P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281

Reviewing Information and Electronic Transaction Act from a Convention on Cybercrime of 2001

Wahyu Priyanka Nata Permana[1]

[1] *Faculty of Law, Universitas Islam Indonesia, Indonesia*
154101308@uii.ac.id

Abstract

Introduction to the Problem: This research analyses the norms of substantive criminal Law regarding Information and Electronic Transaction Act Number No. 11 of 2008 in conjunction with Bill Number 19 of 2016 on Amendments to Information and Electronic Transactions Act No. 11 of 2008 and its compliance with the Convention on Cybercrime, 2001.
Purpose/Objective Study: This research aims to analyze the conformity of offenses, criminal liability, and criminal sanction in the Information and Electronic Transaction Act (IETA) to the principles promulgated in the Convention on Cybercrime, 2001.
Design/Methodology/Approach: This research is a normative legal study using statute and conceptual approaches.
Findings: This study concluded that, in general, offenses regulated in IETA had confirmed the Convention. Nevertheless, the provision of computer-related fraud in IETA has a broader range than that of the Convention. IETA also lacks formulation concerning when and who bears criminal liability for corporate crime as suggested in the Convention. The research also finds that IETA did not adopt the principle of effectiveness and proportionality in promulgating both punishment and treatment. This study suggests that IETA should adopt criminal liability for a corporation, set the penal punishment proportionate to the seriousness of conduct and culpability of the actor, and regulate treatment.
Paper Type: Research Article
Keywords: Substantive Criminal Law, Information and Electronic Transaction Act; Convention on Cybercrime of 2001

Introduction

This research analyses the norms of material criminal Law regarding Information and Electronic Transaction Act Number No. 11 of 2008 in conjunction with Bill Number 19 of 2016 on Amendments to Information and Electronic Transactions Act Number 11 of 2008 (hereinafter referred to as the IETA) and its compliance with the Convention on Cybercrime, 2001 (hereinafter referred to as the Convention). The study directs the analysis to the regulation of criminal offenses, criminal liability, and criminal sanctions. The IETA regulates the three aspects in Article 25 to Article 37 and Article 45 to Article 52. In the Convention, these three aspects are regulated in Chapter II concerning Material Criminal Law (Substantive Criminal Law), starting from Article 2 to Article 10.

Article History
Submitted 18 November 2020 - Revision Required 27 November 2020 - Accepted 5 October 2021

JURNAL HUKUM NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281
P-ISSN: 1412-6834
E-ISSN: 2550-0090

There are several reasons why this research is essential to do. First, the Convention is the first international agreement that aims explicitly to fight cybercrime phenomena. A crime crosses the State's geographic barriers and causes numerous and transnational victims (Marler, 2002).

Second, the first Convention was established and signed by member states of the European Union. However, the states outside the European Union have ratified the Convention (Setiyawan, 2020). They have inserted into their National Legal System, such as United States, Japan, Canada, Australia, Argentine, Brazil, and the Philippines. It means the ratification has become global awareness. The ratification demands harmonization of the national legal system related to cybercrime regulation (Murphy, 2001).

Third, Indonesia has not ratified the Convention yet. Nevertheless, it is deemed necessary to adjust national criminal law to the Convention. The last revision of the IETA was in 2016, which still emerges several shortcomings and critics. The criminal threat in the IETA is regarded much severe compared to the primary offense in the Penal Code (Putri, 2016). The practice to enforce a crime against an act that fulfills offenses formulation within the Law turns out to be deviating from the principles of fair criminal law enforcement, for instance, in defining cyber defamation (Afiyatun, 2019). Cybercrime is increasingly high in Indonesia, such as Web phishing, an online scam, or fraud to imitate popular websites to scam and steal information. (Sulisrudatin, 2019). Interpol in Cybercrime: Covid-19 Impact, reveals that cybercriminals are not hesitant to imitate the appearance of public service portals such as official government websites, telecommunication companies, banks, taxes authorities, to national customs. They do the tricks to target financial assistance schemes for the poor and financial support for entrepreneurs or Micro, Small, and Medium Enterprises (MSMEs). Indonesia needs to be cautious. Interpol in ASEAN Cyberthreat Assessment 2020 conveys that Indonesia became the highest ASEAN Web phishing target in 2019. Indonesian status is one of ASEAN's biggest markets with its infrastructure and technology to increase the economy. The minimum supervision of cybersecurity and cleanliness of the internet makes it a valuable destination for cybercriminals (Hodges, 2008).

Based on the above background's descriptions, the research's legal issue is whether the provisions for criminal offenses, criminal liability, and criminal sanctions in the IETA Act correspond to or consider the principles in the Convention?

Methodology

The research includes the normative legal study because it reviews legal norms within legislation regarding the conformity of criminal offenses arrangements, criminal liability systems, and criminal sanctions in the IETA with the Convention. The primary legal material in this study is IETA and the Convention. The secondary legal material is from books, journals, or research related to criminal offenses, criminal

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281

liability, criminal sanction, and cybercrime. The research approach is in legislation and conceptual approach (Marzuki, 2006). The research collects legal material through library research. Afterward, research analysis uses qualitative descriptive analysis, which means legal material is described within a narration arranged systematically, logically, and from the researcher's interpretation of the legal material produced.

Results and Discussion

The Concept of Cybercrime

Cybercrime (CC) is used in 'background paper' for workshops in the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders 2000. This document explains that cybercrime is divided into two categories, i.e., cybercrime in a narrow sense, which is so-called computer crime, and cybercrime in a broader sense, which is called computer-related crime. Computer crime is any illegal behavior directed to employ electronic operations that target computer systems' security and their data. Simultaneously, the computer-related crime defines as 'any illegal behavior committed utilizing, or with a computer system or network, including such crimes as illegal possession, offering or distributing information utilizing a computer system or network' (Brenner, 2002). Based on the above definitions, cybercrime covers crimes committed (Arief, 2001):

1. Utilizing a computer system or network;
2. Within a computer system or network; and
3. Towards a computer system or network.

Referring to the above explanation, it seems that cybercrime has a broad spectrum and coverage that can reach various domains of activities such as broadcasting, decency, telematics, intellectual property rights, taxation, privacy, trade, terrorism, and others. Ahmad Ramli describes several types of cybercrime, among others; 1) breaching website content, which is pornography, defamation, humiliation, libel and hoax, and copyright infringement. 2) crimes in electronic trade, in the form of online auction scams, online stock scams, online multilevel marketing scams, credit card scams; 3) Immorality breaching such as recreation hacker, cracker or criminally-minded hackers, political hacker, denial of service attack, viruses, piracy, fraud, gambling, pornography, pedophilia, cyberstalking, hate sites, and criminal communication; and 4) terror via SMS (Ramli, 2003).

The broad spectrum and coverage of cybercrime are understandable because it related to two characteristics: transnational and anonymity (Salsa, 2020). Article 3 paragraph (2) of the Palermo Convention Against Transnational Crime, 2003 stipulates that a crime includes a transnational crime if; a) it is committed in more than one country; b) it is committed in a Country; however, most of the criminal preparation is organized, directed, and controlled in another country; c) it is committed in a Country but involving organized criminal groups in more than one

Article History
Submitted 18 November 2020 - Revision Required 27 November 2020 - Accepted 5 October 2021

JURNAL HUKUM NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281
P-ISSN: 1412-6834
E-ISSN: 2550-0090

country; and d) it is committed in a Country, but it impacts substantially toward another country. The anonymity nature of cybercrime is that it is possible and easy for someone to hide his identity while continuing to communicate online within the internet. It is possible because communication takes place in bytes and text rather than image or a person sound (Supancara, 2007)

Substantive Criminal Law in the Convention

The Convention establishes several principles that need to take into account in criminalizing cyberspace activities and their legal enforcement. First, the principle of unity covers all aspects, including the legal enforcement aspect (Convention). Second is the principle of international cooperation. According to Article 23 of the Convention, this principle has a close connection with the unity principle and wishes that international cooperation is necessary for fighting cybercrime. One nation is impossible to fight crime alone without the help of other nations. The third is the principle of protection. The principle needs to exist so that it protects society from cybercrime. The Conventions' regulations regarding prohibited actions aim to protect every citizen (Preamble and Chapter II of the Convention). Fourth, the balance principle emphasizes the necessity of a balance between legal enforcement and human rights protection. According to Article 15 of the Convention, offenses subjected to punishment must not violate the freedom and human rights.

The fifth is the principle of anticipation, which closely connects to the dynamics in the cyber world. It requires a set of legal regulations to protect the interested parties either in the present or future (Convention preamble). Sixth, the liability principle stresses the offender's liability for the cybercrime committed, including the third parties that intentionally and deliberately provide hardware and software to commit cybercrime (Article 2-13 of the Convention). Seventh is the principle of legal certainty. Besides using legal terminology in the Convention to avoid the varied interpretation, the principle is also related to the certainty of prohibited actions divisions (Preamble and Article 2-10 of the Convention). Eighth, the nationality principle has a close connection with the right to judge on cybercrime cases. The principle is also related to strengthening international cooperation to overcome cybercrime, which has become a transnational crime (Article 2-22 of the Convention). Ninth, the principle of conformity between legal regulations in the real world with legal regulations in the cyber world. Tenth, the principle for not overloading the legal enforcement. In criminalizing an act in the cyber world, the legislator must, as best as possible, avoid making legal norms that cannot be upheld high because of their limitations (Article 9 of the Convention). The eleventh is the principle of mutually beneficial cooperation. Through the principle, every nation is requested to cooperate widely to fight against cybercrime by providing means and equipment, communication, inquiries and investigations, extradition to other countries (Article 25-35 of the Convention). Twelve, the reciprocity principle requires that every country request other countries based on an extradition agreement. Subject to the National Law, cybercrime criminals

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 12, Issue 02, 2021, pp. 267-281

should be submitted to their jurisdiction to be punished (Article 24 of the Convention).

In the Convention, prohibited actions are regulated in Chapter II of Substantive Criminal Law, starting from Article 2 to Article 10. There are 9 (nine) types of cybercrime, which are included in four criminal offenses categories. The first category relates to the criminal offenses against confidentiality, integrity, data availability, and computer system, including illegal access, illegal interception, data interference, system interference, and devices' misuse.

1. Offenses including Illegal access is deliberately accessing the whole or part of the computer system without right (Article 2);
2. Offenses including illegal interception are by intentionally commit interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data (Article 3);
3. Offenses including data interference are by intentionally commit damaging, deletion, deterioration, alteration, or suppression of computer data without right (Article 4);
4. Offenses including system interference are by intentionally committing the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data (Article 5);
5. Offenses, including as misuse of devices is by intentionally commit and without the right to produce, sell, procurement for import, distribution, or otherwise making available: a device, including a computer program, designed or adapted primarily to commit any of the offenses established following Article 2 through 5; a computer password, access code, or similar data by which the whole or any part of a computer system with the intent that it would use to commit a crime. It is not included as misuse of devices if the offense is not deliberately to commit a crime, for instance, for the authorized testing or protection of a computer system (Article 6).

The second category is the criminal offenses related to a computer, which consists of computer-related forgery and computer-related fraud.

1. Offenses, including computer-related forgery, intentionally commit and without right, inputting, alter, deleting, or suppress computer data, resulting in inauthentic data. It was intended or acted upon for legal purposes as authentic, regardless of whether the data is directly readable or intelligible. A party may require an intent to defraud or similar dishonest intent before criminal liability attaches (Article 7).
2. Offenses, including computer-related fraud, is intentionally committed and without right, which causes a loss of property to another person by:
   a. Any input, alteration, deletion, or suppression of computer data;

Article History
Submitted 18 November 2020 - Revision Required 27 November 2020 - Accepted 5 October 2021

JURNAL HUKUM
NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281
P-ISSN: 1412-6834
E-ISSN: 2550-0090

b. Any interference with a computer system's functioning with fraudulent or dishonest procuring intent, without right, an economic benefit for oneself or another person (Article 8).

Third categories on action included offenses related to child pornography by performing intentionally and without right, the following conduct:
1. producing child pornography for its distribution through a computer system;
2. offering or making available child pornography through a computer system;
3. distributing or transmitting child pornography through a computer system;
4. procuring child pornography through a computer system for oneself or another person;
5. possessing child pornography in a computer system or on a computer data storage medium (Article 9).

The fourth category is criminal offenses related to copyright infringements and related rights: 'offenses related to the copyrights infringement committed willfully on a commercial scale and employing a computer system (Article 10). The Convention also regulates personal or corporate liability. Article 12 paragraph (1) states: all offenders are held responsible for all crimes under this Convention which are committed for their benefit by a natural person, either individually or as part of an organ of the legal entity, who has a leading position within it, based on:
1. power of representation of the legal entity;
2. an authority to make decisions on behalf of the legal entity;
3. an authority to exercise control within the legal entity.

A legal entity is also liable where a natural person's lack of supervision or control has committed a criminal offense by a natural person acting under its authority (Juniar, 2021). Liability here includes civil, administrative, and criminal (Article 12 paragraph (2) and paragraph (3) Convention). Sanctions and measures regulated in Article 13 state that it is essential to guarantee that criminal offenses established in Articles 2 through 11 are punishable by effective, proportionate, and dissuasive sanctions, including deprivation of liberty non-criminal sanctions or measures, including monetary sanctions.

Substantive Criminal Law in IETA

The IETA regulates the prohibited offenses starting Article 27 through Article 37, which if it is detailed as follows:
1. actions by distributing, transmitting, and/or causes to be accessible Electronic Information and/or Electronic Documents with contents of:
   a. against morality (Article 27 paragraph 1);
   b. gambling (Article 27 paragraph 2);
   c. affronts and/or defamation (Article 27 paragraph 3);
   d. extortion and/or threats (Article 27 paragraph 4)
2. distributing to:

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281

   a. disseminates false and misleading information resulting in consumer loss in electronic transactions (Article 28 paragraph 1);
   b. inflict hatred or dissension on individuals and/or certain groups of community-based on ethnic groups, religion, races, and inter-groups SARA (Article 28 paragraph 2);
3. Sending electronic messages containing violent threats and/or scares certain person (Article 29);
4. Intentionally and without rights to:
   a. Access computer and/or electronic system belong to other by any means whatsoever (Article 30 paragraph 1);
   b. Access to get electronic information and/or electronic document (Article 30 paragraph 2).
   c. Breach, hack, trespass, or break into a security system by any means whatsoever (Article 30 paragraph 3).
5. Intentionally and without rights or unlawfully:
   a. Any person who intentionally and without right or unlawfully commit interception or wiretapping of Electronic Information and/or Documents within a computer and/or specific Electronic system of another person (Article 31 paragraph 1)
   b. Commit interception of the non-public transmission of Electronic Information and/or documents from, to, and within a computer and/or specific Electronic system of another person, whether or not causing alteration, deletion, and/or suppression of Electronic Information and/or Documents in transmission (Article 31 paragraph 2).
6. Without right or unlawfully in any means whatsoever:
   a. Alters, adds, reduces, transmits, tempers with, deletes, moves, hides an Electronic Information and/or Document of other person or the Public (Article 32 paragraph 1);
   b. Moves or transfers Electronic Information and/or documents to unauthorized persons' electronic systems (Article 32 paragraph 2).
7. Commits any act resulting in faults on Electronic system and/or resulting in Electronic System working improperly (Article 33).
8. Produces, sells, causes to be used, imports, distributes, provides, or owns: a) computer hardware or software designed or specifically developed to facilitate acts as intended by Article 27 through Article 33; b) Computer passwords, Access Codes, or the line to make Electronic Systems accessible with the intent to facilitate acts as intended by Article 27 through Article 33 (Article 34 paragraph 1)
9. Manipulates, creates, alters, deletes, destructions of Electronic Information and/or Document with the intent that such Electronic Information and/or Document would seem to be authentic data (Article 35)

Besides acknowledging individuals as the subject of the offense, IETA also recognizes corporations as the offense's subject (Mulasari, 2012). Article 1 item 21 states that a

Article History
Submitted 18 November 2020 - Revision Required 27 November 2020 - Accepted 5 October 2021

JURNAL HUKUM NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281
P-ISSN: 1412-6834
E-ISSN: 2550-0090

person is a natural person, either Indonesian citizen, foreign citizenship, or legal entity. Thus, a corporation in this Act is limited as a legal entity. Even though Article 1 items 22 states that a business entity is an individual company or partnership company, either legally established or not, the corporation's meaning cannot be expanded, including businesses with the legal entity or without a legal entity. The formulation of offenses in Article 27 through Article 37 uses 'any person,' not 'any party.'

Corporate recognition as the subject of the offense must also be followed with its penal liability formulation (Suartha, 2018). It means that when the corporate is liable for criminal offenses committed and personal liability, it needs to be formulated in Article so that its jurisdiction construction is apparent. Unfortunately, the research does not find both of these matters in the IETA. Nevertheless, this Act recognizes the corporation as the subject of a crime, regulating when the corporation is liable, but the party's liability for the crime is absent.

There are two types of primary penal sanctions (*strafsoort*) threatened with criminal offenses under the IETA: imprisonment and monetary sanctions formulated in cumulative alternatives intended to individual offenders or corporations (Rauf, 2019). The Act did not recognize minimum sanctions as what existed in the other Acts outside the Penal Code. The maximum penalty (*strafmaat*) imprisonment imposed on (offender) of the criminal offenses in the provision of Article 45 paragraph (3) and Article 51 is 12 years. Meanwhile, the least penalty is six years, which is regulated in Article 45 paragraph (1) and paragraph (2) and Article 46 paragraph (1). The maximum fine of 12 billion in Article 51, while the least is 600 million, is regulated in article 46 (1). The interesting part is that there is an amendment to the specific criminal threat for violations of Article 45 in conjunction with Article 27; from a full six years of imprisonment and/or maximum of 1 billion fine becomes a maximum four years imprisonment and/or maximum of 750 million fine. This Act also regulates increasing sanctions by adding one-third of primary crime either subjected to individual or corporate offenses. This Act does not regulate additional crime or measures sanction (treatment).

Analysis of the Conformity between the Provisions on Substantive Criminal Law in IETA and Convention

To analyze whether there is any conformity between material criminal Law in IETA and the Convention refers to the three aspects described above, i.e., provision of prohibited actions, criminal liability, and criminal sanction. The first is regulation on prohibited actions. The substance of the offenses prohibited in Article 46 in conjunction with Article 30 of the IETA is related to the prohibition of access without rights, which is called illegal access regulated in Article 2. The formulation of unauthorized access considers the same formulation on illegal access in the Convention. The Illegal Interception in Article 47, in conjunction with Article 31

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281

paragraph (1) and paragraph (2) of the IETA, also conform or considering the formulation of illegal interception in Article 3 Convention.

Prohibition to disturb data in Article 48 in conjunction with Article 32 of the IETA has considered data interference formulation in Article 4 Convention. The prohibition in interfering on the system in Article 49 in conjunction with Article 33 of the IETA has the same formulation as the prohibition on interference system in Article 5 Convention. The prohibition regulates computer hardware device misuse by considering the misuse of devices in Article 6 of the Convention. Provision on forgery related to utilizing the computer in Article 51 paragraph (1) in conjunction with the IETA has also considered the formulation of computer-related forgery in Article 7 Convention.

The difference in the prohibition of computer-related fraud in Article 51 paragraph (2) in conjunction with Article 36 in conjunction with Article 32 paragraph (1) or Article 33 of the IETA compared to the formulation of computer-related fraud in Article 8 of the Convention is that the scope and coverage of the IETA are broader than the latter. In formulating elements resulting in the loss for another person, Article 36 IETA covers all loss materially and immaterially, while Article 8 Convention only limited economic loss, especially in the loss of another person's wealth. Besides, the prohibition offenses mentioned in Article 27, Article 28, Article 29, Article 30, Article 31, Article 32, Article 33, and Article 34, of which offenses of the Articles cause the loss of other people. Article 8 Convention particularly formulates elements to cover without rights, causing of a loss of property to another person by input, alteration, deletion of computer data or by interference in the computer function, with the intent to gain economic benefit for himself or other people, by fraudulent or dishonest (Wisnusubroto, 2011).

IETA also regulates content-related offenses, which regulates in Article 9 Convention. It is just that the content of the prohibited offenses is different. If Convention prohibited child pornography, IETA, on the contrary, broaden not only without right action to distribute, transmit, and/or access Electronic Information and/or Document which containing morality offenses, but also gambling, humiliation, and/or defamation, and extortion and/or threat. It is understandable if child pornography is not regulated in the IETA because it has been regulated in Article 37 in conjunction with Article 11 and Article 38 in conjunction with Article 12 on Pornography Act Number 44 of 2008. Article 37, in conjunction with article 11, is formulated as follows:

> "Any person who involves children in activities and/or as the object as referred in Article 11 shall be punished with the same penalties as those referred to in Article 29, Article 30, Article 31, Article 32, Article 34, Article 35, and Article 36, plus 1/3 (one third) of the Maximum penalty threat."

Provision of Article 38 in conjunction with Article 12 is as follows:

> "Any person who invites, persuades, takes advantage of, permits, abuses power, or forces children to use pornography services or products, as referred

Article History
Submitted 18 November 2020 - Revision Required 27 November 2020 - Accepted 5 October 2021

JURNAL HUKUM
NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281
P-ISSN: 1412-6834
E-ISSN: 2550-0090

> to in Article 12, shall be punished. By imprisonment at least 6 (six) months and maximally 6 (six) years and/or minimal fine as much as Rp250,000,000.00 (two hundred fifty million rupiahs) and maximum fine as much as Rp3,000,000,000.00 (three billion rupiahs)."

The substance in both Articles forbids child pornography. Therefore, IETA does not have to forbid it again so that it does not overlap a regulation to a crime prohibited in two Acts and to prevent an overcriminalization (Todd, 2015). Likewise, copyright infringement committed intentionally on a commercial scale and by means of a computer system intended in Article 10 Convention is also not regulated in the IETA. Before IETA and legislation, Indonesia has established Copyright Act Number 19 of 2002, which was replaced by Act Number 28 of 2014. In contrast, one of the crimes forbade is conducting copyright infringement or rights related to commercial purposes.

Based on the above description, regulation of criminal offenses in the IETA, in general, has considered the conducts prohibited in the Convention. However, several provisions in IETA did not have broader coverage and scope compared to Convention. Child pornography and Copyright Infringement are also regulated in the Convention. However, it is not regulated in the IETA because Indonesia has prohibited both criminal offenses in specific Acts.

The second is criminal liability. Both IETA and Convention acknowledge a person or a corporation as the subject of the offense. However, corporate recognition as a subject in the IETA is not followed with the provision of corporate criminal liability, when a corporation is liable and whom parties are liable if a corporation commits a cybercrime. It is different with Convention, states that corporate is liable if cybercrime is committed by corporate management and benefit for the corporation. Parties are held liable are 1) authorized person representing corporate; 2) authorized to decide on behalf of the corporation; or 3) authorized to control the corporate (Arief, 2013).

The management authority in representing, taking the decision or controlling the corporate shows that what the management does is identical with what a corporation is doing. In theory, it so-called identification theory (Akbari, 2017). According to this theory, the corporate can commit many direct offenses through an agent with a close connection with the corporate, act for and on behalf of the corporate (Colvin, 1995). They are not a replacement, and therefore, corporate liability is not an individual liability. The direct corporate crime liability requirement is still within the corporate's scope of work. As long as it is related to a corporate, certain offenses of a corporation are considered the Act of corporate itself (Weissmann, 2007). The specific agent in a corporate is considered as "directing mind" or "*álter ego*." An act and *mens rea* of the individual is then related to the corporate. If an individual is given authority to act on behalf of and while managing corporate business, *mens rea* of the individual is the same as the corporate *mens rea* (Sheley, 2019).

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281

Based on the above description, it seems that criminal liability regulation, especially for corporate in IETA, has not considered the provision of criminal liability in the Convention. Suppose the Convention regulates when a corporation is liable and parties liable for cybercrime committed by a corporation. IETA only regulates corporate as offenses, while when and parties who liable is not regulated.

The third is criminal sanction. IETA only regulates primary crime sanctions covering imprisonment and forfeiture. Meanwhile, additional penalties and sanctions are not regulated. Even though Convention regulates primary crime such as imprisonment and forfeiture, it also regulates other sanctions that its forms are left to the countries adopting Convention. Besides, even though IETA regulates forfeiture, it is not clear whether it is intended for corporate. It is because IETA does not regulate crimes of corporate. Article 52 paragraph (4) only states, 'If a corporation commits the criminal offenses as referred to in Article 27 through Article 37, the punishment shall be the principal sentence plus two-thirds.' The problem is that the corporation's principal sentence is not regulated in the IETA, so the Article is unclear. This ambiguity results from the absence of regulation regarding when the corporate is liable and parties liable for such cybercrime committed by the corporation.

The absence of the primary crime sentence for a corporation in IETA shows that criminal penalties formulation does not reflect 'effective' criteria in the Convention. The effectiveness principle mentioned can be seen from several indicators, i.e., first, the objective of punishment is to prevent the committing of a criminal offense, restore balance, and solve conflict (general prevention). Second, correcting the offender (special prevention). The absence of primary punishment type regulation reflects the effectiveness principle in implementing punishment toward cybercrime committed by a corporation.

Regarding the punishment weight, the Convention emphasizes that the imposition of criminal sanctions must be proportional to conformity between the severe punishment with the crime impact (offender's crime) (Luna, 2003). Proportionality refers to ordinal proportionality and cardinal proportionality. The ordinal proportionality principle refers to all punishment scale levels, maximum punishment, and real legal distance. It does not have to be proportional to the scale of the committed offense. Whether the level must exist within a particular country is debatable, based on criminology research, and inevitably, limited by social conventions. The cardinal proportionality leads to a crime that must be punished compared to similar offenses, compared to the more or less severe character of other crimes (Ardika, 2018). However, the proportionality concept needs to maintain a relationship between a relative crime's seriousness with relatively harsh punishment (Berry, 2011). In Barbara A. Hudson's words, the principle is called 'ranking offenses according to the seriousness and then establishing a scale of penalties of commensurate severity' (Hudson, 1996).

Article History
Submitted 18 November 2020 - Revision Required 27 November 2020 - Accepted 5 October 2021

JURNAL HUKUM
NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281
P-ISSN: 1412-6834
E-ISSN: 2550-0090

The ordinal proportionality still requires three things, i.e., parity, rank-ordering, and spacing of penalties (Hirsch, 1994). Parity occurs when a person has committed several crimes that are similar to its seriousness; then, they are feasible to get punishment whose weight is comparable. Criminal offenses with equal seriousness receive a balanced criminal sanction. Rank-ordering relates to crimes that should be arranged based on the punishment scale so that its crime sentence relatively reflects on the level of crime seriousness. The decision of criminal sanctions that are heavier for offense Y than offense X shows that offense Y is more reproached than offense X. Therefore, the offense must be regulated according to the rank so that its degree of punishment reflects on the level of offense. The spacing of penalties depends on how precisely the severity of the penalties being compared can be adjusted. Spacing contains determining the distance between one crime to another crime. Offenses A, B, and C are different in their severity ratings, from severe to minor. A is more severe than B but slightly less severe than C. An offense's seriousness can be understood from a distance between serious and minor offenses (Hirsch, 1990).

Referring to the proportionality principle above, it appears that several stipulation/crimes punishment threat is inaccurate and disproportionate. *First*, the legislator has not ranked offenses in regulating crimes weight for every offense. It stipulates crimes punishment without referring to its seriousness causes over penalization, which is a severe punishment threat toward minor offenses or the light punishment threat toward serious offenses. The first is called over penalization, while the latter is called under penalization. So, over penalization also covers under penalization (Ali, 2020). Second, the formulation of a maximum of 6 years imprisonment and/or a maximum of 1 billion fine in Article 45 paragraph (1), paragraph (2) and paragraph (4) in conjunction with Article 27 paragraph (1), paragraph (2), and paragraph (4) is inaccurate and disproportionate. Criminal sanctions regard the same actions with different qualifications and qualities of criminal offenses between decency, gambling, and extortion/threatening (Suseno, 2012). Third, the provision of criminal sanction in Article 45 paragraph (2) in conjunction with Article 28 is also inaccurate and neglects the proportionality principle. It generalizes between criminal sanction for crimes of 'spreading hoax and misleading information' with 'spreading hatred and/or hostile speech based on ethnicity, religion, race, and inter-groups (hate speech)'. According to the researcher, hate speech is a more severe offense than spreading hoaxes and misleading information because it has potential social effects and the economy. The crimes' sanctions are more severe than the latter. Fourth, determination of criminal sanctions by a maximum of 12 years imprisonment sentence and/or a maximum of 12 billion fine for violating the provisions of Article 27 through Article 34 as stipulated in Article 51 paragraph (2) in conjunction with Article 36 are also inappropriate and contrary to the principles of proportionality and fair Law. The evil offenses mentioned in the Articles are not the same so that the punishment must not be measured the same. The

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281

severe or minor offenses should be equal to the quality of a crime and offenses (Ashworth, 2005)

Based on the above description, criminal sanction regulation in IETA has not considered the provision of criminal sanctions and measures in the Convention. Besides criminal sanctions regulations/provisions that did not reflect the principle of effectiveness and probability, IETA also does not regulate additional punishment and measures sanctions.

Conclusion

Regulation of criminal offense in the IETA is generally has considered offenses prohibited in the Convention. Even though several provisions in the IETA have broader scope and coverage than the Convention, such as the prohibition of scams, the latter has a broader formulation than computer-related fraud. Child pornography and Copyright infringement are regulated in the Convention, but not in the IETA because Indonesia has prohibited both felonies in special legislation. Regulation on corporate crimes liability in IETA has not considered the provision of crimes liability arrangements in the Convention. IETA only regulates corporate as a subject of offenses.

Meanwhile, when and liable parties are not regulated. The regulations of criminal offenses in the IETA have not considered the provisions/regulations of criminal offenses and measures in the Convention. Criminal offenses' stipulation did not reflect the effectiveness and proportionality principles and did not regulate sanctions measures as mentioned in the Convention. The research suggests the necessity to revise the IETA on corporate criminal liability and proportional principles in formulating criminal punishment threats and measures sanctions.

Acknowledgment

The authors would like to thank the Faculty of Law, the Universitas Islam Indonesia, for the support, especially Dr. Mahrus Ali, S.H., M.H, as a discussion partner in this research. Including I would like to thank the Editorial Board of Jurnal Hukum Novelty, Faculty of Law, Universitas Ahmad Dahlan for accepting this research. Including sincere gratitude also goes to reviewers and editors who have provided constructive feedback so that this manuscript looks worth reading and citing.

Declarations

Author contribution : Initiated the research ideas, instrument construction, data collection, analysis, and the final draft writing, as well as improving the revised manuscript.
Funding statement : The author declares no funding.
Conflict of interest : The author declares no conflict of interest.
Additional information : No additional information is available for this paper.

JURNAL HUKUM
NOVELTY
Volume 12, Issue 02, 2021, pp. 267-281
P-ISSN: 1412-6834
E-ISSN: 2550-0090

References

Afiyatun, A. W. (2019). Penentuan Kriteria Tindak Pidana Penghinaan Pasal 45 ayat (1) Juncto Pasal 27 ayat (3) UU ITE Studi Putusan-putusan Pengadilan. *Istinbath: Jurnal Hukum*, 216-217. https://doi.org/10.32332/istinbath.v16i2.1709

Akbari, A. R. (2017, March). Interpretasi Asimetris Pertanggungjawaban Pidana Korporasi di Indonesia Kajian Putusan No 862 K/Pid.Sus/2010. *Jurnal Dictum Kajian Putusan Pengadilan, 12*, 28.

Ali, M. (2020). *Overpenalization dalam Hukum Pidana.* Yogyakarta: UII Press.

Ardika, I. K. (2018). Relevansi Sanksi Pidana Bagi Koruptor yang Merugikan Keuangan dan atau Perekonomian Negara . *Jurnal Kertha Semaya, 8*(6), 882.

Arief, B. N. (2001). *Masalah Penegakan Hukum dan Kebijakan Penanggulangan Kejahatan.* Bandung: PT. Citra Aditya Bakti.

Arief, B. N. (2013). *Kapita Selekta Hukum Pidana.* Bandung: PT. Citra Aditya Bakti.

Ashworth, A. v. (2005). *Proportionate Sentencing: Exploring the Principles.* New York: Oxford University Press.

Brenner, M. D. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, 143-154.

Colvin, E. (1995). Corporate Personality and Criminal Liability. *Criminal Law Forum*, 8-9. https://doi.org/10.1007/BF01095717

Fairfax, R. A. (2011). From "Overcriminalization" to "Smart on Crime": American Criminal Justice Reform-Legacy and Prospects. *Journal of Law, Economic & Policy*, 608-609.

Hirsch, A. v. (1990). Proportionality in the Philosophy of Punishment. *Criminal Law Forum*, 261.

Hirsch, A. v. (1994). Censure and Proportionality. In R. D. Garland, *A Reader on Punishment.* England: Oxford University Press.

Hodges, M. (2008). CyberCrime: The Reality of the Threat. *Journal of High Technology Law*, 6.

Hudson, B. A. (1996). *Understanding Justice an Introduction to Ideas Perspectives and Controversies in Modern Penal Theory.* Philadhelpia: Philadelpia University Press.

Berry, W. W. (2011). Promulgating Proportionality. *Gerogia Law Review*, 98.

Juniar, A. (2021, July). Mencari Bentuk Pemidanaan Terhadap Pemegang Saham Korporasi . *Jurnal Pakuan Law Review, 7*(2), 114.

K.Brown, D. (2009). Prosecutors and Overcriminalization: Thoughts on Political Dynamics and a Doctrinal Response. *Ohio State Journal of Criminal Law*, 461-463.

Luna, E. (2003). Punishment Theory, Holism, and the Procedural Conception of Restorative Justice. *Utah Law Review*, 216.

Marler, S. L. (2002). The Convention on Cyber Crime: Should the United States Ratify? *New England Law Review*, 183.

Marzuki, P. M. (2006). *Penelitian Hukum.* Jakarta: Prenada Media.

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 12, Issue 02, 2021, pp. 267-281

Mulasari, L. (2012, April). Ajaran Pertanggungjawaban Pidana Korporasi dalam Kebijakan Hukum Pidana di Bidang Mayantara. *Jurnal Hukum dan Dinamika Masyarakat, 9*(2), 115. http://dx.doi.org/10.36356/hdm.v9i2.301

Murphy, S. D. (2001). Contemporery Practise of United States relating to International Law. *Amercian Journal of International Law*, 890. https://doi.org/10.2307/2555235

Putri, H. (21-22). Ancaman Pidana terhadap Delik Penghinaan dalam UU ITE. *Majalah Info Singkat Hukum*, 2016.

Ramli, A. (2003). *Perkembangan Cyber Law terhadap Pemanfaatan Teknologi Informasi di Indonesia.* Jakarta: Badan Pembinaan Hukum Nasional.

Rauf, A. (2019, Februari). Aspek Pidana dalam Penyebaran Informasi Melalui Media Elektronik. *Prosiding Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, 8*(1), 92-93.

Salsa, S. N. (2020). Mutual Legal Assistance dalam Penyidikan Tindak Pidana Perdagangan Manusia melalui Media Sosial sebagai Kejahatan Terorganisasi Transnasional. *Procceding National Conference For Law Studies :Pembangunan Hukum Menuju Era Digital Society* (p. 1139). Jakarta: Fakultas Hukum UPN Veteran .

Setiyawan, W. B. (2020, November). Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. *Jurnal USM Law Review, 3*(2), 286-287. http://dx.doi.org/10.26623/julr.v3i2.2773

Sheley, E. L. (2019). Tort Answers to the Problem of Corporate Criminal Mens Rea. *North Carolina Law Review*, 788-789.

Smith, S. F. (2012). Overcoming Overcriminalization. *Journal of Criminal Law and Criminology*, 540.

Suartha, I. D. (2018). Kebijakan Hukum Pidana dalam Pertanggungjawaban Tindak Pidana Korporasi di Indonesia. *Jurnal Kertha Wicaksana, 12*(1), 7-8. https://doi.org/10.24843/JMHU.2016.v05.i04.p10

Sulisrudatin, N. (2019, September). Analisa Kasus Cyber Crime Bidang Perbankan berupa Modus Pencurian Data Kartu Kredit. *Jurnal Ilmiah Hukum Dirgantara, 9*(1), 31-31. https://doi.org/10.35968/jh.v9i1.296

Supancara, I. B. (2007). *Peran Kerjasama Internasional dalam dalam Pencegahan dan Penanggulangan Cyber Crime.* Jakarta: Badan Pembinaan Hukum Nasional.

Suseno, S. (2012). *Yurisdiksi Tindak Pidana SIber.* Bandung: PT. Refima Aditama.

Todd, H. (2015). Overcriminalization's New Harm Paradigm. *Venderbitl Law Review*, 1197.

Weissmann, A. A. (2007). A New Approach to Corporate Criminal Liability. *American Criminal Law Review*, 1319.

Wisnusubroto, A. (2011). *Konsep Hukum Pidana Telematika.* Yogyakarta: UAJY Press.

Article History
Submitted 18 November 2020 - Revision Required 27 November 2020 - Accepted 5 October 2021