International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 12, Issue 8, 2020

Impact Analysis of Information and Electronic Transactions Law (Law Number 19 Year 2016) on the Level of Cyber-Crime in Social Media

H. Nurianto RS[a], [a]Postgraduate Legal Studies, Mahendradatta University Ken Arok Street, No.10-12 Denpasar-Bali,

This study was aimed to determine the impact of law number 19, year 2016 about information and electronic transactions (UU ITE) on the level of cyber-crime in social media. This research was a qualitative study with a normative juridical approach. The method used in this research comprised a literature study and exploratory methodology involving secondary data. The object examined in this study was Law Number 19, year 2016 and other relevant sources. Crimes involving social media have become increasingly diverse alongside the development of information technology. Before the enactment of the ITE Law, several criminal cases involving information technology as a medium did not have clear laws. However, with the enactment of Law Number 19, Year 2016 which was a result of the refinement of Law Number 11, Year 2008, cyber-crime can now be prosecuted with strict and binding sanctions. This research is based on data from 2019 cyber cases that occurred which were dominated by cases of fraud and the spread of provocative content. Information from the Indonesian Cyber-crime Directorate indicates that the number of cyber-crimes from 2016-2019 increased. The increasing number of cyber-crimes was proportional to the increasing number of social media users. Even though the numbers of cyber-crime incidence increased, criminal acts that were not previously regulated in the Criminal Code at least with the law number 19 of 2016 can be dealt with according to the rules and sanctions in force.

Key words: *Cyber-crime, social media, law number 19 year 2016.*

Background

Technological developments in the industrial era 4.0 have an impact on the changing of all community activities that are mostly based on technology and are online. With this paradigm, the internet has become a basic obligation in this era. All information can be accessed online through electronic devices in just seconds. Through devices that are connected to the internet, people can access anything be it news, education, entertainment, buying and selling transactions or anything else. Of course, with the existence of these developments makes the life of society to be very much easier. However, although the internet itself has a positive impact on people's lives, some individuals use the internet to commit criminal acts. This is a negative impact of the development of technology itself.

Based on observations of trusted news sites, in recent years crime in online media has become more frequent. Various types of crimes that use online media as a medium are increasingly prevalent. Some cases of crime in online media such as data manipulation, espionage, sabotage, provocation, money laundering, hacking, software theft, on-line fraud have become a threat to security stability and national order with a relatively high escalation (Maria, 2017). In addition to this, the development of technology has resulted in freedom of opinion in online media by a number of misused users. As a result of freedom of expression that is not responsible for many circulating HOAX news, hate speech (hate speech), cyberbullying, defamation and many other criminal acts that use online media as a medium. From the development of internet networking technology (networking) other criminal acts that have emerged in the e-commerce field include the occurrence of credit theft, burglary credit cards, ATM cards and others.

Based on this reality, the government and its devices have not been able to keep up with crime techniques that have been carried out with computer technology, especially on the internet and internet networks. Acts against cyber law are very difficult to overcome by relying on conventional positive law, because talking about crime cannot be separated from 5 (five) interrelated factors, namely the perpetrators of crime, victims of crime, social reactions to crime and the law (Maria, 2017). The law is indeed an important instrument in preventing and overcoming crime. However, to make a legal provision for a fast changing legal field, such as information technology, is not an easy thing. This is where often laws (regulations) quickly become obsolete when regulating fields that experience rapid changes, so the situation is like experiencing a vacuum (vacuum recht). With such a variety of criminal acts that emerged through online media, therefore Law Number 11 year 2008 concerning Electronic Information and Transactions (UU ITE) appeared. The existence of the ITE Law originated from several studies aimed at forming regulations in the field of information and communication technology in Indonesia. In fact these studies are limited research aimed at enhancing the development and utilization of telecommunications. Until 2003, a bill was

formed called the Information and Electronic Transaction Bill (ITE Bill). In 2005 the Indonesian Ministry of Communication and Information took steps to finalize the design, until it was completed in March 2008 (Atmaja, 2014).

The use of information and communication technology has changed the behavior of people to human civilization globally. This has been stated in Law of the Republic of Indonesia Number 11 Year 2008 Regarding Information and Electronic Transactions, which has been revised in Law of the Republic of Indonesia Number 19 year 2016 concerning Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. The development of information and communication technology has caused world relations to become unlimited, causing social, economic, and cultural information changes. On the basis of this, the so-called cyber law or cyber law was born.

Juridically, activities in cyberspace cannot be approached with conventional legal measures and qualifications, because there will be too many difficulties and things that get away from the enactment of law. By issuing Law Number 19 Year 2016 which is the result of revision of Law Number 11 Year 2008 is an appropriate step for the government to deal with criminal acts that escape the articles of the Criminal Code. However, despite the fact that there are several articles which seem to be multiple interpretations between the ITE Law and the Criminal Code, this does not reduce the meaning of the law itself which incidentally is binding. Seeing so many phenomena and assumptions arising in the community related to crime in online media and the ITE Law that have been in effect, based on the background above, the purpose of this study is to find out how the impact of Law Number 19 Year 2016 on the level of criminal acts in the media social.

Research Methods

This research was a qualitative research with a normative juridical approach. Normative Juridical Approach was a problem approach by looking at, analyzing and interpreting theoretical matters concerning legal principles in the form of conceptions, statutory regulations, views, legal doctrines and related legal systems (Leuwol, 2018). This type of approach emphasizes obtaining information in the form of legal texts relating to the object under study. The method used in this research was literature study and exploratory method from the data of the brother. The objects examined in this study are Law Number 19 Year 2016 and other relevant sources. This study aimed to analyze the impact of Law Number 19 Year 2016 regarding Information and Electronic Transactions on the level of criminal acts on social media. Data obtained from the results of the study will be analyzed descriptively.

Results and Discussion

Substance of Law Number 19 Year 2016 Amendment to Law Number 11 Year 2008 Concerning Information and Electronic Transactions

Law Number 19, Year 2016 amendments to Law Number 11, Year 2008 form the Law on Information and Electronic Transactions (ITE Law) having a wide content and scope in regulating cyberspace, although on some sides there are still less direct regulations and there's also something missing. If the material content is analyzed, it appears that the ITE Law adheres to two regulatory models, namely: (1) Arrangements which favor the strict separation of legal material so that the regulations made are narrow and specific to certain sectors. (2). A regulation that is comprehensive in the sense of material content that is regulated covers broader matters tailored to the needs that currently occur (Sidik, 2016). So that the regulation will include aspects of material civil law, civil procedural law and criminal law (although it can be in the form of certain legal guidelines) of proof and criminal law. Referring to the two models mentioned above, the ITE Law itself tends to follow this second regulatory model.

The main material summarized of ITE Law is as follows: (1) Principles and Objectives. (2) Information, documents and electronic signatures; in this case, electronic signatures are recognized to have the same legal force as conventional signatures (wet and stamped ink). (3) Organizer of Electronic Certification and Electronic Systems. (4) Electronic evidence that is recognized to have the same legal force as other evidence recognized in the Criminal Procedure Code. (5) Electronic Transactions (e-commerce). (6) Domain name regulation, Intellectual Property Rights and protection of personal rights. (7) Prohibited acts, explained in Chapter VII (articles 27 to 37) include: (a) Article 27 (Asusila, Gambling, Humiliation, Extortion). (b) Article 28 (Deceptive and Misleading News, News of Hatred and Hostility) (c) Article 29 (Threats of Violence and Scare) (d) Article 30 (Computer Access of Other Parties Without Permission, Cracking) (e) Article 31 (Tapping, Amendment, Disappearance of Information) (f) Article 32 (Transfer, Destruction and Opening of Confidential Information) (g) Article 33 (Viruses, Making the System Not Working) (h) Article 35 (Making it appear as Authentic Documents). (8) Settlement of disputes. (9) The role of government and the role of the community (10) Investigation. (11) Criminal provisions (Sidik, 2013).

Based on the main material and the form of regulation mentioned above, it can be seen that there are at least eleven breakthroughs made by Law No. 19 of 2016 concerning Electronic Information and Transactions, namely: (1) The first law relating to the use of Information and Communication Technology (ICT) as well as Electronic Information and Transactions (ITE). (2) Be extra territorial; applies to every person who is in the Interior (DN) and Overseas (LN) who has legal consequences in the Republic of Indonesia. (3) Ensuring legal certainty for

people conducting electronic transactions. (4) Electronic evidence is recognized as any other evidence regulated in the Criminal Procedure Code (KUHAP). (5) Electronic Signature (TTE) is recognized to have the same legal force as a Conventional Signature (wet ink and seal). (6) Providing formal legal definitions of various matters relating to the use of Information and Communication Technology (ICT). (7) Electronic Information and / or Documents and / or their printouts are legal evidence and have legal consequences. (8) Determine acts that are prohibited in the use of Information and Communication Technology (ICT). (9) Establish sanctions for violations committed. (10) Encouraging economic growth in Indonesia as an effort to prevent Information Technology (IT) based crime. (11) Protecting the community of service users by utilizing Information Technology (IT) (Sidik, 2013).

Cyber-crime as referenced in Law Number 19, year 2016 concerning Information and Electronic Transactions in a juridical perspective, especially in the scope of criminal law, was subject to many important breakthroughs including the following;

a. Careful affirmation of several terms related to the world of mayantara, for example understanding of computers, data, electronic transactions, and others;
b. Many regulated criminal acts have referred to the provisions stipulated in the Convention on cyber-crime, both criminal acts that target computers and use computers as crime tools;
c. Some traditional crimes that use computers, such as gambling, pornography, unpleasant acts, defamation, insults and others that have been made a crime;
d. Threats for every person who commits a crime in the form of a criminal type (strafsourt) use a cumulative-alternative threat system, and the length of conviction or the magnitude of the threat of a fine (strafmaad) is quite high compared to the threat in conventional criminal law;
e. An electronic signature (digital signature) is recognized as evidence that has the same legal force as a conventional signature that uses wet ink and stamped. Electronic mail (e-mail), websites, and other virtual devices have been recognized as legal evidence so that they can be used as legal evidence in criminal justice processes, other than as regulated in Article 184 of the Criminal Procedure Code;
f. If a corporation commits a criminal offense also is threatened with a crime, even the threat of a penalty is more severe than that of a human;
g. The scope of the enactment of UU-ITE is for every person who commits legal actions in the territory of Indonesia and abroad who have legal consequences in Indonesia (Maria, 2017).

The revision of the ITE Law was carried out on 8 Articles with the addition of 2 Articles. The amended articles are Article 1, Article 26, Article 31, Article 40, Article 43, Article 45, and

Elucidation of Article 5 and Explanation of Article 27. The details are presented in Table 1 below.

Table 1: The Revision of Law Number 11 year 2008

Article	The Change
Article 1	Addition of 1 number, which is the definition of "System Operator Electronic"
Article 26	Addition of 3 paragraphs, namely the existence of Electronic System Provider obligations and provisions regarding procedures for deleting Electronic Information and / or Electronic documents are regulated in government regulations (the right to be forgotten).
Article 31	Changes to paragraphs (2) and (3) are related to interception and interception.
Article 40	Adds 2 verses, changes to paragraph (6), and Explanation of paragraph (1) related Government obligations to prevent dissemination and use of Electronic Information and / or Electronic Documents that have prohibited cargo in accordance with statutory provisions; and the authority of the Government to terminate access.
Article 43	Changes to paragraph (2), paragraph (3), paragraph (5), paragraph (6), paragraph (7), and paragraph (8), as well as the addition of one verse. This article deals with the authority of Investigators for Civil Servants (PPNS), and the implementation of their duties and authorities.
Article 45	Amendments related to criminal provisions against violations in

	Article 27 paragraph (3) concerning defamation or defamation, and affirmation of criminal acts of defamation or defamation is a complaint offense.
Article 45A dan Article 45B	Addition of 2 Articles, namely Article 45A and Article 45B. The addition of these articles is related to technical writing in the Law.
Elucidation of Article 5	Changes in Explanation as the implications of the Court's Decision Constitution.
Elucidation of Article 27	Changes in explanation that include definitions of words / phrases "Distribute", "transmit" and phrase "make accessible" and affirm that the provisions regarding defamation and / or slander, as well as extortion and / or threats refer to the Criminal Code (KUHP).

(Mahayoni, 2016)

Criminal Acts on Social Media

Broadly speaking, social media can be regarded as an online media, where users (users) can share, participate, and create accounts in the form of blogs, forums and social networks using internet-based applications supported by information technology to create virtual world space (Rifauddin, 2016). Social Media has the following characteristics:

a. The content submitted is shared with many people and is not limited to one specific person.
b. The contents of the message appear without going through a gatekeeper and there are no barrier gates.
c. The contents are delivered online and directly.
d. Content can be received online in a faster time and can also be delayed acceptance depending on the time of interaction that is determined by the user.
e. Social media (social media) makes its users as creators and actors who allow themselves to actualize themselves.

f. In social media content there are a number of functional aspects such as identity, conversation (interaction), sharing (presence), presence (existence), relationships (relations), reputation (status) and groups (groups) (Rifauddin, 2016).

The high internet usage in Indonesia is one of the supporting factors in the development of such friend and information site networks in Indonesia. Based on data from the Ministry of Communication and Information, internet and mobile user statistics in Indonesia in 2014, developed reaching 15% or 38,191,873 of the total population value of 251,160,124, while indicators of social media users in Indonesia were around 15%, the percentage was almost the same as the total development of internet users in Indonesia or in other words almost all internet users in Indonesia have social media accounts. Social media users in Indonesia spend time accessing their social media accounts on average around 2 hours 54 minutes and around 74% of social media users in Indonesia on average access their accounts via mobile / smartphone (Kominfo, 2014).

Crime in online media is termed cyber-crime. In general, what is meant by computer crime or cyber-crime is a crime committed by a person, group or corporation using computer facilities and other telecommunications tools such as mobile phones as a negative impact of the development of internet applications (Ali, 2012). The scope of the scope of cyber-crime are, (a) piracy; (b) fraud; (c) theft; (d) pornography; (e) harassment; (f) forgery; (g) defamation; (h) gambling; and others. Based on literature and practice, cyber-crime has several characteristics, namely;

a. Acts committed illegally, without rights or which are unethical that occur in cyber space / territory, so it cannot be ascertained which state jurisdiction is applicable to them.
b. The act is carried out using any equipment connected to the internet.
c. These actions result in material or immaterial losses which tend to be greater than conventional crime.
d. The culprit is the person who masters the use of the internet and its applications.
e. Such acts are often carried out transnationally / across national borders.

Some forms of crime that are closely related to the use of information technology based on computers and telecommunications networks, in some literature and practice are grouped in several forms, including:

a. Unauthorized Access Computer System and Service Crimes committed by entering / infiltrated a computer network system illegally, without permission or without the knowledge of the owner of the computer network system entered.
b. Illegal Contents Is a crime by using data or information to the internet about something that is not true, unethical, and can be considered unlawful or disturbing public order.

c. Data Forgery It is a crime to falsify data on important documents stored as scriptless documents over the internet.
d. Cyber Espionage is a crime that utilizes the internet network to carry out spy activities against other parties, by entering the target party's computer network system.
e. Cyber Sabotage and Extortion crime is effected by making interference with, destruction or destruction of data, computer programs or computer network systems that are connected to the internet.
f. Offense against Intellectual Property crime is directed against intellectual property rights owned by other parties on the internet. For example, imitating the appearance on a web page of a site belonging to someone else illegally, broadcasting information on the internet that turns out to be confidential trade information of others and so on (Mansur, 2005).

Analysis of the Impact of Law Number 19 Year 2016 on the Level of Criminal Acts in Social Media

On November 25, 2016 the new ITE Law Revision was enacted with Law No. 19 of 2016. In accordance with Article 87 of Law No. 12 of 2011 which states that "Statutory Regulations come into force and have binding power on the date of promulgation, unless otherwise stipulated in the relevant Regulations", then since November 25, 2016 is also Law No. 19 of 2016 has legal force and every Indonesian is considered to know and must implement it. UU no. 19 of 2016 which came from a joint agreement in the plenary meeting between the Parliament and the Government on November 27, 2016 has an important mandate for the public to build ethics in the use of social media so that they are more careful in the realm of social media.

In Law No. 19 of 2016 also the public is prohibited from making and disseminating information that is accusation, slander, or racial intolerance. In this law it is also regulated that what can be ensured is not only those who make it, but also those who distribute and transmit it. So it is necessary for media users to always be ethical so that media users do not easily spread information that can cause hatred towards certain groups. As for Law No. 19 of 2016 is not intended to prohibit people from arguing or criticizing on social media. It must be understood that Article 28E paragraph (3) expressly states that "Everyone has the right to freedom of association, assembly and expression." So that it is also known that freedom on social media is freedom which is a Human Rights (HAM) protected by the constitution.

However, it is also necessary to look at Article 28J paragraph (2) of the 1945 Constitution of the Republic of Indonesia, because in that article it also states that "In exercising their rights and freedoms, every person is obliged to submit to limitations imposed by law with the sole purpose of guaranteeing recognition and respect for the rights and freedoms of others and to

meet fair demands in accordance with moral considerations, religious values, security and public order in a democratic society. "Therefore, human rights are not freedoms without limitations but the state needs to set boundaries but rather because someone's human rights are also limited by other people's human rights in accordance with the mandate of Article 28J paragraph (2) of the 1945 Constitution of the Republic of Indonesia.

Cyber -crime in terms of the Criminal Code

Empirically the definition of crime can be seen from two perspectives, the first is crime in a juridical perspective where crime is formulated as an act which the state is given a criminal offense (Maria, 2017). The granting of the crime is intended to restore the balance disturbed by the act. Such acts or crimes in Criminal Law are commonly referred to as Criminal Acts. Second, crime in a sociological (criminological) perspective is an act that is sociologically a crime, but from a juridical point of view it is not a crime (Maria, 2017).

This is regulated in Chapter I of the First Book of the Criminal Code which consists of 9 articles ranging from Article 1 to Article 9. Scope of the Applicability of Criminal Law in Cyber Crimes the Indonesian Criminal Code (KUHP) has provided clear arrangements regarding the limits of entry into force criminal law rules. In Article 1 of the Criminal Code set about the limits of the validity of criminal law according to the time or time the crime occurred. While Article 2 through Article 9 of the Criminal Code regulates the limits of the enactment of criminal law in accordance with the place of action. Basically, there are two things that cause regulations in the Criminal Code to have a limited reach, namely: a) Limitations on the regulation of types of criminal acts. This is very reasonable, considering the atmosphere that influences the formulation of the Criminal Code we are very much different from the present conditions loaded with the rapid development of information technology. b) Limitations in the regulation of the perpetrators of criminal acts. In an era of information technology such as the current, determination of who can qualify as a perpetrator of a criminal act is more complex.

Criminal Law in the Field of Cyber Crimes in Indonesia

Before the enactment of UU-ITE, the court used the provisions in adjudicating cyber-crime to be the Criminal Code and the provisions in laws outside the Criminal Code governing criminal offenses. Provisions in the Criminal Code used to deal with cyber-crime are provisions on Counterfeiting (Articles 263-276), Fraud (Articles 378-395) and Property Damage (Articles 407-412). Whereas the provisions of legislation outside the Criminal Code that can be used in dealing with cyber-crime (material or formal criminal law) include the following;

a. RI Law No. 3 of 1971 concerning Eradication of Corruption, which was then replaced by RI Law No. 31 of 1999 concerning Eradication of Corruption, and finally amended by RI Law No. 20 of 2001 concerning Amendments to RI Law No. 31 of 1999 concerning Eradication of Corruption;
b. RI Law No. 6 of 1982 concerning Copyright, then amended through RI Law No. 7 of 1987 concerning Amendments to RI Law No. 6 of 1982 concerning Copyright. Finally the two Laws were replaced by RI Law No. 19 of 2002 concerning Copyright, RI Law No. 28 of 2014 concerning Copyright substitute for RI Law No. 19 of 2002 concerning Copyright;
c. RI Law No. 7 of 1992 concerning Banking junto Law No. 10 of 1998 concerning Banking;
d. RI Law No. 5 of 1999 concerning Business Competition;
e. RI Law No. 36 of 1999 concerning Telecommunications;

Based on data from the Directorate of Cyber Crime (Dittipidsiber) the Criminal Investigation Police noted that there were 4,586 cases of cyber-crime from January to December 2019 (Patolisiber, 2019). This number continues to increase from 2016 to 2019. From the report, Kasubdit III Dittipidsiber Bareskrim Polri Kombes Kurniadi said fraud cases and the dissemination of provocative content became the most dominating number of cyber-criminal cases. This provocative content covers negative political issues. The following are statistics on the number of cyber-crime reports compiled by the Indonesian Cyber Crime Directorate which are presented in Table 2 below.

Table 2: Number of Reports on Cyber Crimes in Indonesia

Year	2016	2017	2018	2019
Online Fraud	1.570	1.430	1.781	1.617

Disseminating Provocative Content	1.047	1.157	1.724	1.769
Pornography	155	180	266	364
Illegal Access	147	153	263	248
Gambling	26	24	35	35
Extortion	17	22	36	132
Data Theft	20	47	88	143
Electronic Hacking Systems	0	35	43	148
Illegal Interception	15	10	5	3
Changing the Site Appearance	42	5	5	4
System Disruption	71	13	1	9
Data Manipulation	0	33	113	114
Report Total	3.110	3.109	4.360	4.586

Source: Directorate of Cyber Crime (www.patrolisiber.id)

If seen from the data above, it appears that there has been an increase in cyber-crime from year to year. The factors causing the increase in cyber-crime are: 1) Public legal awareness, 2) Security, 3) Law Enforcement (Ali, 2013). Indonesian people's legal awareness in responding to cyber-crime activities is still lacking. This is caused, among others, by the lack of understanding and knowledge (lack of information) of the community against types of cyber-crime. This Lack of Information has caused obstacles in dealing with cyber-crime, in this case constraints relating to legal compliance and the process of controlling the public for any activity that is allegedly related to cyber-crime.

In addition to public legal awareness, law enforcement factors are often the cause of the rise of cyber-crime (Ali, 2013). This is motivated by the lack of law enforcement officials who understand the ins and outs of information technology (internet), so that when a criminal is arrested, law enforcement officials have difficulty finding evidence that can be used to ensnare the perpetrator, especially if the crime committed has an operating system that very complicated. The efforts to overcome the occurrence of cyber-crime in social media, which consists of both penal and non-penal efforts. Where the penalties consist of giving sanctions to the perpetrators by giving prison sentences in accordance with what has been stipulated in the ITE Law to provide a deterrent effect. While the non-penal effort is to provide counseling or outreach to the wider community regarding the impact of electronic media if not used wisely, the ethics of using social media by providing legal knowledge about the ITE Law (Febriyani, 2018).

The enactment of Law Number 19 Year 2016 has positive and negative impacts in Indonesia. The positive impact of the enactment of this law is that cyber-crime has its own legal umbrella, so that the handling of sanctions can be carried out more precisely in accordance with the law. In addition, with Law Number 19 Year 2016 the public is expected to become a

wise society in using social media because the perpetrators of crime in the cyber world will be subject to strict sanctions. This is in line with the opinion of Members of the Sukamta DPR Commission I, which states that the direction of the political policy in the revision of the ITE Law is more towards forming a civilized nation. He believes that the main spirit of the revised ITE Law spirit is at least two things, namely the community and government aspects. According to him, examined from the aspect of society, there is freedom in politely issuing opinions. In addition, the public can enjoy a healthy and well-maintained internet.

Freedom of opinion is guaranteed by the constitution and other laws as derivative rules. However, it is true that they must not violate the rights of others when expressing their opinions in public, behaving badly, let alone attacking others with slander. In ITE law, legal protection of freedom of opinion is indeed limited. The limitation includes not allowing intentional distribution, dissemination of electronic information, electronic documents containing violations of decency, insults, defamation, extortion, threats, hoaxes, and things that trigger hatred based on SARA (Permatasari, 2019).

Based on observations from several sources, it is stated that with the UU-ITE all forms of crimes arising from social media can be dealt with firmly whether from the perpetrators, disseminators or parties involved in these crimes. So that a few years after the issuance of the ITE Law, crime in the online world can be controlled handled in accordance with the rules and sanctions in force in the law. Although the enactment of the ITE Law has had a positive impact on society, there is a negative side to the enactment of Law No. 19 of 2016, which is from the government side, law enforcement is now not easy to detain perpetrators of alleged defamation or slander through cyberspace. Including not carrying out detention of people who expressed their critical attitude towards public policy. The Minister of Communication and Information, Rudiantra, stated that along with the development of the use of social media, a number of articles in the ITE Law were considered detrimental, even threatening freedom of expression and opinion. The reason, a number of articles tend to be multiple interpretations and overlap with other legal regulations. The polemic arose after many legal cases related to violations of the ITE Law (Online Law, 2016).

Apart from positive and negative arguments of Law No. 19 of 2016, Indonesia as a state of law, is obliged to implement the rules set out in the law. Although in several articles there are still multiple interpretations between articles in the Criminal Code, the purpose of this law is to protect Indonesian people from cyber-crime. The positive impact seen in the community after the enactment of this law is freedom of opinion which is responsible. Society can freely express opinions but must be wiser and responsible for the utterances expressed through social media. With the enactment of the ITE Law the public is expected to be smarter and more vigilant in using the internet, maintaining ethics in communicating and disseminating information, as well as avoiding SARA, radicalism, and pornographic content. With the

issuance and enforcement of the ITE Law, the management, use and utilization of information and electronic transactions must continue to be developed through the legal infrastructure and regulations. So that its use can be carried out safely to prevent its misuse by paying attention to the religious, social and cultural values of the Indonesian people, as well as to maintain, preserve, and strengthen national unity and integrity based on legislation in the national interest.

Conclusion

Cyber -crime acts from 2016 to 2019 have continued to increase. The increase was offset by an increase in the number of social media users. Cyber-crimes that occurred during 2016 until 2019 were increasingly diverse, but the cases that dominated for four years were cases of online fraud and the dissemination of provocative content. Although there has been an increase in number, but with the enactment of Law Number 19 Year 2016 which is a revision of Law Number 11 Year 2008 on Information and Electronic Transactions has succeeded in providing binding and strict rules against cybercriminals. Cyber-crime that was not originally contained in the Criminal Code in the presence of the ITE Law at least has a clear legal umbrella with strict and binding rules. The enactment of Law Number 19 Year 2016 cannot be separated from the pros and cons of several parties. The impact arising from the enactment of the law also has positive and negative impacts. Basically the law applies to protect Indonesian citizens from cyber-crime, therefore as a law-abiding Indonesian citizen, citizens must act wisely regarding the use of electronic media. Acting appropriately with social media use and not in violation of existing rules is the most appropriate way to reduce social media crime.

REFERENCES

Ali, M. H. (2012). *Cyber-crime Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang ITE (Perspektif Hukum Pidana Islam)*. (Doctoral dissertation, Universitas Islam Negeri Alauddin Makassar).

Atmaja, A. E. 2014. "Kedaulatan Negara di Ruang Maya : Kritik UU ITE Dalam Pemikiran Satipto Rahardjo". *Jurnal Opinio Juris* , XVI(2), 71-72.

Direktorat Tindak Pidana Siber. 2019. *Statistik Jumlah Laoran Polisi Yang Dibuat Masyaraka*t. Https://Patrolisiber.Id/Statistic (Diakses Pada Tanggal 10 Januari 2020).

Febriyani, M. And Sunarto, B.R.H., 2018. "Analisis Faktor Penyebab Pelaku Melakukan Ujaran Kebencian (Hate Speech) Dalam Media Sosial" *Jurnal Poenale*, 6(3).

Leuwol, T., 2018. "Penerapan Sanksi Pidana Terhadap Pelaku Cyber-crime Yang Menyebarkan Isu Suku, Ras, Agama Dan Antar Golongan (Sara) Melalui Media Sosial Ditinjau Dari Undang-Undang Ite Nomor 19 Tahun 2016". *Jurnal Lex Crimen*, 7(2).

Mahayoni, M., 2019. "Aspek Hukum Penggunaan Sosial Media Sesuai Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008". *Problematika Hukum*, 3(1), Pp.15-50.

Mansur, Dikdik M. Arif & Elisatris Gultom, 2005*, Cyber Law (Aspek Hukum Teknologi Informasi)*. Bandung : PT Refika Aditama.

Maria, A., Syahrin, A. And Hasibuan, S., 2017. "Kejahatan Siber Sebagai Dampak Negatif Dariperkembangan Teknologi Dan Internet Di Indonesia Berdasarkan Undang-Undang No. 19 Tahun 2016 Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Dan Persfektif Hukum Pidana". *Jurnal Mahupiki*, 1(01).

Permatasari, I. A., & Wijaya, J. H. (2019). "Implementasi Undang-Undang Informasi dan Transaksi Elektronik Dalam Penyelesaian Masalah Ujaran Kebencian Pada Media Sosial". *Jurnal Penelitian Pers Dan Komunikasi Pembangunan*, 23(1), 27-41.

Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Nomor 58 Tahun 2008.

Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Sidik, S., 2013. Dampak Undang-Undang Informasi Dan Transaksi Elektronik (Uu Ite) Terhadap Perubahan Hukum Dan Sosial Dalam Masyarakat. Jurnal Ilmiah Widya, 4(2).