RESEARCH ARTICLE

Indonesian 'Saracen' Syndicate and the Legal Gap for Hoax Eradication in Indonesia

Andre Tri Wibowo[1]✉
[1] Indonesian Cybercrime Fighting Communities
(*Komunitas Masyarakat Perangi Cybercrime Indonesia*)
✉ andretriwibowo@gmail.com

OPEN ACCESS

Citation: Wibowo, A. T. (2021). Indonesian 'Saracen' Syndicate and the Legal Gap for Hoax Eradication in Indonesia. *Law Research Review Quarterly, 7*(2), 183-196.
https://doi.org/10.15294/lrrq.v7i1.43190

Submitted : December 13, 2020
Revised : February 2, 2021
Accepted : April 12, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract
The phenomenon of 'saracen' is one of the more serious cases in the context of cybercrime. It is not just a matter of fake news and hoax news, but 'Saracen' being an organized organization creates division, unrest, and slander in society, especially in general elections to influence society at large. This study aims to analyse the legal instruments in handling the 'Saracen Syndicate' case in Indonesia. This study finds that there are gaps in the rule of law in various cases of cybercrime, including the 'Saracen' case. On the one hand, this study confirms that there are elements of dirty political practices carried out during the general election, and on the other hand, this community develops because of the response from people who are thirsty for information (but are not careful in filtering the available information).

Keywords: *Saracen Syndicate; Cybercrime; Fake News, Hoax*

1. INTRODUCTION

Various inventions in the field of information and communication technology currently allow people to use the internet through personal computers (Personal Computers / PCs) or other electronic media anywhere. These conveniences and benefits for humans have provided many conveniences and benefits for humans in their efforts to improve the welfare of mankind. Information and communication technology is currently used by individuals, corporations, governments, and community groups for

various human activities, such as education, health, business, government, communication, entertainment, and others. However, these advances in the field of information and communication technology are also accompanied by negative impacts that threaten and endanger the social and economic development of mankind in the world, not only materially but also human lives, for example the threat of attacks on connected information and communication technology infrastructure. globally, which can endanger not only material but also human life (Suhariyanto, 2013; Mansur & Ghultom, 2005).

The crimes that arise in the field of information technology, among others, are data manipulation, espionage, sabotage, provocation, money laundering, hacking, software theft and the most widespread hoax today (Karnasudiraja, 1999).

According to the Big Indonesian Dictionary, Hoax is a fake news. In the Oxford English dictionary, Hoax is defined as 'malicious deception' or 'lies made with malicious intent', unfortunately, many social media users define Hoax as news that I do not like. Hoax or fake news is not something new, and widely circulated, and has been in circulation since Gutenberg invented the printing press in 1439. Before the internet age, 'hoaxes were even more dangerous than they are today because they are difficult to verify (Supanto, 2016; Respati, 2017; Suseno, 2012).

CNN Indonesia even mentions that in the data presented by the Ministry of Communications and Information Technology, there are as many as 800,000 sites in Indonesia which are indicated as spreading fake news and hate speech. The Ministry of Communication and Information has also blocked 773 thousand hundred based on 10 groups in 2016. The ten groups include elements of pornography, SARA, fraud/illegal trade, drugs, gambling, radicalism, violence, children, internet security, and intellectual property rights, of which pornography is the most.

With such facts, a legal instrument is needed that can regulate this, so that crimes that can harm humans can be avoided. Law is a component of the social system that is considered more effective in solving social problems in the form of crime in society. Changes in society can trigger

changes in crime which in fact follow the development of the community.

Laws or rules made by people, or an area are strongly influenced by local customs, norms, and values that live in the community itself. with other members of the community in one norm guaranteeing normative life values (Suseno, 2012).

The existence of law in society, among others, is to regulate the interests that arise in society, where these interests can conflict with each other. For that the law regulates in such a way that in a traffic interest do not conflict with each other. The law protects a person by applying a power to him to act in the context of his interests. The allocation of this power is carried out in a measurable manner in the sense that it is determined by law. Such power is called a right. However, not every power in society can be called a right but rather a right. only certain powers, namely those given by law to a person, this is what is then called legal rights (Widodo, 2010; Rahadi, 2017; Prehantoro, 2017).

The public international legal instrument that regulates cybercrime issues that currently receive the most attention is the 2001 Convention on Cyber Crime, which was initiated by the European Union. Although this convention was originally made by European regional organizations, in its development it is possible to be ratified and accessed by any country in the world that is committed to efforts to overcome cybercrime. from cybercrime, either through law or international cooperation (Prehantoro, 2017; Putra, 2014; Juliaswara, 2017).

2. METHOD

This research is a normative juridical research. Data was carried out not on people but on library materials, especially those related to information regulations and electronic transactions. The data used is secondary data. Secondary data sourced from library materials, and legal materials. Method of Data Collection by means of identification. How to identify by collecting library data in the form of archives, official documents, other library data that are closely related to research problems. Library data (secondary data) were analysed using a combination of deductive and inductive thinking patterns. The final result of data processing are qualitatively analysed, then analysed using normative

qualitative methods, interpretation methods in legal science, and interpreting data based on theories as mentioned in the literature review (Supanto, 2016).

3. RESULT AND DISCUSSION

A. The History of Cybercrime

Research on forms of cybercrime has been carried out by Stanford Research International (SRI) in the United States from 1971 to 1985. The research found 1600 cases that occurred since 1958, as well as public and government reactions to them, including settlements based on civil law. In 1979 SRI obtain more valid data, namely stating that of the 244 cases that occurred, 191 could be brought to court and the defendants from 161 cases could be convicted. The studies conducted in the 1970s were not able to clearly show the arrangements in criminal law, so they have not been included into criminal statistics Several forms of Cyber Crime in the United States attracted public attention between 1974 and 1988 (Prehantoro, 2017).

In 1974, a number of Brooklyn College New York students illegally accessed computer data to the academy's registration section, then changed the list of academic achievements of themselves and their friends online. After an investigation was carried out the act was proven to have been carried out by 12 students. In 1977, two employees of the computer programming division in a company used the company's computer illegally for 3 years. The computer was used to meet the needs of other companies founded by criminals. In 1986, three children have been detained by the US police for allegedly destroying the credit card company's TRW security system and copying other people's credit card numbers and spending USD 10,000. In 1988, a student managed to enter the internet worm virus in the internet system which caused disturbances to 6000 internet systems.

Based on the court's decision, cybercrime has occurred in Indonesia since 1983, namely in the case of the burglary of the Bank Rakyat Indonesia (BRI) branch of Brigjend Katamso Yogyakarta, in 1986 there was a burglary of Bank Negara Indonesia (BNI) by using computer facilities. In 1898 there was a bank burglary. Bali with the suspect Budiman Hidayat, in 1990 Cybercrime occurred in Bandung, namely the unauthorized copying of the Word Star program version 5.0.

In the following year, there were many cybercrimes, such as cracking, credit card fraud, bank break-ins, pornography, including abuse of dominant names, the most prevalent nowadays are hoaxes and hate speech (Herawati, 2016; Marwan & Ahyad, 2016).

B. Cybercrime: Definition and Its Limitation

At first, Cybercrime was defined as a computer crime, regarding the definition of computer crime itself until now scholars have not agreed on the meaning or definition of computer crime. Even the use of the term criminal offense for computer crime in English is still not uniform.

The law commission in England, defines "*computer fraud*" as computer manipulation in any way carried out in bad faith to obtain money, goods and other benefits or is intended to cause harm to other parties (Tianotak, 2011).

At first, legal experts focused on tools/hardware, namely computers. However, with the development of information technology in the form of internet networks, the focus of identification on the definition of cybercrime was further expanded, namely as wide as activities that can be carried out in cyber/virtual world through information systems used, so it is not just the hardware component that the crime is interpreted as cybercrime but has been expanded in the scope of the world explored by the information technology system concerned. So, it would be more appropriate if the meaning of cybercrime is Information Technology crime, as well as what Barda Nawawi Arief said as cybercrime (Anggara & Darmadha, 2016; Astuti, 2013).

Based on several sources and practices, Cybercrime has several characteristics, namely:

1. The act that is carried out is not in accordance with the law and, without rights or is unethical, occurs in the cyber space/territory, so that it is not certain which country's jurisdiction applies to it.
2. Manufacture is done using equipment that is connected to the internet.
3. The act results in material loss or not and tends to be greater than conventional crimes.
4. Perpetrators are people who understand the use of the internet and its applications.

5. These acts are often carried out transnationally/across national borders (Astuti, 2013).

C. Hoax and Fake News in Cybercrime Case

Hoax is an attempt to deceive or trick the reader/listener into believing something, even though the creator of the fake news knows that the news is fake. One of the most common examples of fake news is claiming an item or event with a different name from the actual item/event. The definition states Hoax is a hoax that is used to believe something that is wrong and often unreasonable which through online media Hoax aims to create public opinion, lead public opinion, shape perceptions also just for fun. The purposes of spreading Hoaxes vary widely but in general, these lies are distributed as jokes or just to play, bring down competitors, deceptive promotions, or invitations to do good deeds that have no clear argument in them. People are more likely to believe in hoaxes if the information matches their opinion or attitude (Nte, Esq, Enokie, & Bienose, 2020). Types of Hoax Information, such as:

1. Fake news; Fake news: News that tries to replace the original news, this news aims to falsify or include untruths in a news. Fake news writers usually add things that are not true and conspiracy theories, the more bizarre, the better. Fake news is not a humorous comment against some news.
2. Clickbait: Trap links: Links placed strategically on a site with the aim of attracting people to other sites. The content in these links is factual but the title is exaggerated or has interesting images attached to lure readers.
3. Confirmation bias; Confirmation bias; Tendency to interpret recent events as well as evidence as pre-existing beliefs.
4. Misinformation; False or inaccurate information, especially those intended to deceive.
5. Satire: An article that uses humor, irony, exaggeration to comment on current events. Satirical news can be found on television shows such as "Saturday Night Live" and "This Hour has 22 Minutes".
6. Post Truth: Post truth: Events where emotions play a role more than facts to shape public opinion.

7. Propaganda: Activities: spreading information, facts, arguments, half-truth gossip, or even lies to influence public opinion.

Further question, *how hoaxes work?* According to a psychologist's point of view, there are two things that make a person believe easily against fake news, people tend to believe lies if their information is what they believe various conspiracy theories about satellite photos, then that person will believe because it is a flat earth follower, so tend not to care whether the information he receives is correct or just inventive information (Smith, 2020). This is then exacerbated if the hoax advocate has poor knowledge of using the internet and cannot learn what he can.

D. Saracen Syndicate in Indonesia

Saracen is a special syndicate that has recently shocked the public, this is because Saracen is one of the syndicates that run a hate speech 'business' by accepting orders from various parties, the order value starts from Rp. 75 million to Rp. 100 million. These called themselves Saracens, the name for the adherents of Islam in the Middle Ages.

Recorded in the Encyclopedia Britannica, Saracen is a term for Muslims, both Arabs and Turks who live on the Sinai peninsula, the term Saracen was then used to refer to all Arabs in the following centuries. And, after the formation of the caliphate, the Byzantines called all Muslims caliphs as the Saracens. Through the Byzantines and the crusaders, the name spread to western Europe and persisted into modern times.

The discovery of the Saracen network is considered a serious cyber threat. The reason is the Saracen group is suspected of not only attacking one religion but attacking various parties including the government with fighting techniques.

E. Law Enforcement in Cybercrime Case

The development of cybercrimes that have occurred today has received reactions from countries in the world both nationally, regionally, and internationally, with various policies using criminal law means. The state's reaction to the development of cybercrimes is a consequence

of the sovereignty of a country (Muhtada & Arifin, 2018; Diniyanto, 2016).

In Indonesia, regulations regarding cybercrime, especially in cases of hoaxes and hate speech, are regulated in such a way with various rules (Suseno, 2012; Muhtada, 2016), for example with the Criminal Code, then Law No. 11 of 2008 concerning Information and Electronic Transactions, along with the Law No. Law No.40 2008 concerning the Elimination of Race and Ethnic Discrimination.

In Law No. 11 of 2008 concerning Information and Electronic Transactions, namely article 27 paragraph (3), it is regulated about the prohibition of someone from spreading electronic information without knowledge and containing forms of insults and defamation, while the article reads: Everyone intentionally and without the right to distribute and/or transmit and or make accessible electronic information and/or electronic documents that contain insults and/or defamation (Adji, 2020; Sinaga, 2020).

The National Police has also disseminated Circular Letter Number SE/06/X/2015 to all members of the National Police regarding the Handling of Hate Speech with the aim that Polri members understand and know the forms of hate speech in various media and how to handle it. This circular letter of the Chief of Police refers to several laws, including; the Criminal Code (KUHP), Law No. 39 of 1999 concerning Human Rights, Law No. 2 of 2002 concerning the National Police, Law No. 12 of 2008 concerning the Ratification of the International Convention on Civil and Political Rights, Law no. 11 of 2008 concerning Information and Electronic Transactions, Law no. 40 of 2008 concerning the Elimination of Racial and Ethnic Discrimination, as well as Law no. 7 of 2012 concerning Handling Social Conflict. Number 2 letter (f) Circular Letter of the Chief of Police Number SE/06/X/2015 states that: Hate speech can be in the form of criminal acts as regulated in the Criminal Code (KUHP) and other criminal provisions outside the Criminal Code, which include:

1. Humiliation;
2. Defamation;
3. Blasphemy;
4. Unpleasant conduct;
5. Provoking;
6. Incite; and

7. Spreading fake news and all of the above actions have a purpose or may result in acts of discrimination, violence, loss of life, and/or social conflict.

Furthermore, in letter (g) Circular Letter Number SE/06/X/2015 it is stated: Hate speech as referred to above, aims to incite and incite hatred against individuals and/or groups of people, in different communities distinguished from:

1. Tribe;
2. Religion;
3. Religious sects;
4. Belief or belief;
5. Race;
6. Between classes;
7. Skin colour;
8. Ethnicity;
9. Gender;
10. Disabled people; and
11. Sexual orientation.

In letter (h) Circular Letter Number SE / 06 / X / 2015 it is stated that: Hate speech as mentioned above can be done through various media, including:

1. In the oration of campaign activities;
2. Banners or banners;
3. Social media networks;
4. Public opinion submission (demonstration);
5. Religious lectures;
6. Print or electronic media;
7. Pamphlets in the territory of Indonesia.

As for now, articles that are quite effective in preventing the emergence of Hoax and hate speech crimes are articles 27, 28, and 29 of the ITE Law, although many also regret the existence of this article due to its rubbery nature, until 2015 this article 134 victims have been ensnared. Of the 134 cases, only 20 have been processed and the remaining status is still unclear. This victim has increased significantly since 2013 with the number of victims as many as 20 people with the largest percentage being a violation of Article 27 paragraph 3 of the ITE Law (Herawati, 2016).

Because the spread of hoaxes is increasingly massive and out of control, an effort is needed to dispel the hoax news, as for steps that can be taken to assist in identifying which news is hoax and which news is genuine.

1. Be careful with provocative titles.

   Hoax news often uses provocative sensational titles, for example by directly pointing the finger at a certain party, the contents can also be taken from official media news, but they are changed to create the perception that the hoax maker wants.

   Therefore, if you encounter news with provocative titles, you should look for references in the form of similar news from official online sites, then compare the contents, whether they are the same or different. Thus, at least we as readers can get a more balanced conclusion.
2. Pay attention to the site address.

   For information obtained from the website or include a link, pay attention to the URL address of the site in question. If it comes from a site that has not been verified as an official press institution, for example using a blog domain, then the information can be considered dubious. in Indonesia which claims to be a news portal.

   Of these, less than 300 have been verified as official news sites. This means that there are at least tens of thousands of sites that have the potential to spread fake news on the internet that must be watched out for.
3. Check the Fact.

   Pay attention to where the news comes from and who the source is, whether from official institutions such as the KPK or the National Police. Pay attention to the balance of news sources, if there is only one source, the reader does not get the complete picture.

   Another thing that needs to be observed is the difference between news made based on facts and opinions. Facts are events that occur with testimony and evidence, while opinions are the opinions and impressions of news writers so that they have a tendency to be subjective.
4. Photo authenticity.

   In the current era of digital technology, not only content in the form of photos or videos, there are times when fake news makers also edit photos to provoke readers.

5. Join an anti-hoax discussion group

   On Facebook, there are a number of anti-hoax fanpages and discussion groups, such as the Anti-Slander, Incitement, and Hoax Forum, the Indonesian Hoaxes Fanspage, and the Lifeboat Group. In such groups, netizens can participate in the selection, which news is classified as Hoax or not.

4. CONCLUSION

The development of information technology changes all patterns of communication and social order so that it becomes a new forum for people to express their opinions and expressions. On the one hand, this development is very useful because it can facilitate people in communicating, but on the other hand this development can also trigger the emergence of new problems, namely Hoax and hate speech. The community is very easy to spread information that is not yet clear and convey hate speech. With a good media literacy campaign and law enforcement through the law on information and electronic transactions, it is hoped that the spread of hoaxes and hate speech crimes can be reduced, and the use of information technology can be wiser.

5. DECLARATION OF CONFLICTING INTERESTS

The Author declares that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

6. ACKNOWLEDGEMENT

Special thanks for Indonesian Cybercrime Fighting Communities for their invaluable support.

7. REFERENCES

Adji, R. A. (2020). Upaya Penanganan Tindak Pidana Penipuan Online oleh Satreskrim Polres Ciamis. *Advances in Police Science Research Journal*, *4*(10). Retrieved from http://journal.akademikepolisian.com/index.php/apsrj/article/view/396

Anggara, B., & Darmadha, I. N. (2016). Penegakan Hukum Kejahatan Dunia Maya (Cybercrime) Yang Dilakukan Anak Di Bawah Umur. *Kertha Wicara: Journal Ilmu Hukum*, *5*(5). https://ojs.unud.ac.id/index.php/kerthawicara/article/view/21996

Astuti, D. P. (2013). Implementasi Penyidikan Tindak Pidana Cyber Crime Berkaitan Dengan Penjualan Barang Yang Tidak Sesuai Dengan Perjanjian Dalam Rangka Perlindungan Konsumen (Studi Di Polda Jawa Timur). *Kumpulan Jurnal Mahasiswa Fakultas Hukum*, *1*(2), 1-16. http://hukum.studentjournal.ub.ac.id/index.php/hukum/article/view/240/232.

Diniyanto, A. (2016). Indonesian's Pillars Democracy: How This Country Survives. *JILS (Journal of Indonesian Legal Studies)*, *1*(1), 105-114.

Herawati, D. M. (2016). Penyebaran Hoax dan Hate Speech sebagai Representasi Kebebasan Berpendapat. *Jurnal Promedia*, *2*(2), 128-155. https://doi.org/10.52447/promedia.v2i2.793

Juliaswara, V. (2017). Mengembangkan Model Literasi Media yang Berkebhinekaan dalam Menganalisis Informasi Berita Palsu (Hoax) di Media Sosial. *Jurnal Pemikiran Sosiologi*, *4*(2), 142-164. https://doi.org/10.22146/jps.v4i2.28586

Karnasudiraja, E. J. (1999). *Bahaya Kejahatan Komputer*. Jakarta: Sinar Grafika.

Mansur, D. M. A., & Ghultom, E. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.

Marwan, M. R., & Ahyad, A. (2016). Analisis penyebaran berita hoax di Indonesia. *Jurusan Ilmu Komunikasi, Fakultas Ilmu Komunikasi Universitas Gunadarma*, *5*(1), 1-16.

Menkumham. (2011). UU RI Tentang Pornografi dan Informasi dan Data Transaksi Elektroni. Yogyakarta: Pustaka Mahardika.

Muhtada, D. (2016). Finding Some Alternatives in Indonesian Legal Development. *JILS (Journal of Indonesian Legal Studies)*, *1*(1), 1-2.

Muhtada, D., & Arifin, R. (2018). Introducing JILS 3 (2), November 2018 Edition: Crimes and Society and its Contemporary Issues. *JILS (Journal of Indonesian Legal*

Studies), *3*(2), 147-148.

Nte, N. D., Esq, U. K., Enokie, B. K., & Bienose, O. (2020). Cyber Crime Management among Students: An Evaluation of Legal Correlates of Cyber Crime Management among Tertiary Institutions Students in Nigeria (a Case Study of Delta State). *JILS (Journal of Indonesian Legal Studies)*, *5*(2), 295-334.

Prehantoro, P. (2017). Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional. *Justice Pro: Jurnal Ilmu Hukum*, *1*(2). http://www.ojs.uniyos.ac.id/index.php/jp/issue/view/20

Putra, A. K. (2014). Harmonisasi Konvensi Cyber Crime dalam Hukum Nasional. *Jurnal Ilmu Hukum Jambi*, *5*(2), 95-109.

Rahadi, D. R. (2017). Perilaku Pengguna dan Informasi Hoax di Media Sosial. *Jurnal Manajemen dan Kewirausahaan*, *5*(1), 58-70.

Republic of Indonesia. (2008). *Undang-Undang No 40 Tahun 2008 tentang Penghapusan Diskriminasi Ras dan Etnis*.

Republic of Indonesia. (2008). *Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE).*

Republic of Indonesia. *Kitab Undang-Undang Hukum Pidana (KUHP).*

Respati, S. (2017). Mengapa banyak orang mudah percaya berita "hoax". *Kompas. com. Retrieved from* https://nasional.kompas.com/read/2017/01/23/18181951/mengapa.banyak.orang.mudah.percaya.berita.hoax.?page=all

Sinaga, G. Y. (2020). Penyelidikan Tindak Pidana Cyber Crime Oleh Sat Reskrim Untuk Meningkatkan Crime Clearance Di Polres Cimahi. *Indonesian Journal of Police Studies*, *4*(7). Retrieved from http://journal.akademikepolisian.com/index.php/ijps/article/view/233.

Smith, R. B. (2020). Cybercrime in ASEAN: Anti-Child Pornography Legislation. *JILS (Journal of Indonesian Legal Studies)*, *5*(2), 277-294.

Suhariyanto, B. (2013). *Tindak Pidana Teknologi Informasi (Cybercrime) Urgensi*. Jakarta: PT RajaGrafindo Persada.

Supanto, S. (2016). Perkembangan Kejahatan Teknologi

Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy. *Yustisia Jurnal Hukum*, *5*(1), 92-117. https://doi.org/10.20961/yustisia.v5i1.8718

Surat Edaran Kapolri No:SE/06/X/2015.

Suseno, S. (2012). *Yurisdiksi Tindak Pidana Siber*. Bandung: PT Refika Aditama.

Tianotak, N. (2011). Urgensi Cyberlaw di Indonesia dalam Rangka Penangan Cybercrime di Sektor Perbankan. *Jurnal Sasi*, *17*(4), 20-27.

Widodo, W. (2010). *Sistem Pemidanaan dalam Cyber Crime*. Yogyakarta: CV. Aswaja Pressindo.

Quote

Social media can be a useful and fun way to interact with others and to share content, but use it carefully. Remember that there is nothing totally private on the internet and once online it is hard to control.

***Amanda-Jane Turner**, Cybersecurity for everyone - demystifying cybercrime*

ABOUT AUTHORS

Andre Tri Wibowo is graduated from Faculty of Law Universitas Negeri Semarang, Indonesia. Now, he is serving as researcher and volunteer at Indonesian Cybercrime Fighting Communities (Komunitas Masyarakat Perangi Cybercrime Indonesia).