RESEARCH ARTICLE

Typosquatting Crime in the Electronic Transactions

Alif Kharismadohan
Postgraduate Program, Faculty of Law, Universitas Negeri Semarang, Indonesia
✉ alifkharismadohan@gmail.com

OPEN ACCESS

Citation: Kharismadohan, A. (2021). Typosquatting Crime in the Electronic Transactions. *Law Research Review Quarterly, 7*(1), 111-124. https://doi.org/10.15294/lrrq.v7i1.43188.

Submitted : October 25, 2020
Revised : December 19, 2020
Accepted : January 19, 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

Today's technological developments have brought many changes to human life. This change will certainly bring benefits to life, including making all transactions easier and faster. However, there are still some parties who take advantage of technology to act crimes. Among them is typosquatting, which is impersonating a domain name that is almost similar to the original domain name and has the same contents as the original domain. This will be detrimental to transaction service users. This research aims to analyze and study typosquatting in electronic transactions in Indonesia and its law enforcement. This study found that these crimes often committed on the internet were used to trick internet users by creating a fake website using names that were very similar to well-known websites. Furthermore, this research underlines that typosquatting legal arrangements in Indonesia can be seen in the Trademark Law, the Criminal Code, as well as the Information and Electronic Transaction Law.

Keywords: *Typosquatting; Cybercrime; Law Enforcement*

1. INTRODUCTION

In this 21st century, which is better known as the information century, the role of information technology is increasingly important. The importance of this role is further spurred by the need for the fast-paced activities of the modern world and the demands of an all-globalizing era. As a result, the activities of the modern world really require efficient communication technology and can reach large areas without being hindered by national borders (Wijaya & Arifin, 2020). One technology that has successfully

answered these needs is the internet (Rosidawati & Santoso, 2013).

Internet as a form of advancement in information technology, has changed the lifestyle of humans. Internet is almost used in every area of life. For example, education, banking, business and so on.

In today's era, almost all transactions can be done electronically. This of course is a form of progress because business transactions can be done anytime and anywhere as long as there is an internet network. Marketing that used to be done conventionally is now mostly done with the help of technology (Maherni, 2015; Muthia & Arifin, 2019; Mooere & Edelman, 2010). However, of course there are negative impacts with the existence of these electronic transactions such as fraud, spread of personal data and typosquatting. Typosquatting is site plagiarism that can mislead internet users (Widodo, 2013; Spaulding, Upadhyaya, & Mohaisen, 2016). Typosquatting can be detrimental to internet users who might make a typo in typing the domain.

In Indonesia, crime through the internet is regulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008. However, in reality cyber crime in Indonesia still occurs in the community, especially in typosquatting cases. In the case of typosquatting, that is, if an internet user types the wrong domain name, but the pages and contents of the domain are the same. So, it can create confusion for internet users about the original website. Because, this fake domain can cause various losses if we have entered our personal data (Dharmaadi, Bakhrun, Saputra, & Putra, 2014).

2. METHOD

For this research, the author uses several sources and types of data, namely: *Source and type of data*: the source of data that the authors use is secondary data, namely data arranged in the form of documents (Suryabrata, 1987). Secondary data needed in this paper is data regarding various definitions of cybercrime, typosquating and applicable laws to solve typosquating problems. While the types of data obtained are quantitative and qualitative. *Data collection*: in the method of writing this paper, the authors collect data using the literature study method. Literature study was conducted to obtain data using literature related to writing this paper,

namely about typosquatting. *Data analysis*: the data that has been collected is then selected again and examined again. After that researched using descriptive and argumentative analysis techniques. *Conclusion***:** draw research conclusions always have to base themselves on all data obtained in research activities (Arikunto, 2015).

3. RESULT AND DISCUSSION

A. Definition Cybercrime: Limitation based on Law

When we discuss cybercrime, it will not be separated from the network security problem. Cybercrime comes from the word cyber which means cyberspace or the internet and crime which means crime (Rahardjo, 2002; Zulkefli, Singh, Shariff, & Samsudin, 2017). So, cybercrime is a crime in cyberspace. Cybercrime is all kinds of use of computer networks for criminal purposes and/or technology criminals by misusing the convenience of digital technology (Wahid & Labib, 2005; Rosidawati & Santoso, 2017). Cybercrime, is not a crime that should be underestimated. Even though they do not meet in person, cyber crime can have fatal consequences. *Cybercrime* has a distinctive character compared to conventional crime (Setiawan, 2005; Tamara, 2016):

1) Acts that are carried out illegally, without rights or unethical occur in cyberspace / areas, so it cannot be ascertained which country's legal jurisdiction will apply to it.
2) This action is carried out using any equipment that can be connected to the internet.
3) These acts result in material and immaterial losses (time, value, services, money, goods, self-respect, dignity, and confidentiality of information) which tend to be greater than conventional crimes.
4) The perpetrator is a person who masters the use of the internet and its applications. These acts are often carried out transnationally / across countries.

In Indonesia, cyber crime has been regulated in Law Number 11 of 2008 concerning electronic information and transactions in Article 35 which stated that: "*Every person intentionally and without right or against the law manipulates, creates, changes, removes, destroys electronic information and / or electronic documents with the aim that the electronic information and / or electronic documents are considered as authentic data.*"

Apart from the Law on Information and Electronic Transactions, the basic regulations in the handling of cyber crime cases in Indonesia are the implementing regulations for the ITE Law and also the technical regulations for investigations in each investigating agency (Ansyahrul, 2003; Sirait & Simangungsong, 2020).

B. Forms of Cybercrime

There are some types and forms of cybercrime occurred in Indonesia, as follows:

1) Based on the type of activity
   a. *Unauthotized Access to Computer System and Service*
      Crimes committed by infiltrating a computer network system illegally, without permission or without the knowledge of the owner of the computer network that he entered (Sofwan & Naufal, 2012).
   b. *Illegal Contents*
      It is a crime to enter data or information on the internet about something that is untrue, unethical, and can be considered to violate the law or disturb public order. For example, the posting of fake news or slander that will destroy the dignity and self-respect of other parties and so on (Hius & Nasution, 2012).
   c. *Data Forgery*
      The crime was falsifying data on important documents stored as scripless documents via the internet. This crime is usually shown in e-commerce documents by making as if a 'typo' occurred which will ultimately benefit the perpetrator because the victim will enter personal data and credit card numbers which can be misused. For example the case *www.klikbca.com* by hacker Steven Haryanto (Arifah, 2011).
   d. *Carding*
      Carding is counterfeiting and illegally using credit cards belonging to other parties to shop online for the benefit of the perpetrator (Widodo, 2003).
   e. *Cybersquatting* and *typosquatting*
      Cybersquatting is registering the domain name of a certain person or company and trying to sell it to that company at a higher price. Meanwhile, typosquatting is a crime by creating a pun domain, which is a

domain that is similar to someone else's domain name.

f. *Cyber Espionage*
It is a crime that utilizes the internet network to carry out spying against other parties, by entering the target party's computer network system. These crimes are usually directed against business rivals whose important documents or data are stored in a computerized system (Tahir, Raza, Ahmad, Kazi, Zaffar, Kanich, & Caesar, 2018).

g. *Cyber Sabotage* and *Extortion*
This crime is committed by disturbing, destroying or destroying data, computer programs or computer network systems connected to the internet. Usually this crime is carried out by inserting a logic bomb, computer virus or a certain program, so that data, computer programs, or computer network systems do not run as they should and run as the perpetrators want. In some cases that have occurred, the perpetrator of the crime will offer to repair the computer program data or computer network system that has been sabotaged, of course for a certain fee. This crime is often referred to as cyberterrorism (Saputra & Nasution, 2014).

2) Based on the Motive of Activity
   a. Cybercrime as a *pure crime*
   Crimes that are purely criminal acts are crimes committed because of the motive of crime. This type of crime usually uses the internet only as a means of crime (Ketaren, 2016).
   b. Cybrcrime as a "*gray*" crime
   With the type of crime on the internet that falls into the "*gray*" area, it is quite difficult to determine whether it is a crime or not. Given that the motive for his activities is sometimes not for crime (Ketaren, 2016).

3) Based on Activity Objectives
   a. Cybercrime that *attacks individuals*
   Crimes committed against other people with the motive of vengeance or fun which aims to destroy one's good name, to try or play with someone to get personal satisfaction (Ketaren, 2016).

b. Cybercrime that *attacks copyright*
Crimes committed against someone's work with the motive of creating, marketing, modifying the purpose of personal / public interest or for material / non-material purposes.

c. Cybercrime that *attacks the government*
Crimes committed with the government as an object with a terror motive, are hijacking or destroying the security of a government which aims to disrupt the government system, or destroy a country.

C. Domain Name in Cybercrime Cases

Definition of Domain Name is the internet address of a person, association, organization or business entity which is one of the important factors that must be taken in using the internet for commercial purposes or not. The address serves as a medium of liaison between a person or legal entity that posts information on an internet website and users of internet services (Rosidwati & Santoso, 2013; Marheni, 2013; Irfan, Ramdhani, Darmalaksana, Wahana, & Utomo, 2018).

Registration system domain name, is done by applying the principle of first come first served, meaning, whoever registers first, he is entitled to the domain name. Another system that is implemented is that domain name registration is carried out without going through a first examination process, so that to find out whether a domain name has been registered by another party or not, registrants must first contact the domain name registrar's organization (Moeljatno, 2005; Iman, Susanto, & Inggo, 2019).

In relation to cybercrime protection, several problems arise relating to brands and *Domain name* on the internet network (Rosidwati & Santoso, 2013; Ersya, 2017), namely:

1) A dispute arises if a third party deliberately registers a domain name that he thinks other people will be interested in. This method is widely used by someone who has no relationship at all with a brand that is registered as a domain name.
2) A dispute arises if a third party registers a list name that is the same or similar to someone else's trademark with the intention of being used by the registrant himself.
3) Domain name registrars are carried out by third parties based on the brands they own and without realizing it

have the same brands as other companies, but in different class categories of goods and services.

D. Understanding Typosquatting

Typosquatting is a trick on the internet that is used to trick internet users by creating a fake website using names very similar to the famous website. This method is almost the same as phishing, it's just that this method relies on a typo or typo on the website domain name that will be visited via an Internet browser (Sukayasa & Suryantho, 2018; Chintia, Nadiah, Ramdhani, Haedar, Febriansyah, & Kom, 2019). This sneaky trick is very widespread, website Indonesia is the most widely used for typosquatting tricks including bank sites. Because indeed many users in Indonesia often visit website banks to make transactions, for example on such as website click bca. What this bank's web domain address should be *www.klikbca.com* and there are parties who are not responsible for creating a fake website address of the BCA bank with the address *www.kilkbca.com*. So if a user makes a transaction via website such as *kilkbca.com*, he will enter the fake BCA website bank.

The fake website made by irresponsible parties is also very much like the real thing and has been targeted to trap typosquatting victims. And if an internet user will transact and get into the fake website and log in on the website, then the user's login identity will be easily stolen.

Typosquatting is basically an act of buying and operating domain names that are the result of variations of a well-known domain name, in the hope that the site is visited by internet users due to spelling or typing errors from the original site that the user wants to visit (Bunga, 2019; Jhon, 2018).

In 2001, the world of banking through the internet (e-banking) in Indonesia was shocked by the act of a man named Steven Haryanto, a hacker and journalist for the master web magazine. This man from Bandung deliberately created a genuine site but a fake internet banking service for Bank Central Asia (BCA). This idea arose when Steven also mistyped the website address. Steven buys domains with similar names *http://wwww.klikbca.com* (BCA internet banking original site), namely *http://www.klik-bca.com*, *http://www.kilkbca.com*, *http://www.clikbca.com*, *http://www.klickca.com*, *http://www.klikbac.com*. If we log in to

the five sites, users will get the same internet site as the klikbca.com site, except there is no transaction security and fake login from. When logging in, you will not enter the BCA internet banking facility and will display the message "*the page cannot displayed*". Fatal, by logging on to these sites, your internet username and pin will be sent to the site owner (Raodia, 2019; Widodo, 2013; Sjahdeini, 2018).

E. Laws Regarding Typosquatting

In connection with cases of disputes over domain names that have begun to spread in Indonesia, based on the description above, it is clear that the statutory instruments that can be used in this matter are Law Number 14 of 1997 concerning marks for typosquating cases.

1) Article 72
   a. Anyone who deliberately and without right commits the act as referred to in Article 2 paragraph 1 or Article 49 paragraph 1 and paragraph 2 shall be punished with a minimum of 1 month and / or a fine of at least IDR 1,000,000.00 (one million rupiah) or criminal a maximum imprisonment of 7 years and or a maximum fine of Rp.5,000,000.00 (five million rupiah).
   b. Anyone who broadcasts, exhibits, circulates, sells to the public a work or goods resulting from a copyright infringement or related things as referred to in paragraph 1 shall be punished with imprisonment for a maximum of 5 years and / or a maximum fine of Rp. 500,000,000.00 (five hundred million rupiah.)
   c. Anyone who deliberately and without rights reproduces the commercial use of a computer program, shall be punished with a maximum imprisonment of 5 years and / or a maximum fine of Rp. 500,000,000.00 (five hundred million rupiah).
2) Article 82
   Any person who deliberately and without rights uses the same mark substantially as the registered mark of another person or other legal entity, for goods and / or the like that is produced and / or traded, shall be punished with a maximum imprisonment of 5 years and a maximum fine of Rp. 000.00 (fifty million rupiah).

3) Article 378 of the Criminal Code concerning Fraud
   Anyone who with the intention of illegally benefiting himself or another person by using a false name or fake dignity with trickery or a series of lies moves another person to surrender something to him or to give a debt or to write off a debt, is threatened with fraud by imprisonment for the longest 4 years (Moeljatno, 2005).
4) Article 362 of the Criminal Code concerning Theft
   Anyone who takes property wholly or partly belonging to another with the intention of illegally possessing it, shall be punished for theft by a maximum imprisonment of 5 years or a maximum fine of sixty rupiahs (Moeljatno, 2005).

Meanwhile, the provisions state that someone who is without rights or not related to the owner of the mark or owner of a well-known name protected by trademark law can be sued by the trademark owner if:

1) Register, trade or use as a domain name
2) At the time of registering the domain name uses the same or identical or similar marks to the mark
3) When registering to use a well-known mark that is the same or similar to a well-known mark so it can be confusing.

4. CONCLUSION

It is clear, that cybercrime cases according to law recognized as all kinds of criminal activity through the internet network. In Indonesia the law regarding cybercrime has been regulated in Law number 11 of 2008 concerning electronic information and technology, which emphasized that everyone deliberately and without rights or against the law manipulates, creates, changes, removes, destruction of electronic information and/ or electronic documents with the aim that electronic information and electronic documents are considered as if the data is authentic. Cybercrime is not a crime that should be underestimated. Even though they do not directly visit the perpetrators, cybercrime can have fatal consequences for the victims. This research concluded and emphasized that typosquatting is a type of cybercrime crime where the perpetrator makes a play on a domain name that he wants to impersonate. After that the perpetrator will copy the entire contents of the

domain to be copied. So that if a user makes a typo they don't realize that he is accessing a mock web. Typosquatting generally attacks the banking domain or other payment transactions. Thus the perpetrator can obtain a username and password from the bank user. This of course will be detrimental to bank users and the bank itself because it will get a bad image. Therefore, there needs to be protection regarding typosquatting cases so that this crime does not spread widely. Furthermore, legally, typosquatting is considered a criminal act, but until now there is no law that explicitly and specifically regulates typosquatting. However, only in Law No. 14 of 1997 on trademarks for typosquatting. In this case, Indonesia in particular has not been given too much attention. So this crime can arise because of legal incapacity and including the authorities who reach him because this crime is virtual in which the perpetrator is not physically visible. Therefore it is necessary to have a special rule of law that regulates firmly and has permanent strength.

5. DECLARATION OF CONFLICTING INTERESTS

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

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Ansyahrul, A. F. (2003). *Domain Name dalam Hukum Indonesia* (Doctoral Dissertation, Universitas Airlangga).

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi*, *18*(2), 185-195.

Arikunto, S. (2013). *Prosedur Penelitian Suatu Pendekatan Praktik*. Jakarta: Rineka Cipta.

Bunga, D. (2019). Legal Response to Cybercrime in Global and National Dimensions. *Padjadjaran Journal of Law*, *6*(1), 69-89. https://doi.org/10.22304/pjih.v6n1.a4.

Chintia, E., Nadiah, R., Ramadhani, H. N., Haedar, Z. F., Febriansyah, A., & Kom, N. A. R. S. (2019). Kasus Kejahatan Siber yang Paling Banyak Terjadi di

Indonesia dan Penanganannya. *JIEET (Journal of Information Engineering and Educational Technology)*, *2*(2), 65-69. http://dx.doi.org/10.26740/jieet.v2n2.p65-69.

Dharmaadi, I. P. A., Bakhrun, A., Saputra, D., & Putra, A. M. A. (2014, November). Typo-squatting crime in Indonesia online banking. In *2014 International Conference on Information Technology Systems and Innovation (ICITSI)* (pp. 269-272). IEEE.

Ersya, M. P. (2017). Permasalahan Hukum dalam Menanggulangi Cyber Crime di Indonesia. *Journal of Moral and Civic Education*, *1*(1), 50-62.

Hius, J. J., Saputra, J., & Nasution, A. (2014). Mengenal Dan Mengantisipasi Kegiatan Cybercrime Pada Aktifitas Online Sehari-Hari Dalam Pendidikan, Pemerintahan dan Industri Dan Aspek Hukum Yang Berlaku. *Prosiding SNIKOM*.

Iman, N., Susanto, A., & Inggi, R. (2019). Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review). *InComTech: Jurnal Telekomunikasi dan Komputer*, *9*(3), 186-192. http://dx.doi.org/10.22441/incomtech.v9i3.7210.

Irfan, M., Ramdhani, M. A., Darmalaksana, W., Wahana, A., & Utomo, R. G. (2018, November). Analyzes of cybercrime expansion in Indonesia and preventive actions. In *IOP Conference Series: Materials Science and Engineering* (Vol. 434, No. 1, p. 012257). IOP Publishing.

Jhon, R. M. (2018). Existence of Criminal Law on Dealing Cyber Crime in Indonesia. *IJCLS (Indonesian Journal of Criminal Law Studies)*, *3*(1), 25-34. https://doi.org/10.15294/ijcls.v3i1.16945.

Ketaren, E. (2016). Cybercrime, Cyber Space, dan Cyber Law. *Jurnal Times*, *5*(2), 35-42. https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/556.

Marheni, N. P. D. (2013). Perlindungan Hukum Terhadap Konsumen Berkaitan Dengan Pencantuman Desclaimer Oleh Pelaku Usaha Dalam Situs Internet (Website). *Thesis,* Universitas Udayana, Bali.

Moeljatno, M. (2005). *Kitab Undang-undang Hukum Pidana*. Jakarta: PT Bumi Aksara.

Moore, T., & Edelman, B. (2010, January). Measuring the perpetrators and funders of typosquatting. In *International Conference on Financial Cryptography and*

Data Security (pp. 175-191). Springer, Berlin, Heidelberg.

Muthia, F. R., & Arifin, R. (2019). Kajian Hukum Pidana Pada Kasus Kejahatan Mayantara (Cybercrime) Dalam Perkara Pencemaran Nama Baik Di Indonesia. *RESAM Jurnal Hukum*, *5*(1), 21-39. https://doi.org/10.32661/resam.v5i1.18.

Rahardjo, A. (2002). *Cybercrime Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: PT.Citra Aditya Bakti.

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie: Jurusan Ilmu Hukum Fakultas Syariah dan Hukum*, *6*(2), 230-239. https://doi.org/10.24252/jurisprudentie.v6i2.11399.

Rosidawati, I., & Santoso, E. (2017). Pelanggaran Internet Marketing Pada Kegiatan E-Commerce Dikaitkan dengan Etika Bisnis. *Jurnal Hukum & Pembangunan*, *43*(1), 27-53. http://dx.doi.org/10.21143/jhp.vol43.no1.1507.

Setiawan, D. (2005). *Sistem Keamanan Komputer*. Jakarta: PT. Elex Media Komputindo.

Sirait, T. N., & Simangungsong, J. B. (2020). Analisis Yuridis Pelaksanaan Tugas Pokok Pengelola Domain Internet Indonesia. *Nommensen Journal of Legal Opinion*, *1*(01), 52-62. https://ejournal.uhn.ac.id/index.php/opinion/article/view/38.

Sjahdeini, S. R. (2018). e-commerce Tinjauan dari Perspektif Hukum. *Jurnal Hukum Bisnis*, *6*(6), 6-15.

Sofwan, H., & Naufal, M. (2012). *Penegakan Hukum Cyber Crime Ditinjau Dari Hukum Positif dan Hukum Islam.* Yogyakarta: Universitas Islam Indonesia.

Spaulding, J., Upadhyaya, S., & Mohaisen, A. (2016, August). The landscape of domain name typosquatting: Techniques and countermeasures. In *2016 11th International Conference on Availability, Reliability and Security (ARES)* (pp. 284-289). IEEE.

Sukayasa, I. N., & Suryathi, W. (2018). Law Implementation of Cybercrime in Indonesia. *Soshum: Jurnal Sosial dan Humaniora*, *8*(2), 123-130.

Suryabrata, S. (1987). *Metode Penelitian*. Jakarta: Rajawali Press.

Tahir, R., Raza, A., Ahmad, F., Kazi, J., Zaffar, F., Kanich, C.,

& Caesar, M. (2018, April). It's all in the name: Why some URLs are more vulnerable to typosquatting. In *IEEE INFOCOM 2018-IEEE Conference on Computer Communications* (pp. 2618-2626). IEEE.

Tamara, A. D. (2016). *Analisis Kasus-Kasus Kejahatan Perbankan Melalui Internet Banking di Indonesia* (Doctoral dissertation, University of Muhammadiyah Malang).

Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime).* Jakarta: PT.Refika Aditama.

Widodo, W. (2013). *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: Asswaja Presindo.

Wijaya, M. R., & Arifin, R. (2020). Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?. *IJCLS (Indonesian Journal of Criminal Law Studies)*, *5*(1), 63-74. https://doi.org/10.15294/ijcls.v5i1.23273.

Zulkefli, Z., Singh, M. M., Shariff, A. R. M., & Samsudin, A. (2017). Typosquat cyber crime attack detection via smartphone. *Procedia Computer Science*, *124*, 664-671. https://doi.org/10.1016/j.procs.2017.12.203.

Ransomware is unique among cybercrime because in order for the attack to be successful, it requires the victim to become a willing accomplice after the fact.

James Scott
Sr. Fellow, Institute for Critical Infrastructure Technology

ABOUT AUTHORS

Alif Kharimadohan is a Postgraduate Student at Faculty of Law Universitas Negeri Semarang. His area of research interests are concerning Criminal Law, Cybercrime Law, Cyberlaw, as well as Law and Technology.