

# The Nature of Article 27 the Law on Information and Electronic Transaction in Indonesia Practice

Maskun\*, Nur Fitriani Khairunnisa\*\*

\* Lecturer at International Law Department, Faculty of Law - Hasanuddin University.

\*\*Assistant Lecturer at International Law Department, Faculty of Law - Hasanuddin University and Postgraduate Student at Postgraduate Hasanuddin University.

## Abstract

Indonesia has been known as one of top five social media worldwide users. The Indonesia people are one of the biggest contributions to information sharing on Internet. Indeed, the increase number of social and economic activities with constellation of society has entered information-oriented society, not only in Indonesian society but also in global society. Due to the transnational dimension of cybercrime, the legal instruments are the same for developing and developed countries. Mechanism of cooperation across national borders to solve and prosecute crimes is complex and slow. The violations on Article 27 of the Law of Number 11 of 2008 Concerning Electronic Information and Transactions, in particular for Article 27 section (3), become the most common cases that occurred in Indonesia. According to SAFENet Voice, there was an increase of reported cases from 2013 to 2014. Approximately 53% or 41 of 72 cases occurred in 2014.

**Keywords:** The Nature of Article 27, Electronic Transaction, Indonesia Practice

## 1. Introduction

Indonesia has been known as one of top five social media worldwide users. The Indonesia people are one of the biggest contributions to information sharing on Internet.<sup>1</sup> Indeed, the increase number of social and economic activities with constellation of society has entered information-oriented society, not only in Indonesian society but also in global society. The information and technology system basically has been used in several lives' sectors such as e-commerce, electronic education, tele-creation, transportation, industry, tourism, environmental and entertainment sectors.<sup>2</sup>

Information and Communication Technology (hereinafter referred to ICT) has contributed positively to the economic growth in every country. Positive economic growth occurs because ICT provides solutions as an enabling of a process. It has proved that the proper infrastructure of ICT is able to support socio-economic development.<sup>3</sup> A rapid development in the ICT sector has given not only a positive impact on economic growth, but also a big threat for cyber security in Indonesia. The current threat for every country nowadays is resulted from both physical and cyber threat. In this context, the cyber threat is potentially to destroy the economy and destabilize the country's security. To anticipate the threats, the government needs to develop a defense and security system and strategy.<sup>4</sup>

Basically, the technology is created to satisfy the specific needs of the human being. After it is created, the technology become more and more develops everyday in order to be more effective and efficient to fulfill the needs of the society. Furthermore, after the technology is established and developed, the use of technology can be appropriate with the creation and development even though considering the first purpose, as known as double-edged perspectives and information technology and communication as well.<sup>5</sup>

Started from cybernetics and the role of internet, the important role in building virtual world is known as cyberspace. Cybernetics is a science that regulates and directs system from the simplest aspect to the most complex one by understanding its system and acts, then set outside the system as tools, and method. Thus, in the computer development, occurred symbiosis between human and machine. Cybernetics is able to facilitate problem solving or solution from formulated issues.<sup>6</sup>

<sup>1</sup> See Mika Isac Kriyasa. *Case of Defamation through Social Media in Indonesia: Is it Possible for a Company to Make a Report to the Police?*. News & Updates, Legal Headlines.

<sup>2</sup> See Danrivanto Budhijanto. *Telecommunication Law, Broadcasting and Information Technology: Regulation and Convergency* (Hukum telekomunikasi, Penyiaran dan Teknologi Informasi-Regulasi dan Konvergensi). PT Refika Aditama. Bandung, 2010.

<sup>3</sup> Fariyasa Setiadi. *An Overview of the Development Indonesia National Cyber Security. Paper is presented on: International Conference on Information Technology, E-Government and applications*, ICITEA, Jakarta, 2012, p.1.

<sup>4</sup> Ibid, p.2.

<sup>5</sup> Josua Sitompul. *Cyberspace, Cybercrimes, Cyberlaw – an overview to Criminal Law Aspects (Tinjauan Aspek Hukum Pidana)*, PT. Tatanusa. Jakarta. 2012, p.6.

<sup>6</sup> Ibid.p.8.

ICT has become parts of human's life aspects. Even though from the scale of distribution percentage and population penetration of internet is still low, Indonesia is one of states with the biggest internet users in Southeast Asia.<sup>1</sup> Technological advancement has dual facets with divergent results. Electronic media have facilitated communication with friends and family and the sharing of the information. They are a source of entertainment and provide tools for socializing.<sup>2</sup> Cellphone is not only used as communication tool but also as the tool of information. Internet uses has influenced computation expense and information processing. Internet makes life easy, not only in technology of information and communication, but also in education, culture, social, politic, and economy. Almost all societies in the world use social medias to communicate, share private message, download, upload pictures, share their location, and for online transaction. Through social media people can share threats and do crimes as well. Freedom to use anonym identity needs solid trust between transaction parties. The basis for the exclusion involves any aspect that distinguishes the victim from a group: race, gender, sexual orientation, outstanding abilities, or having special needs or disabilities.<sup>3</sup> Major risk in amount and value of transactions is getting more and broad.

Many countries highlight that an expedited mechanism for international cooperation procedures in criminal matters involving cybercrime should be developed. Some countries propose that this could be through the strengthening of existing informal police-to-police networks and it could be achieved by further development of existing formal international cooperation channels, including bilateral and multilateral agreements. Some countries emphasized that all options should be implemented in line with international human rights standards, including rights to freedom of expression and to privacy.<sup>4</sup>

Difficulties that can be raised, for example, in determining locus delicti, investigator can easily investigate by collecting evidences and clues and also call forensic laboratory party to find fingerprint. Investigators also hardly find witnesses who were in crime scene. Another difficulty raise in collecting evidences which needs a lot of cost because it needs high technology. These give impacts towards the development of information technology and communication, cybercrime's scope is wider because unlimited to geographical location, this possibly occurred locally, nationally and even internationally. Victims can be from all over the world and causes difficulties in law enforcement process.<sup>5</sup> Therefore, Indonesian government needs law as regulation on people's attitude and behavior from cyberspace – society who has value and interest individually or together that must be protected.

Indonesian government has tried to support the development of information technology in particular management of information and electronic transactions including the law and regulation infrastructure. Therefore, utilization of information technology activities can be conducted safely by pressing negative impacts as minimum as possible.<sup>6</sup> Moreover, the Indonesian government released the Law No 11 of 2008 Concerning Information and Electronic Transactions and forced on April 21, 2008. This law has scope not only in Indonesia and/or conducted by Indonesian citizen, but also applied in outside Indonesia whether conducted by Indonesian citizen, foreigner or Indonesian legal entity, or foreign legal entity that gives legal impact in Indonesia. Considering the utilization of information technology for electronic transactions is universal.

The issues in implementing the Law No 11 often cause confusion, considering the number of information technology users increasing every year by using technological means. Article 27 of the Law No 11 of 2008 Concerning Information and Electronic Transactions mention the prohibited acts such as violating decency, containing gambling, has a charge of insult and / or defamation and has a charge of extortion and / or threatening.<sup>7</sup> The purpose of this study is to examine the elements, which contained in the Article 27 of the Law Number 11 of 2008 and its exercise in Indonesian practice. This research will analyze variables that may effect

---

<sup>1</sup> Indonesia Media Defense Litigation Network and Institute for Criminal Justice Reform, 2000-2010: Indonesia's Freedom of Internet: Struggle Paved the Limit [Briefing Paper Nomor 3 Tahun 2011], Jakarta, 2001 cited in AP Edi Atmaja, *State Sovereignty in Cyberspace: Critics on Law Concerning Electronic Information and Transactions* in Satipto Rahardjo Perspective, *Opinio Juris Journal* Vol. 16, May-September 2014, p.51.

<sup>2</sup> See Ruth Broster and Ken Brien., *Cyber-bullying of Educators by Students: Evolving Legal and Policy Developments*. Unversity of Brunswick Frederiction, p.1.

<sup>3</sup> Sharen Shariff, "Cyber-Bullying and Legal Liability in Today's Schools - See more at: <http://www.cambridgeblog.org/2010/06/cyber-bullying-and-legal-liability-in-todays-schools/#sthash.mqfsCu13.dpuf>. 2010.

<sup>4</sup> United Nation Office on Drugs Crime. *Comprehensive Study on Cybercrime*.

<sup>5</sup> Josua Sitompul. *Op.cit*.p.135.

<sup>6</sup> See Togi Robson Sirait. *Information Validity of Social Media as an Evidence in Defamation Based on The Law No.11 of 2008* (Keabsahan Informasi pada Media Sosial sebagai Alat Bukti dalam Pembuktian Tindak Pidana Pencemaran Nama Baik Berdasarkan UU No. 11 Tahun 2008). *Jurnal Ilmiah*. Universitas Sumatera Utara. Medan. 2014. P.8

<sup>7</sup> Josua Sitompul. *op.cit*, p. 135.

compliance of the exercise in Indonesian practice, why the regulation needs to be applied for and how the society's behavior through the Law that exist in Indonesia.

## 2. The Nature of The Law No. 11 of 2008

Cyber criminals are no different than traditional criminals in that they want to make their money as quickly and easily as possible. Cybercrime prevention can be achieved fairly quickly and in a cost-effective manner. When armed with a little technical advice and common sense, many cybercrime attacks can be avoided. Similar to target hardening for a residence or a business (e.g., lights, locks, and alarms), the more difficult it is for a cyber criminal to successfully attack a target, the more likely he or she is to leave it alone and move on to an easier target.<sup>1</sup>

The improvement of information technology has changed human's perspective regarding activities that only monopolized by physical activities. Internet's birth has changed human's thinking concept in socialization, business and interaction with other humans. It also changes the concept of distance and time drastically. Internet makes world small and unlimited. Every person can connect, talk and have a business with another person who is million away only by typing keyboard and mouse in front of him/her.<sup>2</sup>

The raise of crimes grown and developed in society, there is no crime without society. Due to the transnational dimension of cybercrime, the legal instruments are the same for developing and developed countries. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.<sup>3</sup>

The laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts.<sup>4</sup> The development of information technology including Internet has its own challenge for the development of law in Indonesia. Law in Indonesia requires adjusting with social changing; social changing in society, and legal changing or vise-versa does not proceed together.

However, the references used are selected for the benefit of developing countries. In addition to a broad selection of resources, it provides for a more in-depth study of the different topics.<sup>5</sup> Because the influence of technology development is very tight, it causes the law sees it rigidly. According to the Computer Emergency Response Team Coordination Center (CERT/CC), the number of reported incidences of security breaches in the first three quarters of 2000 has risen by 54 percent over the total number of reported incidences in 1999.<sup>6</sup> Cybercrimes have increased rapidly in Indonesia, unfortunately the regulations are not able to charge the perpetrators with a strict sanctions. Thus, these crimes increase more through the development of information technology and telecommunication.

The draft of this law started since March 2003, Being warned by the development of internet and the increase number of its users, the Indonesian government through The Ministry of Communication and Information Technology set several regulations. One of those is the Law No. 11 of 2008 Concerning Information and Electronic Transactions<sup>7</sup> on 21 April 2008. However, the Law is still several unclear parts. The Law No 11 of 2008 consists of 13 Chapters, 54 Articles which is relatively new, in terms of enactment time and material.<sup>8</sup>

---

<sup>1</sup> National Crime Prevention Council. *Cybercrime Prevention Strategies*. Bureau of Justice Assistance U.S. Department of Justice. United States of America. September 2012.

<sup>2</sup> Togi Robson Sirait. op.cit. p.8.

<sup>3</sup> McConnell International. *Cyber Crime . and Punishment? Archaic Laws Threaten Global Information*. Dec. 2000. p.2

<sup>4</sup> Ibid.

<sup>5</sup> Telecommunication Development Sector. *Understanding Cybercrime: Phenomena, Challenges and Legal Response*. September 2012. The ITU publication *Understanding cybercrime: phenomena, challenges and legal response* has been prepared by Marco Gercke and is a new edition of a report previously entitled *Understanding Cybercrime: A Guide for Developing Countries*. The author wishes to thank the Infrastructure Enabling Environment and E-Application Department, ITU Telecommunication Development Bureau.

<sup>6</sup> See [www.cert.org](http://www.cert.org). Although the following organizations also track reported incidents, global statistics have yet to be compiled: the National Infrastructure Protection Center (NIPC), [www.nipc.gov](http://www.nipc.gov), the Computer Security Institute (CSI), [www.gocsi.com](http://www.gocsi.com), and the Internet Fraud Complaint Center, [www.ifccfbi.gov](http://www.ifccfbi.gov).

<sup>7</sup> AP Edi Atmaja, op.cit.p. 53.

<sup>8</sup> Togi Robson Sirait. op.cit. p.10.

In accordance with main materials and setting forms, it can be known that there are at least eleven breakthrough made by the Law No 11 of 2008 Concerning Information and Electronic Transactions, as followings:<sup>1</sup>

1. The first legislation concerning the use of Information and Electronic Transactions and Information and Communication.
2. Having extra territorial characteristics; it means that it is applied to every person inside the state or abroad who has legal effects in Republic of Indonesia.
3. Ensuring legal certainty for people who conduct electronic transactions.
4. Electronic evidence recognized as well as other evidence provided in the Law of Criminal Procedure (Criminal Code)
5. Electronic signature recognized has legal power equal to conventional signature (ink and stamp)
6. Providing formal legal definition for several matters related to the application of Information and Communication Technology.
7. Information and / or Electronic documents and / or the print results are legal evidence and have a valid legal effect.
8. Defining prohibited acts in the application of Information and Communication Technology.
9. Applying sanctions for offenses that conducted.
10. Encouraging economic growth in Indonesia as part of efforts to prevent crime based on Information Technology (IT).
11. Protecting public service users by applying Information Technology (IT)

Contained materials in the Law of IET are implementation of several international principles that applied in many European, American, and Asian countries. It is UNCITRAL Model Law and Electronic Commerce UNCITRAL Model Law on Electronic Signature, Convention on Cybercrime, EU Directives on Electronic Commerce and EU Directives on Electronic Signature. The Law of IET encompasses material crimes that include cyber crimes, with reference to Convention on Cybercrime. It is not only the material criminal law but also specific formal criminal law to enforce cyber criminal law.<sup>2</sup> As we known, cyberspace is a crime that is not limited by region, the characteristics of a ubiquitous and borderless crime affects not have happened in it that in fact a criminal offense is transnational in nature so that raises the question of locus delicti of the crime of this

### 3. The Article 27 of the Law No. 11 of 2008

The Article 27 of the Law No 11 of 2008 is part of Chapter VII that regulates prohibited acts. Article 27 states that:

- (1) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents against propriety.
- (2) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of gambling.
- (3) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of affronts and/or defamation.
- (4) Any Person who knowingly and without authority distributes and/or transmits and/or causes to be accessible Electronic Information and/or Electronic Records with contents of extortion and/or threats.

As the number of social media has increased rapidly in recent years, the violations on Article 27 of the Law of Number 11 of 2008 Concerning IET<sup>2</sup>, in particular for Article 27 section (3), become the most common cases that occurred in Indonesia. According to SAFENet Voice<sup>3</sup>, there was an increase of reported cases from 2013 to 2014. Approximately 53% or 41 of 72 cases occurred in 2014.

The development of information technology impacts on revolution of criminal forms from conventional to modern of which one of those is gambling.<sup>4</sup> Crime of gambling has been regulated in Article 303 of the Criminal Code and Article 303 bis of the Criminal Code. However, internet gambling has created the eradication of

---

<sup>1</sup> Suyanto Sidik. *Effect on the Law No. 11 of 2008 to Legal Change and Social Society* (Dampak Undang-Undang Informasi dan Transaksi Elektronik terhadap Perubahan Hukum dan Sosial Masyarakat). Jurnal Ilmiah WIDYA. Universitas Bhayangkara Jakarta Raya. p. 5.

<sup>2</sup> Josua Sitompul. op.cit.p.136.

<sup>3</sup> Southeast Asia Freedom of Expression Network (SAFENET) is a network of Southeast Asia bloggers and online activists who dedicated to promote freedom of expression online. Further see <http://safenetvoice.org/>. Accessed on February 10, 2016

<sup>4</sup> Hetty Hassanah, *Internet Gambling According to the Law No. 11 of 2008* (Tindak Pidana Perjudian Melalui Internet Ditinjau dari Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik), *Majalah Ilmiah UNIKOM* Vol. 8, No 2, pg 232. Accessed on file:///Volumes/Rafika's%20Data/Data/Documents/Tindak%20Pidana%20Pasal%2027%20ayat%20(2).pdf

gambling that become more difficult. It can be conducted by anyone and anywhere.<sup>1</sup> One of the internet gambling cases is gambling on the website [www.TebakHuruf.com](http://www.TebakHuruf.com) established by bookies from Hong Kong and Indonesia since 2005.

Moreover, among all the articles in the Law No 11 of 2008 Concerning IET, 92% reported as defamation which stated in the Article 27 section (3) whether from Facebook account, twitter, or even private social media such as line group.<sup>2</sup> According to Indonesian Criminal Code, defamation termed as an insult/defamation against a person, stated in Chapter XVI, Book II of Criminal Code. Explained further in Article 310 paragraph (1) and (2), Article 311 paragraph (1) and Article 318 paragraph (1) Criminal Code.

Based on monitoring of ICJR, from 2009-2015, there were 20 cases of Article 27 section (3), of those prosecuted in court.<sup>3</sup> The most famous case occurred in 2008, Prita Mulyasari Case. Prita Mulyasari was charged under Article 45 paragraph (1) Jo Article 27 section (3) of the Law Concerning Electronic Information and Transactions, Article 310 section (2) of Criminal Code and Article 311 section (1) of Criminal Code.<sup>4</sup> Prita wrote an email to [customer\\_care@banksinarmas.com](mailto:customer_care@banksinarmas.com) regarding her complaint about service from Omni International Hospital and the doctors who examined her. The email went viral on several mailing lists and online forum. Her complaint was taken as defamation by Omni International Hospital then they sued her.

Defamation applied when the aim is to attack the honor of a person of which different from critics or complaints. Therefore, it needs to be considered with elements of crimes in legal provisions. It will not cause second victim due to error observation of a case.<sup>5</sup>

#### 4. Conclusion

The Law of Number 11 of 2008 Concerning IET was made by the government to regulate the actions performed in the cyberspace, even there are still many cases happen and many shortcomings under the this law, so it can cause more cases and more victims. ICT growth in Indonesia gives impact on a high cyber threats. The Indonesian government has tried to address that problem by issued policies and regulations, developed technical and procedures, established organization security, improved capacity building and conducted international cooperation. Therefore, further work is to determine the ideal conditions for cyber security in Indonesia, furthermore by understanding the current conditions and the ideal conditions we can view the gaps that might be improved.

#### References

- Danrivanto Budhijanto. *Telecommunication Law, Broadcasting and Information Technology: Regulation and Convergency* (Hukum telekomunikasi, Penyiaran dan Teknologi Informasi-Regulasi dan Konvergensi). PT Refika Aditama. Bandung, 2010.
- Farisya Setiadi. *An Overview of the Development Indonesia National Cyber Security. Paper is presented on: International Conference on Information Technology, E-Government and applications, ICITEA, Jakarta, 2012, p.1.*
- Hetty Hassanah, *Internet Gambling According to the Law No. 11 of 2008* (Tindak Pidana Perjudian Melalui Internet Ditinjau dari Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik), *Majalah Ilmiah UNIKOM* Vol. 8, No 2, pg 232. Accessed on file://Volumes/Rafika's%20Data/Data/Documents/Tindak%20Pidana%20Pasal%2027%20ayat%20(2).pdf.
- Indonesia Media Defense Litigation Network and Institute for Criminal Justice Reform, 2000-2010: Indonesia's Freedom of Internet: Struggle Paved the Limit [Briefing Paper Nomor 3 Tahun 2011], Jakarta, 2001 cited in AP Edi Atmaja, *State Sovereignty in Cyberspace: Critics on Law Concerning Electronic Information and Transactions* in Satipto Rahardjo Perspective, *Opinio Juris Journal* Vol. 16, May-September 2014, p.51.

<sup>1</sup> Josua Sitompul. Op.cit. p.233.

<sup>2</sup> SAFENET, 8 Points Notes from Netizen Criminalization with Law Concerning Elctronic Information and Transactions <http://id.safenetvoice.org/2014/11/8-poin-catatan-dari-kriminalisasi-netizen-dengan-uu-ite/> as cited in DEMOS (Center for Democracy and Human Rights Studies), *Cyberbullying: A Threat of Freedom of Expression in Social Media* [http://demosindonesia.org/2015/05/cyberbullying-ancaman-kebebasan-berekspresi-di-media-sosial/#\\_ftnref1](http://demosindonesia.org/2015/05/cyberbullying-ancaman-kebebasan-berekspresi-di-media-sosial/#_ftnref1) Accessed on February 10, 2016

<sup>3</sup> ICJR: Majority of Court Decisions for Cases of Article 27 section (3) of Law No 11 of 2008 Concerning Electronic Information and Transactions are Poor <http://icjr.or.id/icjr-mayoritas-putusan-pengadilan-untuk-kasus-pasal-27-ayat-3-uu-ite-buruk/> Accessed on February 25, 2016

<sup>4</sup> Further see Kasus Prita Mulyasari <http://id.safenetvoice.org/2009/06/kasus-prita-mulyasari/> Accessed on February 25, 2016.

<sup>5</sup> Atven Vemanda Putra, et al, the Existence of Article 27 section (3) of Law No 11 of 2008 Concerning Defamation <http://ejournal.uajy.ac.id/4921/1/AtvenVemanda%20NPM%20090510007.JURNAL.pdf> Page 3. Accessed on February 25, 2016.

- Josua Sitompul. *Cyberspace, Cybercrimes, Cyberlaw – an overview to Criminal Law Aspects (Tinjauan Aspek Hukum Pidana)*, PT. Tatanusa. Jakarta. 2012, p.6.
- McConnell International. *Cyber Crime . and Punishment? Archaic Laws Threaten Global Information*. Dec. 2000. p.2
- Media Defense Litigation Network and Institute for Criminal Justice Reform, 2000-2010: Indonesia's Freedom of Internet: Struggle Paved the Limit [Briefing Paper Nomor 3 Tahun 2011], Jakarta, 2001 cited in AP Edi Atmaja, *State Sovereignty in Cyberspace: Critics on Law Concerning Electronic Information and Transactions* in Satipto Rahardjo Perspective, *Opinio Juris Journal* Vol. 16, May-September 2014, p.51.
- Mika Isac Kriyasa. *Case of Defamation through Social Media in Indonesia: Is it Possible for a Company to Make a Report to the Police?*. News & Updates, Legal Headlines.
- National Crime Prevention Council. *Cybercrime Prevention Strategies*. Bureau of Justice Assistance U.S. Department of Justice. United States of America. September 2012.
- Ruth Broster and Ken Brien., *Cyber-bullying of Educators by Students: Evolving Legal and Policy Developments*. University of Brunswick Frederiction, p.1.
- Sharen Shariff, "Cyber-Bullying and Legal Liability in Today's Schools - See more at: <http://www.cambridgeblog.org/2010/06/cyber-bullying-and-legal-liability-in-todays-schools/#sthash.mqfsCu13.dpuf>. 2010.
- Southeast Asia Freedom of Expression Network (SAFENET) is a network of Southeast Asia bloggers and online activists who dedicated to promote freedom of expression online. Further see <http://safenetvoice.org/> . Accessed on February 10, 2016
- Suyanto Sidik. *Effect on the Law No. 11 of 2008 to Legal Change and Social Society (Dampak Undang-Undang Informasi dan Transaksi Elektronik terhadap Perubahan Hukum dan Sosial Masyarakat)*. Jurnal Ilmiah WIDYA. Universitas Bhayangkara Jakarta Raya. p. 5.
- Togi Robson Sirait. *Information Validity of Social Media as an Evidence in Defamation Based on The Law No.11 of 2008 (Keabsahan Informasi pada Media Sosial sebagai Alat Bukti dalam Pembuktian Tindak Pidana Pencemaran Nama Baik)*.