International Journal of Humanities, Social Sciences and Business (INJOSS) e-ISSN: 2962-6781
Vol. 4 No. 2 May 2025, page 108-122

THE CRIMINAL PROVISIONS OF DATA PRIVACY LAW AND ANATOMY OF CYBERCRIME LAW IN INDONESIA

Awaludin Marwan *
Bhayangkara Jakarta Raya University
awaludin.marwan@dsn.ubharajaya.ac.id

Amalia Syauket
amalia.syauket@dsn.ubharajay.ac.id
Bhayangkara Jakarta Raya University

Andi Tri Haryono
Wahid Hasyim University
anditri@unwahas.ac.id

Abstract

This paper will discuss the criminal provisions of data privacy law and anatomy of cybercrime law in Indonesia before the amendment of ICT Law and its implementation. During pandemic time, cyber incidents have increased over time. Indeed, cybercrime law in Indonesia regulates prohibition of hacking, phishing, illegal interception, carding, pornography, defamation and so on in accordance with the Electronic Information and Transactions Act (Undang-Undang Informasi dan Transaksi Elektronik, UU-ITE hereinafter also referred to as 'Indonesia ICT Law), Law No. 11 of 2008 which later on revised into Law No. 19 of 2016 and currently became Law No. 1 of 2024. At the same time, Law No. 27 of 2022 (Personal Data Protection/ PDP Law) concerning data privacy protection also stipulated criminal provision and already used in case law. This law can be a part of cybercrime law system in Indonesia side by side with Indonesia ICT Law. Back to Indonesia ICT Law, the implementation of this law can be seen in 210 case law which I have collected and analysed in this paper. I have found that cases are dominated by online defamation, hate speech on social media, pornography, and extortion. Meanwhile, these cases are relatively similar with 'ordinary crime' which is regulated in criminal code. The high technological crimes such as hacking, phishing, illegal interception, carding, are less shown, hereby. The highest case number is online defamation which ~~it~~ was also triggered by some human rights activists sued to judicial review through the constitutional court to eliminate ~~the~~ article concerning online defamation. The reason of judicial review concerning online defamation is because this article may potentially oppress the freedom expression, freedom of speech, and freedom of press. The anatomy of cybercrime law in Indonesia still remains some problems in legal norms and legal practice.

Keywords: cybercrime, defamation, hate speech, hacking

Introduction

Cybercrime may be classified as 'white-collar crime' which uses internet as a new technological means (Castells, 2001). Indonesia is facing the booming of digital economy with e-commerce, financial technology, social media and so on which attract billions USD over time. However, this booming of digital economy is sometimes accompanied with increasing cybercrime in Indonesia. Cybercrimes such as hacking, phishing, content offences like pornography, and copyright offences also exist in Indonesia since the booming of digital economy in the past decade (Castells, 2001). Indonesian citizens seem to become a potential victim of cybercrime (Angkasa, 2018). Cybercrime in Indonesia has been prevented by Indonesian National Police Force that concerns to the incident of credit card frauds, e-banking scams, illegal interceptions, cracking e-commerce, etc (Lim, 2013). However, these high technological crimes are less shown in case law. I have collected 210 case laws which contained criminal cases of cybercrime in Indonesia since 2008-2019. The cases are dominated by online defamation, hate speech on social media, pornography, and extortion.

Meanwhile, cybercrime regulation can be seen at PDP Law. Several articles are stipulated in Law No. 27 of 2022 ranging from illegal usage of data privacy (Article 67) and data forgery (Article 68). Actually, Indonesia PDP Law is inspired from Europe General Data Protection Regulation (GDPR). However, the criminal provisions are a content which created by local consensus between Indonesia Ministry of ICT and Commission I Indonesia Parliament. This criminal provision can be an opportunity and challenges for an effective law enforcement in the practice. Research by PRIVASIMU, a special company for data privacy consultant and technology states that the readiness of privacy compliance less than 40 % in 2024. A criminal provision can be a threat or stimulation for awareness and readiness of privacy compliance. There was a case in District Court of Karanganyar on 4 November 2022 related to illegal usage of data privacy and data forgery based on Law No 27 of 2022. This PDP case becomes one of pivotal academic source to be studied from perspective of cybercrime law system.

During the COVID-19-time, cyber incidents have escalated. Indonesia National Police of Cyber Division has received 2,259 reports of cybercrime cases such as 1.048 fake news/ hoax/ defamation, 649 online fraud, 208 online pornography, 138 illegal access, 39 data breach, 32 online gambling, and 24 illegal interception, etc (Patrolisiber, 2020). However, only some cases are proceeding though the court.

On case law, the cybercrime with high-tech category such as hacking, phishing, carding, cracking, encryption, and soon is not much showed. However, based on the report of ID.CERT, Indonesia Computer Emergency Response Team has released a study of cybercrime incidents (Bjork, 2002). The last report that they published was in May-June 2018 which contained intellectual property rights offences considering the amount of 8.053 incidents. Spam has is 4.233 reports, network incidents are composed of 2.700 cases, malware comprises 1.761 cases, spoofing or phishing contains 1.063 cases, spam complaints are composed of 762 cases (ID.CERT Report, 2019). Nevertheless, these cases are not glimpsed at case law in the courts. These cases are an important data on how huge number of cybercrime incidents. Hence, two things remain. First, the high number cybercrime incidents show criminal justice system as the final tool to solve the cybercrime problem. The government and civil society may

handle these cases through alternative dispute, administrative law, or civil law procedure. Therefore, the criminal prosecution is not much used to take over cybercrime. Second, this may be the opposite side of the first thesis. Criminal justice system is not much effective to be used to puzzle out cybercrime problems in Indonesia. Or simply put, some case law are not yet uploaded by the Indonesian Supreme Court at its website.

I downloaded these 210-case law from the Indonesian Supreme Court's website and begin to analyse them in accordance with Indonesia ICT Law. Since 2008, Indonesian government has issued regulation concerning the Electronic Information and Transactions (Undang-Undang Informasi dan Transaksi Elektronik, UU-ITE hereinafter also referred to as 'Indonesia ICT Law), Law No. 11 of 2008 which later was on revised into Law No. 19 of 2016. This law is the only one of legal product which stipulates cybercrime. Even though the other regulations such as cyber security, data protection, e-commerce, social media, financial technology, and so on are demanded, the complete digital law package still has a long way to go. At the present time, Indonesia ICT Law applies to define and regulate cybercrime with vulnerabilities.

Indonesia ICT Law was originally designed to secure electronic business transactions (Lim, 2013). This is why to regulate cybercrime; this law may be insufficient to cover all problems. Some issues mentioned above is not yet stipulated in this law, including detailed formulation of digital forensics. Regarding digital forensics, police use frequently the regulation of chief of Indonesian National Police (Perkap) No. 10 of 2010 (Prayudi, 2015). And, most of cyber law problems are handled by the Ministries' Regulation. The power of National Police's Regulation and the Ministries' Regulation is limited rather than the Act of Parliament. Least but not last, the Indonesia ICT Law is the one of regulation stipulating against cybercrime.

The anatomy of cybercrime norms can be seen at Indonesia ICT Law. Article 27 is the most popular one. Article 27 contains prohibition of cyber porn in accordance with Article 27 (1) of Indonesia ICT Law No. 11 of 2008. Prohibition of gambling stipulates in accordance with Article 27 (2). Article 27 (3) is the most controversial one in the implementation among Article 27 which comprises prohibition of online defamation. Article 27 (4) is composed of prohibition of extortion or threatening. Furthermore, Article 28 contains two Articles which stipulates the prohibition of fake news that damaging customers in accordance with Article 28 (1) and the prohibition of hate speech in accordance with Article 28 (2). Whilst the substance of Article 29 is the same as Article 27 (4) about prohibition of extortion, violence and threatening through cyber space. Article 27-29 is merely about 'ordinary criminal offences' which are regulated also in criminal code or other regulations, but these are not 'high-tech' of cybercrime such as hacking, phishing, carding, cracking, encryption, etc.

Meanwhile, Article 30 comprises prohibition of without permission entering electronic system of the other, prohibition of copying and destroying cyber security system. Article 31 is composed of prohibition of illegal interception. Prohibition of stealing data, to destroy, to edit, to hide, and to change information within electronic system of the other person in accordance with Article 32. Any person, in purpose, and without permission, and violation of law, who disturbs the other person's electronic system should be punished in accordance with Article 33. In addition, Article 34

contains prohibition to provide software and hardware to criminal offenders who acted to infringe Article 27 to Article 34. The last Article of criminal provisions of Indonesia ICT Law is Article 35, the hacker who changes the information which looks like original one, he or she will be punished. These articles are stipulated in the Indonesia ICT Law No. 11 of 2008. The latest revision of this Law, issued the new law No. 19 of 2016 which amended the previous law, especially revised criminal provisions.

From 210 case law, online defamation is the highest number of cybercrimes in Indonesia which comprises 35 % or 74 court's verdicts of total cases in accordance with Article 27 (3) of Indonesia ICT Law. After online defamation, second highest case is a hate speech on social media which composed of 20 % or 42 cases from total of 210 criminal cases in accordance with Article 28 (2) of Indonesia ICT Law. Furthermore, online pornography has occupied the third largest number of criminal cases about the same amount of 15 % of total criminal cases in accordance with Article 27(1) of Indonesia ICT Law. Only two cases are about carding which describes the offenders who has stolen money from Automated Teller Machine (ATM) of some banks in Bali. Some of these cases will discuss below.

Cybercrime related to data privacy

Law No 27 of 2022 concerning data privacy protection is enacted on 17 October 2022. This law has a reconcilement period within 2 years. However, the criminal provision is already implemented since its being issued. This regulation stipulates several criminal provisions ranging from illegal usage of data privacy (Article 67) and data forgery (Article 68) as well as providing seizure mechanism from criminal offence of data privacy (Article 69) and the board of director, beneficial owner, employee and management within a company and can be punished for 10 times (Article 70).

On 4 November 2022 a suspect, HIS lived in the Regent of Karanganyar, sent a message to YN. He claimed as a police officer, HM from the District Police Office in Central Java. HM is a vice director of special crime investigation in the Central Java District Police Office did not know that his name was being used to cheat YN. Meanwhile, YN is an entrepreneur who quite close with his friend at police community. HIS asked YN for a money and gave a reason that he had a working trip from Semarang to Jakarta. YN transferred sum of 10,000,000 IDR to HIS related to HIS request. Because of HIS act, YN loss sum of money after he realised he contacted to HM. HM who did not know and refused that he received sum of money informing YN that a phishing or social engineering occurred against him. Finally, YN, reported HIS to the police office for further investigation.

Judge, Agus Komarudin considered that HIS act was proven a guilty in exploiting YN privacy data for his benefit and affected a loss for YN. First, HIS as a natural person and had a criminal intention to cheat YN. HIS has a legal responsibility to be liable in committing his act and is not person disability in physically and mentally. Second, HIS evidently falsified his identity and used HM name to be used in cheating YN. He manipulated data privacy and contact of YN and HM in his action. Third, HIS objective was to make a profit from his action and suffered YN sum of loss up to 10,000,000 IDR. HIS obtained a punishment to pay 1 billion IDR and 4 months imprisonment.

Online defamation

As mentioned above, online defamation comprises 35 % or 74 court's verdicts among 210 case law that I collected within this study. Because in the case law stays in the top level of grievance in the criminal justice system, this case can be said as the most controversial criminal provision in Indonesia ICT Law. This section will discuss the implementation of Article 27 (3) of Indonesia ICT Law. This Article has ever been sued through the Constitutional Court for judicial review twice, but the Court seems to preserve the existence of this article. One of most popular case was Prita Mulyasari who complained service of hospital but her complaint was recognized as defamation by hospital. This article is often to be used to criminalize journalist and seems to put the freedom of press at risk.

One of online defamation case was held in 2008, Prita Mulyasari got high fever and went to the Omni International Tangerang Hospital. She felt headache, vomiting, and pain besides high fever. She went to the Emergency Department and was treated by one of doctor in the first help urgent care. Shortly after she was referred by specialist doctor and she felt her condition was down. She pained in her arm and neck. After moved to another hospital, she made a complaint and she received unpleasant response by one of customer service at hospital. She sent her story to some of her friends about her condition. By sending an email concerning the lack of hospital service, Omni International Tangerang Hospital sued Prita through the court. The first case, the judge decided that Prita was not guilty. [1] The public prosecutor appealed this case to the supreme court and decided the opposite to the first court, mentioned that Prita was punished for 6 months imprisonment.[2]

This case was dramatically controversial one at that time. Once the Indonesia ICT Law issued, this case used this law to prosecute Prita who from public side was innocent. Social media campaign was broadly escalated to support Prita. Moreover, people made a crowdfunding for Prita with tagline 'the coin for Prita.' This campaign has successfully gained more than 50.000 USD to support Prita.[3] Fortunately, the last verdict of supreme court on September 17, 2012, decided that Prita was innocent and free from any suspicion of criminal offence. The judge's legal reasoning found that Prita did not have any purpose to make defamation toward the image of hospital service.[4]

The Prita case withdrew many attentions of legal scholars such as Satjipto Rahardjo, an Indonesian socio-legal philosopher. He argued that Prita as ordinary women, a housewife, a mother from two kids. The first child was three-years-old and second child was one-a half-year-old. She is not corruptor, killer, and criminal. However, due to her email (complaint), she had trouble with criminal justice system (Rahardjo, 2009).

Prita was suspected in accordance with Article 27(3) of Indonesia ICT Law. This Article is known as 'a rubber article (*Pasal Karet*)', and too slippery to prosecute innocent people. After Article 27(3) is often used by criminalising innocent people, some human rights activist submitted this article into judicial review through the Constitutional Court. The first case was submitted on December 28, 2008. Naliswandi Piliang, a journalist who wrote a reportage about the gossip of Initial Public Offering

(IPO) for PT Adaro which involved some politicians who are suspected for corruptions. Naliswandi was reported to the police and in charge for defamation. He submitted a judicial review complaint through the Constitutional Court and argued that Article 27 (3) of Indonesia ICT Law against Article 28 of Indonesian Constitution concerning human rights provision.[5] The second case was submitted with wider complainants comprises some journalists and NGOs on January 6, 2009. The complainants were Edy Cahyono, Nenda Inasa Fadhilah, Amrie Hakim, the Legal Aid and Human Rights Foundation (PBHI), The Press Legal Aid Institution (LBH Pers), and Alliance of Independent Journalists (AJI). They claimed that they have a legal standing to submit a judicial review since they have their own website as journalists as well as the institutions. They demanded for freedom of expression, freedom of press, and democracy. What they have to complain is about the Constitutional Court removing Article 27 (3), not only because this article against the human rights provision of Indonesian Constitution, but also, they argue this article was the opposite with the idea of rule of law and people sovereignty in democracy era.[6]

Online defamation in accordance with Article 27 (3) of Indonesia ICT Law is most controversial issues in its implementation. From these two judicial review cases, the Indonesian government argued that this article is demanded due to protect individual's dignity, self-image, prestige or social branding. Furthermore, Indonesian Government stated that this article was previously inspired from Article 310 and Article 311 of Indonesia Criminal Code. Herewith, Indonesian Government insisted that this article is already existed in the criminal legal system and the Indonesia ICT Law just empowered this article based on information technology means. Even though Article 310 and Article 311 of Indonesian Criminal Code have a different formulation, Article 27 of Indonesia ICT Law recognizes them as the one-unit formulation. Article 310 contains defamation which any one may be punished for 9 months and Article 311 comprises slanders with punishment for 4 years. Article 27(3) of Indonesia ICT Law makes two types of criminal offences such as slander and defamation as the same act. Therefore, the citizens who are penalised with this article can be distinguished whether he or she is charged for slander or defamation. The suspect may be prosecuted for 4 years imprisonment directly. Many legal scholars reveal this article unjust and inadequate clear to be implemented.

A charismatic legal scholar, Prof Soetandyo Wignjoseobroto became an expert witness within judicial review concerning Article 27 (3) stated that no clear suspect formulated whether slander or defamation. If the suspect is criminalised for defamation but he or she may be charged for 4 years, that is too heavy to be received by this suspect. However, the Constitutional Judges made a verdict to refuse the appeal and Article 27 (3) of Indonesia ICT Law is still existed until now.

Indeed, the case of judicial review was submitted by some journalists and NGOs that concerns in issue of freedom of press. Because this Article 27(3) of Indonesia ICT Law may become a threat for democracy, especially freedom of press. In fact, some case law has shown that journalists have been criminalised by this Article. Some cases are delineated that journalists under threats when they reported a case of corruption scandal. On September 28, 2016, Dieri Lihawa was suspected for defamation after he

wrote an article about corruption within his media 'Sultra Satu News.' He faced three months imprisonments.[7] The same thing happened in 2018, Mara Salem was criminalised after reporting a corruption of public hospital in Medan. He wrote a reportage in his portal named 'online lesser news today.com.' He obtained imprisonment for a year.[8] Another case was about Mangatur Purba, a journalist recorded a fighting at the Doloksanggul Public Prosecutor Office and uploaded to his Facebook account. After court-hearing process, the judges made their decision that he got three months imprisonment and fine for 2 million rupiah (150 USD).[9]

From the case law discussed above, online defamation contains 35 % or 74 cases occupies the highest rank of cybercrime cases in Indonesia. Indeed, this Article 27 (3) of Indonesia ICT Law may performs to protect the dignity of individuals. However, this article should be used carefully to maintain freedom of press and freedom of expression.

Hate speech on cyber space

From 210 case law, hate speech on cyber space occurred 20 % or 42 cases as mentioned above. Prohibition of hate speech is not only regulated in the Indonesia ICT Law, but also it regulates in several regulations. Hereafter, the prohibition of hate speech, indeed, as the important legal norms in Indonesia. In the past decade, hate speech is escalated during the Jakarta Gubernatorial Election in 2016 since Basuki Tjahja Purnama a Chinese Jakarta Governor incumbent has run for Governor candidate. Islamic populism vis a vis racism was taken place in public sphere, especially on social media. Police and public prosecutor had arrested some key persons such as Jonru Ginting and community so-called Muslim Cyber Army. From the approach of Indonesia ICT Law, these cases can be evaluated from Article 28 (2) that stipulates prohibition of hate speech on cyber space.

Political populism triggers increased hate speech (Marwan, 2018). Hate speech, indeed suffers minority groups whose position is in vulnerability among legal or social protection system. From critical race theories, verbal racial attacks intend to encourage the victim to think his or her identity as inferior to the attacker (Lim, 2013). In Indonesia, Islamic Populism is increased since the Islamic right wing previously grew in prominence due support by top military and police leaders (Hadiz, 2016). However, Indonesian government has issued some regulations which comprises the prohibition of hate speech and banning racism.

The legal norms on prohibition of hate speech has been regulated in several regulations, such as the right of freedom from discrimination in accordance with Law NO. 39 of 1999 concerning human rights; the punishment for hate speech and spreading racial hatred is imprisonment for five years and a fine sum of 500 million IDR in accordance with Article 16 of Law No. 40 of 2008 concerning Eradication of Racial Discrimination; Article 156 of Indonesian Criminal Code in essence regulates the legal protection of minority, and Law No. 29 of 1999 concerning ratification of International Convention on the Elimination of All Forms of Racial Discrimination. The legal system regulates the prohibition of hate speech and Article 28 (2) has specifically stipulated this prohibition through information technological means. Article 28 (2) of Indonesia

ICT Law is written that 'anyone who in purpose and without rights spreads information which contains hate or propaganda towards specific individual or group with background of race, religion, ethnicity, and other social classes.'

Hate speech is originally occurred since long time ago in Indonesia. During the colonial era, social hierarchy was too huge and until intellectual group of young Indonesian student appeared in public sphere to resist the status quo (Suryadinata, 1971). The legal position of minority group in the Netherlands Indies was quite vulnerable (Cheong, 1981). At that time, Indonesian citizen of Chinese descent had also obtained ethnic bullying. During 1965 after failed coup, the purge affected to escalated conflict and racial sentiment (Cribb, 2002). After that, during the economic crisis of 1998 exposed ethnic tensions whilst the collapse of the New Order Government (Bjork, 2002). At the present time, hate speech increases as mentioned above, during the Gubernatorial Election in Jakarta. In April 2019, the presidential election, the hate speech is still growing and police trying to tackle it effectively.

One of popular case in regards with Article 28(2) of Indonesia ICT Law is the case of Jonru Ginting. Jonru Ginting has original name as Jon Riah Ukur. He is well-known as the actor of Islamic right wing who has a lot of followers on social media. Furthermore, he frequently penetrated propaganda of Islamization in public sphere against minority, non-Muslim, and foreigners. Whilst, he used to become a speaker and trainer in seminar with many audiences involved. On September 30, 2017, he arrested by the Indonesian National Police with suspicion of hate speech on social media. He was suspected to violate Article 28 (2) of Indonesia ICT Law and Article 16 of Law No. 40 of 2008 concerning Eradication Racial Discrimination. He has faced charges of inciting hatred and discrimination against minority group in Indonesia. One of his statement in his Facebook account was written that '1945 we got independence from the Netherlands and Japan, 2017 we have not been independence yet from conquer of Chinese.' From this status, he received 12.885 likes, shared by 2.037 people and 556 comments. This huge number of likes, share and comments mean that his status is more or less powerful and influential in social media. The public prosecutor indicted him from his controversial statements on social media. Shortly after, the judges decided that Jonru is charged for hate speech, punished 1 year 6 months imprisonment and fine sum of 50 million IDR.[10]

Some cases can be analysed here. Muslim Cyber Army, social media groups and individuals who penetrate to produce political campaign, has engaged and contributed to hate speech escalation. Muhammad Faizal ~~who~~ charged for hate speech stated that 'warning please, help Muslim Cyber Army and Cyber Native Indonesian to fight against the General Election Body of Jakarta (KPU). At this time, hacker team from abroad has already hacked KPU's server and manipulated vote. Do not believe in survey institute which has already been bribed by the Chinese foreigners (Asing Aseng).' Some his statements are problematic such as 'although Quran was burned by a pervert Chinese, Muslim can survive', 'the President is just a doll of People Republic of China,' etc. Faizal was suspected hate speech in accordance with Article 28(2) of Indonesia ICT Law. He is charged for 1 years and 6 months imprisonment and fine sum of 200 million IDR.[11] Another case charged Muhammad Tamim Pardede who

uploaded some videos in Youtube which comprises content of 'welcome, Chinese Communist brother,' 'betrayal and fraud by Chinese Communist,' 'Chinese Prime Ministry of Penis,' and 'the Danger of Chinese Communist.' His statements infringed Article 28(2) of Indonesia ICT Law and punished for 2 years imprisonment and fine sum of 200 million IDR.[12] Not always case suspected with Article 28(2) of Indonesia ICT Law. Meanwhile, Sandi Ferdian from Way Kanan charged for hate speech due to his statement on Facebook regarding 'Megawati (ex-President of Indonesia and the head of Indonesian Democratic Party for Struggle) requested to the government to ban Azan,' and posted on Group United Muslim Cyber Army about 'save our member, Indonesian Communist Party is innocent and Islam is pervert.' His statement actually does not contain hate speech and insulting ethnicity. However, Sandi is charged with Article 28(2) of Indonesia ICT Law ~~which~~ composed of 1 year imprisonment and fine sum of 500 thousand IDR.[13] This last case is a bit vague to be brought into the interpretation of Article 28(2) related to hate speech.

This article had ever been submitted for judicial review through the Constitutional Court in 2017. The appellants were Habbiburokhman and Asma Dewi who wondered that the activity to criticize the government can be criminalised due to suspicion of hate speech. The constitutional judges refused the appeal to remove the Article 28 (2) Indonesia ICT Law.[14]

Hate speech or cyber racism in accordance with Article 28 (2) of Indonesia ICT Law may function to protect minority and promotes tolerance. From total cases of 210 case law, hate speech contains 20 % or 42 cases are legal fact and number of cases which delineated the criminal justice system in digital era fighting against racism. However, the interpretation of this article should be a proper way. This article may be used to oppress the opposition or critique against status quo.

Cyber porn

Cyber porn contains 15 % of total 210 cases as mentioned above. The concept of prohibition of pornography is somehow problematic from feminism legal school. Mostly cyber porn cases are involved women as the victims. As it can be glimpsed several cases related to cyber porn positions women as a victim.

'The internet is relatively new. Pornography is not.' Lim's quotation emphasizes distinction between definition pornography by male author and female author. The result is different. What the male author writes pornography is to emphasize that this act as infringement of moral and social norm of Indonesian society. Pornography is forbidden and condemned. The view is merely moved by female author who concerns to how secure a woman as a victim (Lim, 2013). However, the bad side is to capitalise pornography for industrial interest and against victimize woman.

In fact, as mentioned above, cyber porn makes woman in vulnerable position and at risk to become victim. One popular case is Baiq Nuril Maknun, an outsourcing teacher at public high school of Mataram, she received a call from the head of school. In Indonesia, an outsourcing teacher position is weak, she may terminate if she has a little mistake. The call contained the head of school's story about his experience in making in love with someone. He told her that he was so strong in making in love, with

many styles including doggy style, blowjob and so on. Baiq Nuril felt uncomfortable with this talk and recorded. She planned to report this conversation to Board of Education concerning impropriate act of the head of school. Despite her complaint responding and she gets legal protection, she was reported by the head of school as her records of talk in accordance with Article 27 (1) of Indonesia ICT concerning cyber porn. In the first level of court, judges stated that Nuril's suspected criminal offence was unfounded.[15] However, the appeal court, unfortunately Nuril charged for 6 month and fine sum of 500 million IDR.[16] This case has been criticized by many human rights activists and scholars. Despite Nuril supposedly became a victim of 'verbal sexual harassment,' she was criminalised by the criminal justice system. In some occasions, Article 27(1) of Indonesia ICT Law is quite problematic in its implementation.

Article 27 (1) is originally not designated for prohibition of pornography. The formulation of Article 27 (1) of Indonesia ICT Law is 'anyone in purpose and without right distributes, transmit, produce to be accessed electronic information which contains substance that violates ethics or social norms or politeness.' The word of politeness refers to forbidding impoliteness or unpleasant act which infringes social norms of Eastern values. However, the implementation of Article 27 (1) is mostly about cyber porn. By the same token, this Article, furthermore, affected victimization of woman in some cases. In August 2016, a woman was exposed her naked picture with her ex-boyfriend. In the past, she terminated her relationship with her ex-boyfriend and shortly after her ex-boyfriend got upset then distributed her naked photo through social media.[17] The naked photo, indeed, was damaged her reputation and she felt stressful because of that. Another case occurred in Banjarmasin, a woman broke his relationship with boyfriend and started to make relation with her new boyfriend. Her ex-boyfriend did not accept to be terminated and sent her naked picture to her new-boyfriend. She felt embarrassed and reported this improper act to police.[18] The similar case happened, a broken relationship ended with ex-boyfriend shared naked picture of his girlfriend through Facebook. Victim became to feel embarrassment and reported to police.[19] Herewith, the cases almost have similar modus operandi. A broken relationship, ex-couple conducted 'a revenge' to share naked picture of woman. Woman hereby becomes a victim.

Some cases of cyber porn comprise 15 % of total 210 cases ~~which~~ related to woman who potentially becomes a victim. Article 27 (1) may function to become legal shield for woman within digital era. However, digital literacy to woman is demanded to prevent woman to become victim of cyber porn. Never naked in the front of camera, even with her boyfriend or spouse.

Carding

Only two cases from 210 case law are composes of carding. A suspect had stolen money from Automated Teller Machine (ATM). He did not hack e-banking or internet banking. But his modus was merely to put a card reader within ATM and obtained victim's secret code and scanned debit card. On February 23, 2016, a person from Republic of Moldova put a scanner machine in ATM. he could duplicate debit card afterward and stole 424 million IDR from 38 banking customers. After he was

arrested, he was charged in accordance with Article 30 (2) of Indonesia ICT Law. The judges punished them for two years imprisonment and fine sum of one billion IDR.[20]

Another case was occurred on Marc 27, 2018. A perpetrator inserted a skimming machine named 'a card-reader writer encoder.' With this machine, he could copy debit card of banking customer who used ATM. After police arrested him, he was suspected in accordance with Article 30 (2) of Indonesia ICT Law. Shortly after, the judge in Denpasar Court decided to give him a punishment for 2 years imprisonment and fine sum of 500 million IDR.[21] The case of carding in Indonesia has similar modus operandi with putting scanner machine at the ATM and hacked banking customer using ATM to get their secret number. Meanwhile, in the case law which collected 210 cases, none of them are criminal offences of hacking, phishing, copyright offences, cracking, and so on which are shown in court's verdict.

With these two cases, police can simply strengthen security around the ATM. Adding security agents, enhancing CCTV, and educating people to participate in reporting the suspected activity at the ATM, may secure people from these two cases of carding. However, hacking of mobile banking or internet banking cannot be shown in court's verdict. In media, this case of hacking into mobile baking or internet banking exist. A black hat hacker may use Trojan to steal secret number and banking records of customer.[22] Or various method which at the present time, the modus operandi is still developing over time.

Cybercrime is regulated in Indonesia ICT Law No. 11 of 2008 which contains prohibition of cyber porn, threatening, defamation, gambling, hate speech, hacking, phishing, illegal interception, and so on. This criminal provision of Indonesian ICT Law also can be seen its implementation in 210 cases from 2008-2019. From 210 cases, 35 % or 74 court's verdicts are about online defamation, 20 % or 42 hate speech or cyber racism cases, 15 % of total criminal cases are about cyber porn. Only two cases from 210 cases are a carding offence. There was none of them cases about hacking, phishing, illegal interception, intellectual property offence, malware, and so forth. I also discussed some popular cases above, such as online defamation which shows Prita case. Prita was convicted for online defamation toward Omni International Hospital. Civil society supported Prita because she did not have a criminal intention to send a complain concerning lacked service of hospital. Shortly after, her suspected crime was unfounded by the judge. Prita was one example of case law concerning online defamation. Online defamation in accordance with Article 27(3) of Indonesia ICT Law has been challenged through the Constitutional Court. Some human rights organisations such as the Legal Aid and Human Rights Foundation (PBHI), The Press Legal Aid Institution (LBH Pers), and Alliance of Independent Journalists (AJI) and journalists such as Edy Cahyono, Nenda Inasa Fadhilah, and Amrie Hakim issued this article and revealed that this article opposites freedom of expression, freedom of press, and freedom of speech. Unfortunately, the constitutional judge refused the request to eliminate this article. The legal norm of online defamation may become of threats of freedom and democracy.

Conclusions

Cybercrimes in the era of pandemic have increased. Meanwhile, the Indonesia Cybercrime Law (Law No. 8 of 2011 revised to Law No. 9 of 2016) has already become a legal basis to combat cybercrime. Despite the original intension of this law is actually for commercial transaction. This is why the cybercrime enforcement seems not optimal. This cybercrime law has also been criticised by human right activists due to many infringements upon freedom of expression. However, for the time being, this law can be used temporarily for the enforcement of computer crime and other forms of cybercrime such as pornography, racism, and so on and so forth. The Indonesia cybercrime law (Law No. 8 of 2011 which is revised to Law No. 9 of 2016 and Law No. 1 of 2024) as anatomy cybercrime regulation that prohibits of cyber porn, online defamation, extortion or terror, racism, illegal access, illegal interception, data interference, etc. In the near future, these criminal provisions can be unified into a criminal code which may be easier to use as codified cybercrime law. Furthermore, criminal provision of data privacy law can be used to prevent and handle a cybercrime related to data privacy exploitation. A case was already used this law, a criminal obtained fine sum of 1 billion IDR and 4 years imprisonment under Article 66 and 68 Law No. 27 of 2022. The use of this criminal provision should be careful in preventing abuses and bias since the reputation of ICT Law was also misuse in some cases.

Reference

Angkasa (2018). "Legal Protection for Cyber Crime Victims on Victimological Perspective." *SHS Web of Conference* 54 08004: 1–6.

Bjork, Christopher (2002). "Reconstructing Rituals : Expressions of Autonomy and Resistance in a Sino-Indonesian." *Anthropology&education Quarterly* 33, no. 4: 465–91.

Castells, Manuel (2001). *The Internet Galaxy: Reflection on the Internet, Business, and Society*. Oxford: Oxford Unievrsity Press.

Cribb, Robert (2002). "Unresolved Problems in the Indonesian Killings of 1965 – 1966." *Asian Survey* 42, no. 4: 550–63. http://www.jstor.org/stable/10.1525/as.2002.42.4.550.

Douzinas, Costas (2007). *The End of Human Rights?* Oxford: Hart Publishing, 2000. https://doi.org/10.1525/sp.54.1.23.

Lim, Merlyna (2013). "The Internet and Everyday Life in Indonesia : A New Moral Panic ?" *Journal of Humanities and Social Sciences of Southeast Asia* 169: 133–47.

M Irfan, MA Ramdhani, W Darmalaksana (2018). "Analyzes of Cybercrime Expansion in Indonesia and Preventive Actions." *3rd Annual Applied Science and Engineering Conference (AASEC)*. https://doi.org/10.1088/1757-899X/434/1/012257.

Marwan, Awaludin (2018). *Good Governance and Ethnic Minorities in Indonesia*. Utrecht: Utrecht University.

Mun Cheong, Yong (1981. "A Survey of Some Dutch-Language Materials on the Chinese in Indonesia." *Journal of Southeast Asian Studies* 12, no. 1: 27–37.

Prayudi, Yudi (2015). "A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia," no. October: 1–8. https://doi.org/10.5815/ijcnis.2015.11.01.

Siburian, Henry Kristian (2016). "Emerging Issue in Cyber Crime : Case Study Cyber Crime in Indonesia." *International Journal of Science and Research* 5, no. 11: 2013–16. https://doi.org/10.21275/ART20162818.
Suryadinata, Leo (2018). "Pre-War Indonesian Nationalism and the Peranakan Chinese Author." *Asia, Southeast Publications, Program* 11, no. 11: 83–94.
Case law
Banjarmasin Court's verdict Number 990/Pid.Sus/2018/PN Bjm.
Bau Court's verdict Number 158/Pid.B/2017/PN Bau.
Blambangan Umpu Court's verdict Number 101/Pid.Sus/2018/PN Bbu.
Constitutional Court's verdict Number 50/ PUU-VI/ 2008
Constitutional Court's verdict Number 2/ PUU-VII/2009
Constitutional Court's verdict Number 76/PUU-XV/2017
Denpasar Court's verdict Number 4/Pid.Sus/2018/PN Dps.
Denpasar Court's verdict Number 573/Pid.Sus/2018/PN Dps.
Jakarta Court, verdict Number 326/ Pid.Sus/ 2017/PT.DKI.
Jakarta Court'verdict Number 350/Pid.Sus/2018/PT. DKI.
Supreme Court's verdict Number 574 K/ Pid.Sus/ 2018.
Tangerang Court Decision Number 1269/PID.B/2009/PNTNG on December 29, 2009
The Supreme Court Verdict Number 822K/ PID.Sus/2010 on June 30, 2011
The Supreme Court Verdict Number 225 PK/ PID. Sus/2011, on September 17, 2012.
Tarutung Court's verdict Number 207/Pid.Sus/2018/PN Trt.
Kuala Kapuas Court's verdict Number 109/Pid.Sus/2018/PN Klk.
North Jakarta Court's verdict Number 1105/Pid.Sus/ 2017/PN Jkt.Utr.
Medan Court's verdict Number 8/Pid.Sus/2019/PT.MDN.
Mataram Court's verdict Number 265/ Pid.Sus/ 2017 PN. MTR.

Online source https://megapolitan.kompas.com/read/2009/12/04/19465569/Koin.Peduli.Prita.Butuh.2.5.Ton.Recehan, accessed on June 5, 2019, see also: https://keuangan.kontan.co.id/news/bi-koin-prita-terkumpul-rp-81094-juta-1 accessed on June 5, 2019
https://www.cnnindonesia.com/teknologi/20170426160647-185-210311/trojan-ini-bisa-bajak-transaksi-internet-banking-di-android, accessed on June 7, 2019. See also, https://www.cnnindonesia.com/teknologi/20170411160549-185-206712/manfaatkan-virus-ajaib-peretas-bobol-atm-di-40-negara?, accessed on June 7, 2019.