e-mail. In Indonesia, it was noted that in mid-2020, the number of spam e-mails was 23.5 million, an increase from 18.5 million in 2019 (quoted from kompas.com). Meanwhile, based on research results from ID-CERT until December 2020, complaints about spam were recorded at 41.7% or as many as 16,087 complaints (ID-CERT, 2019). Based on these data, sending spam e-mails causes harm and as an act that can be criminalized, because sending spam e-mails causes victims.

2. Criminalization is not solely for retaliation

The initial development of the purpose of criminal law was to retaliate for losses suffered by victims. However, in the current context, especially those related to cybercrime, then the purpose of retribution or retributivists certainly needs to be reviewed. Ideally, the current criminal law and punishment should also be restorative. Widodo (2013: 147-148) states that considering the characteristics of cybercrime whose jurisdiction can cross national borders, a non-penal policy strategy is needed to combat cybercrime non-penal, including international cooperation and national action plans to combat cybercrime. This shows that there are efforts to prevent it not just retaliation. The sending of spam e-mails can also accommodate this, considering that the disturbance that appears in the form of a loss from the victim's privacy is not a definite measure and is very subjective, so the form of criminalization is not appropriate when it uses the purpose of retaliation.

3. Based on the Ratio Principle (protection of interest aimed at the making of criminal law)

Basically, every statutory regulation related to criminal law has the objective of protecting the interests of three parties, namely the interests of individuals, groups, and the state. Then the criminalization of an act will show which interests are protected by considering the principle of that ratio. Sending spam e-mails has the interests of individuals being violated, which is related to privacy violations which can then be used as an excuse that sending spam e-mails can be criminalized as a separate cybercrime.

4. There is a social agreement

The social agreement here comes from the government element, where criminalization is the authority of the government to determine an act is regulated as a crime in law. Regarding the sending of spam e-mails, the number of complaints as previously described, shows that there is a real impact on society socially and can be used as government legitimacy to criminalize sending spam e-mails as a cybercrime.

Criminalizing the sending of spam e-mails as a form of cybercrime, can also be seen from the problems that can be caused, especially for parties or users of information technology, which can be seen in the following table:

Table 1. **Problems Due to Spam E-mails**

PARTIES/USERS INFORMATION TECHNOLOGY	PROBLEM RELATED TO E-MAIL SPAM
Consumer	1. Spam pertains to employees and user privacy 2. E-mail harvesting in order to collect e-mail addresses to which junk e-mail is sent 3. E-mails usually contain malicious program code that can damage computers or computer networks 4. Steal important consumer information, such as credit card information 5. Phishing (falsification of identity)
Employees and Companies	1. Time is spent deleting the spam e-mail 2. Additional fees for internet connection fees 3. Loss of productivity
ISP (Internet Service Provider)	1. Additional costs for developing an anti-e-mail spam infrastructure 2. Extra bandwidth and extra storage costs to deal with the amount of spam 3. Poor bandwidth performance 4. Operating System (OS) is damaged due to the amount of spam 5. Consumer dissatisfaction
Businessmen e-Commerce	1. Running out of consumer confidence 2. Excessive spending 3. Abuse (fake) products that shift the superiority of the original product 4. Piracy of software or other digital products
Government	1. Netiquette violations (ethics on the internet) 2. Spam can contain content that violates the law (pornography, fraud, data theft, etc.)

Source: ***Moustakas, Ranganathan, dan Duquenoy (2005:2)***

Based on the above problems, the regulations related to sending spam e-mails are based on the elements of the spam e-mail sending, namely the “bulk”, “unsolicited” and “commercial” elements. The "bulk" and "unsolicited" elements can be accommodated through the ITE Law, both through Article 32 and Article 33. Meanwhile, the "commercial" element means that it relates to online buying and selling activities in electronic transactions. However, in the ITE Law, articles relating to electronic transactions only regulate fraudulent matters relating to the spread of false and misleading news.

The sending of spam e-mails, which are privacy disturbances related to electronic transactions, is still at the promotional stage, but it can be arranged, where disruption of data or electronic systems is then linked to the process of collecting consumer data without permission or violating consumer privacy. The description in the table above can also be seen that there are forms of material losses and immaterial losses. For this reason, considering that the ITE Law is the only statutory regulation related to information technology, it is necessary to regulate a revision related to the criminalization of sending spam e-mails.

In addition, changes regarding the ideal arrangement in the ITE Law on sending spam e-mails, namely changes or additions to articles related to consumer losses in an electronic transaction, where the spread of fake news still exists, but emphasizes the elements of data disruption and electronic systems. which can cause loss or damage to consumer data because of its constitutive elements.

The constitutive consequence is regulated to accommodate phishing elements which are used as a mode of sending spam e-mails, while fake news or electronic information is regulated as an element of action, considering that spam has "bulk" and "unsolicited" elements. In addition, spam e-mail mode usually uses e-mail headers that

appear real, so that the recipient is trapped by the spam e-mail (Moustakas, Ranganathan, and Duquenoy, 2005: 5). Amendments to the addition of this article will at least be able to guarantee privacy protection, especially in relation to sending spam e-mails that are used for promotion, but instead take the form of privacy violations.

5. Closing

The sending of spam e-mails usually aims at two things, namely as a promotional medium and in the form of "e-mail bombs" (e-mail blasts) which can be used to spread viruses, thereby damaging the target's data or computer systems, as well as violating privacy and stealing personal data from the target.

Positive criminal law in Indonesia has no specific regulations regarding the sending of spam e-mails, either Article 32 or Article 33 of the ITE Law, which formally have not been able to accommodate the elements in spam, namely "bulk", "unsolicited", or "commercial". The commercial element defined as electronic transactions under the ITE Law is still limited to consumer fraud in the context of fake and misleading news, which is contained in Article 28 Paragraph 1 of the ITE Law.

Changes are needed in the ITE Law, particularly in relation to the criminalization of sending spam e-mails, by accommodating aspects of phishing and theft of victim data, in this case promotion in electronic transactions. Amendments or revisions to the ITE Law will guarantee protection of the privacy of internet users in Indonesia, especially regarding personal data from users.

References

1. Chazawi, Adami dan Ferdian, Ardi. 2011. *Tindak Pidana Informasi dan Transaksi Elektronik*. Malang: Bayumedia Pub-lishing.
2. Dewi, Shinta. 2009. *Cyberlaw Perlindungan Privasi Atas Informasi Pribadi dalam e-Commerce Menurut Hukum Internasional*. Bandung: Widya Padjajaran.
3. Hamzah, Andi dan Marsita, Boedi D. 1987. *Aspek-Aspek Pidana di Bidang Komputer*. Jakarta: Sinar Grafika.
4. Lessing, Lawrence. 2006. *Code, Basic Books*. New York School of Law Legal Studies Research Paper No. 98/2012.
5. McCusker, Rob. 2005. *Spam: Nuisance or Menace, Prevention or Cure?* Canberra: Trends and Issues in Crime and Criminal Justice No. 294.
6. Moustakas, Evangelos, Ranganathan, dan Penny Duquenoy. 2005. *Combating Spam Through Legislation: A Comparative Analysis of US and European Approaches*. *Proceedings in Second Conference on E-mail and Anti-Spam* (CEAS 2005).
7. Ozbasi, D. (2019). Using Rank-order Judgments Scaling to Determine Students' Evaluation Preferences. Eurasian Journal of Educational Research, 82, 63-80.
8. Prasetyo, Teguh. 2010. *Kriminalisasi dalam Hukum Pidana*. Bandung: Nusamedia.
9. Rosadi, Sinta Dewi. 2015. *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional, dan Nasional*. Bandung: Refika Aditama.
10. Solove, Daniel J. 2003. *Identity Theft, Privacy, and the Architecture of Vulnerability*. Hastings Law Journal Vol. 54.
11. Sitompul, Josua, 2012. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa.
12. Sudarto. 1981. *Hukum dan Hukum Pidana*. Bandung: Alumni.
13. Suhariyanto, Budi. 2012. *Tindak Pidana Teknologi Informasi (Cyber Crime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Raja Grafindo Persada.
14. T. Ngo, Fawn, dan Raymond Paternoster. 2011. *Cybercrime Victimization: An Examination of Individual and Situational Level Factors*. *International Journal of Cyber Criminology*, Vol. 5 Issue 1.
15. Widodo. 2013. *Memerangi Cybercrime: Karakteristik, Motivasi, dan Strategi Penanganannya dalam Perspektif Kriminologi*. Yogyakarta: Aswaja Pressindo.
16. Zavrsnik, Alex. 2008. *Cybercrime: Definitional Challenges and Criminological Particularities*. *Masaryk University Journal of Law and Technology*.