Comparison of the Republic of Indonesia ITE Law No 19 Of 2016 with PDP Law No 27 of 2022 and the Role of the Police in Handling Cases Of Personal Data Dissemination (Doxing)

M. Riansyah Aksar Tarigan [1], **Patricia Riniwigati** [1]

[1] *University of Indonesia*
Kampus Depok, Depok, Jawa Barat, Indonesia

DOI: 10.22178/pos.106-35

JEL Classification: K39

Received 21.06.2024
Accepted 25.07.2024
Published online 31.07.2024

Corresponding Author:
M. Riansyah Aksar Tarigan
riansyahaksar@gmail.com

Abstract. As technology and information develop, regulations and laws are forced to govern the relationship between individuals and individuals in cyberspace. The emergence of Indonesian Republic Law No 19 of 2016 and the Personal Data Protection Law in Article No 27 of 2022 illustrates that the Indonesian government is also involved in maintaining order in Indonesian society on social media. However, what are the differences and similarities between the two laws in tackling the crime of doxing? Then, what is the role of the police in handling the criminal act of doxing in Indonesia? Law No 19 of 2016 concerning Electronic Information and Transactions and Law No 27 of 2022 regarding Personal Data Protection have a similar function in preventing the criminal act of spreading personal data (doxing). In the personal data protection law, suppose the ITE law discusses Electronic Documents and Electronic Information such as images, videos, and sound documents. In that case, the regulation discusses formal data such as genetic data, address, family, etc. The two laws complement each other, and both function as an effort to protect the public from the criminal act of spreading personal data (doxing). In the context of law enforcement officials, the police are currently very good at handling cybercrime because they are assisted by the presence of 11 sophisticated data forensic laboratories and other supporting tools, in harmony with the presence of qualified human resources to deal with cybercrime cases.

Keywords: Cybercrime; Doxing; IT Law; Police Role.

INTRODUCTION

Criminal behaviour can happen anywhere and at any time. It involves breaking the law and goes beyond that by including actions harmful to society, even if laws or criminal statutes do not explicitly regulate them [1]. In the digital age, tasks and education can now be completed efficiently and accurately through online methods. This has resulted in the storage of personal, company, and even confidential state data in internet-based network systems. For instance, the electronic identity card (E-KTP) is a government program in Indonesia that contains information about a person's family, address, and more.

Information theft, unauthorized use of data, and dissemination of one's identity are now widespread [2]. The reason for disseminating personal identity has reached an alarming stage. Especially in the online money lending sector, better known as '*Pinjol*'.

Online loans, or "*Pinjol*'', are widely used by the public because of the ease of disbursing loan funds and the many providers of these facilities, making the lower middle-class flock to online loan applications. Currently, the proliferation of online loans has had more negative impacts on social life in Indonesia than positive ones. Excessively high interest rates and inhumane ways of collecting debts are the adverse effects of the online money lending system. The unilateral use of personal data, even to the extent of disseminating customers' personal information, this action has entered the realm of communicating personal information or doxing without the consent of the person who owns the data. In other cases, the person has even been dishonourably discharged from his or her company because the

online money lending company is constantly terrorizing the victim's office. Because of this, the person has no livelihood to pay the debt while the interest grows and accumulates. Spreading personal information if a customer owes a debt to a third party is an example of doxing, which is spreading one's personal information to the public, not to mention the acts of terror that debt collectors inflict on customers.

In addition, data leaks have also entered entertainment, such as YouTube, Twitch, and other live-streaming video platforms. In the last decade, with the renewal of technology, information and communication, there has been a cultural shift in all aspects of life. Starting from technology that is developing so rapidly and massively, it covers parts of the world and all domains, both in security systems, communications, and vehicles, and not spared in entertainment.

The video-based social media, YouTube, is an online platform that markets various information through video content. Not only information, but YouTube also provides entertainment intake by covering all levels of society, not limited by age from children to adults. With the rampant development of this technology, many people have become famous very quickly through YouTube or social media. This is why there are so many cases surrounding the world of social media and internet networks, although the indicators are not only from one source.

Content creators on Youtube channels, often called 'Youtubers', have now become a job that can prosper a person's life. Their work requires each creator to make videos, advertise products, or do other creative works, and it has now become the main show in filling the daily lives of the world community. Content creators have various concentrations in presenting their creations, ranging from those that educate their audience to those that provide snippets of news, comedy, and music. However, the most popular content, in general, today is gaming content because all groups favour it, whether it is children or adults.

As part of the content creator community, a group of content creators call themselves 'Virtual Youtuber', often called Vtuber. These content creators live stream on YouTube, Twitch or other live-streaming video channels. The purpose of these Vtubers, of course, is the same as that of the usual YouTuber. However, the unique thing that distinguishes them from the others is that they wear animated characters that are played seriously, with a variety of their unique individuality and the distinctive voices of the Vtubers, to create an atmosphere that can entertain the audience and connoisseurs of Vtuber content.

They use two-dimensional animated characters, commonly known as 'Live2D Characters', translated as (Live Two-Dimensional Characters). This is their main asset for live streaming, creating content, and promoting merchandise individuals or corporate agencies advertise.

Not a little money is spent to make one Live2D animation character. Producing a character that can move like a natural person can be worth hundreds or even hundreds of millions. Usually, a Vtuber company agency can pour money into tens, even hundreds of millions, to create a set of Vtuber streamer groups, which will later become the main asset in running the company's economic turnover and attracting investors' attention to the Vtuber agency.

The issue in the world of Vtuber is that it is prone to doxing. Some people want to discover their identity and even leak the identity of the voice actor in the Vtuber character. Essentially, those who wish to leak the secrets of the character's voice actor to discover who the actor behind their idol is. This action is wrong and violates the applicable laws and regulations.

Doxing also has the potential to harm the company, as the individual Vtuber's talent can be jeopardized, and things can happen to them. For example, what happened in Japan, frequent doxing incidents in the country even made a "'Talent" from a Japanese Vtuber agency decide to quit his job because he was constantly being spied on and watched by his fans who liked his idol. The doxing culture in Japan has gone to the extreme, where idol fans even search for the idol's home location, terrorize them, and if the idol has a life partner, they do not hesitate to destroy the idol's life in various ways.

The mindset built by idol artist agencies in Japan is the purity of each group member, making each member appear as an angel to their fans. Therefore, they cannot be dirty, must always be kept pure, and must always look perfect. The formation of the audience's mindset of 'girl band groups' extends to "a female artist must not defecate". That is why idol culture has become part of the toxic culture In Japan, and it has even become a viewpoint for the whole world until now. If an

idol group/girl band cannot have a partner, it must always be perfect and keep their innocence.

This is one of the reasons why keeping the identity of Vtuber personnel a secret is so important, as the value of a mysterious personality is also an essential asset for Vtuber agencies and companies. In addition to stalkers, Vtuber talents are also often exposed to 'body shaming' due to their looks that do not match the expectations of the audience and so on. The main asset in portraying a Vtuber character is the voice of the personal Vtuber, not the physical appearance of the voice actor. This situation is also essential in maintaining the safety and confidentiality of the Vtuber personnel from doxing attacks in cyberspace or reality.

In handling Vtuber cases, there is rarely any formal action in domestic or international cases. The number of doxing cases is more common, specifically in Japan, for cases in the country are still relatively small. Vtuber doxing cases are usually resolved personally by the company and do not reach the court table. Even if the company reports an incident of leaking data of their group members, it is tough to uncover the case - because human resources and legal practices are still inadequate in disclosing similar cases. The economic impact can harm both the company and the Vtuber group personnel.

Dissemination of personal data or 'doxxing/doxing' is a criminal act within the scope of cybercrime [3]. This article is formulated in the ITE Law, which contains elements of cybercrime when spreading someone's information on social media or other media online. The explanation is in Articles 25 and 27, and the provisions are in Article 45.

The threat of Article 45 includes a maximum penalty of six years and a maximum fine of one billion rupiah. The nature of the ITE Law is individual or personal. If a case involves the ITE law, the person concerned can act against those who harm the person or group.

Furthermore, the author's understanding of Article 65 of the Personal Data Protection Law. This article explains that any person or party is prohibited from unlawfully obtaining personal data that does not belong to them for their benefit. In addition, the prohibition also applies to the disclosure of personal data that does not belong to them. However, this law will only become active in 2024 because the PDP Law was only enacted in 2022.

Furthermore, this journal will compare the PDP Law to discuss the ITE Law, which is still actively used by law enforcement in Indonesia. It is hoped that comparing the two laws will provide ideas in the world of law faculty academics.

METHODS

We thoroughly analyzed the cybercrime laws in Indonesia, specifically the Republic of Indonesia ITE Law No 19 of 2016 and Personal Data Protection Law No 27 of 2022. We aimed to compare these laws and understand how they address doxing and cyberbullying cases. We then focused on a specific case study involving the Vtuber Kureiji Ollie incident. We examined the legal complexities surrounding using aliases, reporting procedures, and the challenges of investigating anonymous suspects.

Moving on from the legal frameworks and case study, we investigated the law enforcement system in Indonesia, with a particular emphasis on the role of the Indonesian National Police (POLRI). We analyzed the skills of investigators, challenges related to handling digital evidence, and the availability of digital forensic laboratories across different regions.

To complement our legal and law enforcement analysis, we studied data on cybercrime cases in Indonesia over the past three years. By reviewing information from DITTIPIDSIBER BARESKRIM POLRI, we aimed to identify trends in threatening cases, overall cybercrime incidents, and the percentage of resolved cases.

Additionally, we conducted a comparative analysis of ITE Law and PDP Law, examining how each law addresses doxing *Pinjol* and cyberbullying cases. Our objective was to highlight the similarities and complementarity between these laws in protecting privacy and personal data. Lastly, we interviewed legal experts and law enforcement personnel to gain qualitative insights into the subject matter.

RESULTS AND DISCUSSION

Online Loan Doxing Case. There have been many cases of *Pinjol* lately, most of which have a similar modus operandi. Here are some examples of cases related to the criminal offence of doxing.

The Position of the AdaKami Lending Case. Based on data from the BBC News website, there are cases involving online loans. The case stems from a tweet from account X (formerly Twitter), which tells the fate of his family, who committed suicide due to online loans.


BBC NEWS INDONESIA

Berita Pemilu 2024 Indonesia Dunia Viral Liputan Mendalam Majalah

Pinjol AdaKami diduga teror nasabah karena terlambat bayar cicilan - 'Saya dibilang anak haram, orangtua dimaki dengan kasar'

Foto ilustrasi. OJK mengimbau masyarakat agar menggunakan layanan pinjol sesuai kebutuhan dan kemampuan bayar.

22 September 2023

Otoritas Jasa Keuangan (OJK) didesak mencabut izin perusahaan pinjaman online (pinjol) yang kedapatan melakukan pelanggaran dalam hal penagihan hingga skema pembayaran utang.

Pasalnya, kata pengacara yang menangani ratusan kasus pinjol, Ale Tamaela, praktik semacam itu terjadi di hampir semua pinjaman online, baik legal maupun ilegal.

Desakan tersebut mengemuka setelah viral cerita seorang pengguna pinjol AdaKami yang diduga bunuh diri akibat diteror penagih utang.

Direktur Utama AdaKami, Bernardino Moningka Vega Jr, mengatakan proses investigasi belum berlangsung karena keterbatasan informasi menyangkut pengguna.

Figure 1 – The Position of the AdaKami Lending Case (in Indonesian) [4]

The victim shared his story last Sunday (17/09/23) in a post entitled, "Father with a three-year-old child called to borrow money on the "AdaKami" application for Rp. 9.4 million". However, unexpectedly, the victim was then required to pay a loan of Rp.18–19 million, double the original loan. Unable to pay such a large bill, the victim was terrorized by debt collectors affiliated with AdaKami.

The bills that came into the victim at that time became uncontrollable until finally, the victim, who worked as an honorary employee at one of the government agencies, received similar terror when she was working in her office. The terror triggered the victim's dismissal, and as a result of the dismissal, the victim tried to conceal the incident from her family under the pretext that the office had not renewed her contract.

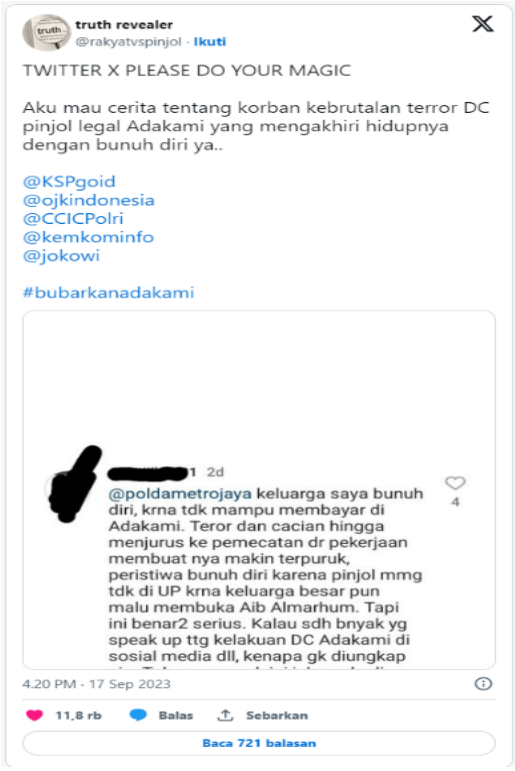

Figure 2 – Excerpt of sender X's tweet (Twitter) regarding the case of victims of loan sharks (in Indonesian)

Over time, the terror by debt collectors became more extreme to the point that fictitious orders attacked the victim. The victim was visited daily by five to six ojol drivers who delivered food and drinks. Several times, the victim's neighbours helped the victim by paying for the food, but because these fictitious orders came every day, the neighbours could not help the victim every day.

For that reason, some ojol blocked the victim's address, but some ojol got angry with the victim because the order was not paid. This incident continued until finally, the victim decided to end her life in May 2023. This story eventually went viral on social media and eventually involved the police to handle the case.

On the latest findings regarding the suicide case allegedly involving Pembiayaan Digital Indonesia or the organizer of the AdaKami peer-to-peer (P2P) lending fintech service. The Ogan Komering Ulu (OKU) District Police Chief stated that the identity of the man who committed suicide due to *Pinjol* cannot be known. The Polres has investigated all suicides in its leadership area, and the results cannot be found. The police finally asked the public to participate in reporting information related to the AkuLaku *Pinjol* case, especially from the victim's family.

Although this case is still not cleanly revealed, the big picture relates to the Personal Data Protection Law, where AdaKami should have used the data wisely, but instead, it was used to terrorize and so on. The act of fictitious orders carried out by debt collectors is one of the unlawful acts involving terrorizing by making the victim depressed, and other online loan applications have frequently used this method.

The doxing status in this case involved tracking the victim's home address identified through the debtor's registration account. In addition, the doxing also occurred at the victim's office, where the perpetrator terrorized the victim until the victim was defamed. Article 27 § 3 of the ITE Law falls under these criteria. They were publicly sharing documents (in the form of personal data of the victim's debt) with the public (here, the location is the office), causing the victim to be defamed.

The above can also be included in Article 65, paragraphs 2 and 3 of the Personal Data Protection Act, explaining that "every person who uses and discloses Personal Data that does not belong to him will be punished with imprisonment of four years and a fine of Rp. 4 billion for disclosing personal data, and five years imprisonment with a fine of Rp. 5 billion for the use of personal data that is not his right."

However, the PDP Law can only be used in 2024 because the PDP Law was only issued in 2022.

Position of Community Loan Application Pinjol Case. The AdaKami case that went viral above is still unfinished in its handling until the writing of this journal is carried out. Many netizens speculate that the victim's family may be tired of this incident and do not want to get involved with the police, or someone has silenced them, or it could even be that the case is indeed fictitious. Whatever the speculation, the status of the AdaKami case above is currently in the fact-finding process.

Apart from the AdaKami case, the author will discuss the case of a person already arrested by law enforcement in 2021. Here are the details of the following case.

A case occurred at the North Jakarta District Court [5]. The case involved threatening the victim, a woman with the initials MV, aged (32) who was caught up in online loans (*Pinjol*), threatened by the perpetrator with the initials MR, who was known to work as a debt collector. An explanation from the authorities provides a statement about the case of arresting a debt collector that originated from a report of MV, a 32-year-old woman from NTT (East Nusa Tenggara) Manggarai Regency, who was traumatized by the threats she received.

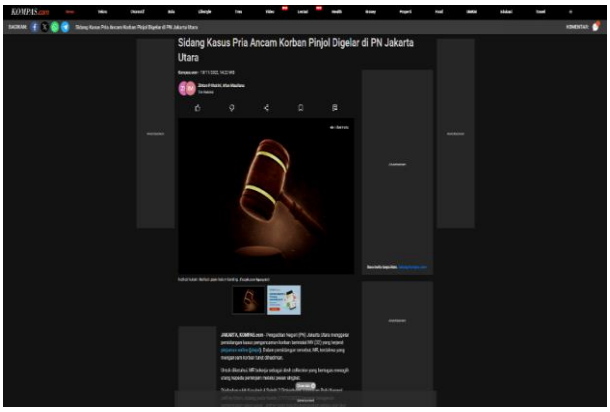

Figure 3 – Case excerpt from Kompas.com website (in Indonesian)

The perpetrator initially warned the victim using the WA (WhatsApp) application. As time went on, threatening messages were sent to the victim.

The threat was made because the victim had a loan of Rp. 1.3 million (one million three hundred thousand rupiah) in the 'Community Loan' application arrears. The threat made by the defendant to terrorize the victim was to terrorize fictitious orders, such as ordering food through the Go-Food application and sending it to MV's address. Fortunately, the fictitious order did not reach the victim's address, and MR, the defendant, was reported by MV, who filed a report with the police in East Nusa Tenggara. The file was eventually transferred to the Indonesian Police Headquarters to facilitate the investigation, as the perpetrator and witnesses were in Jakarta at the time of the case.

The police responded, "Debt collectors at that time had data on their victims that could be accessed to send messages to customers, the data in the form of ID cards, home addresses, photos, until the time when the customer's debt was due, everything was known by debt collectors. They later use this data to send threatening messages whose SOPs have been designed by the company, and these methods are carried out to terrorize borrowers."

The perpetrator was finally processed and arrested for his actions in terrorizing the victim. Therefore, the perpetrator was charged with Ar-

ticle 45 § 4 jo, Article 27 § 4 and/or Article 45B jo, Article 29 and/or Article 36 of Law No 19 of 2016 concerning Amendments to Law No 11 of 2008 concerning Electronic Information and Transactions.

The result of this case is that the Pinjol company that employs him has been frequently reported from many locations. Thanks to this case, the police have included the identity of the owner of the illegal online loan in the list of people being sought / fugitive (DPO).

A similar case occurred at the North Jakarta District Court, which tried a perpetrator with the initials DS, who committed an act of doxing against the victim witness with the initials MI, where the perpetrator intentionally disseminated electronic information or electronic documents containing extortion and threats by the content of Article 27 § 4 because the victim MI was late in paying his debt and penalties. As a result of the verdict, the defendant DS was proven legally and convincingly guilty and sentenced to imprisonment for one year and a fine of 70 million rupiah. If the fine is not paid, it will be replaced by imprisonment for two months.

Illegal Lending Case Position. This case involved five loan shark employees who shared their customers' data in Jakarta in May and June 2022 [6].

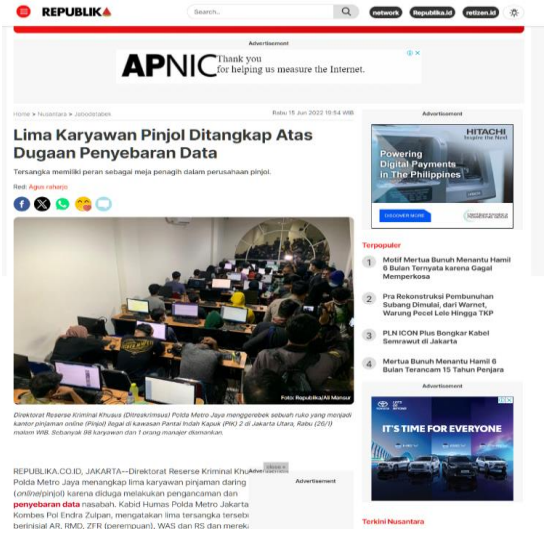

Figure 4 – Case excerpt from the Republika website (in Indonesian)

Dirkrimsus Polda Metro Jaya (PMJ) managed to arrest five debt collectors of the *Pinjol* application, who had spread personal data and threatened their customers. POLRI stated that the five suspects with the initials RS, RMD, AR, WAS, and a woman named ZFR were arrested on June 2, 2022.

According to information from the authorities, The suspects carry out their collection actions through the "online" system against each loan shark customer. What is at issue is the way to collect these collectors, which is by intimidation and using threatening sentences such as spreading customers' data.

The suspects, who worked as collectors, unilaterally used personal data belonging to customers. They carried out their actions using laptops, cell phones, and four SIM cards, which were used as evidence in this terror case.

The perpetrators were arrested because of customer complaints that went to the authorities. There were five incoming reports, leading the investigators to act against the five unscrupulous loan collectors.

Applications used by customers include Pinjam Bahagia, Cepat Pinjam, Dompet Selebriti, Kredit Easy, Dana Now, Dana Impian, Rupiah Go Pundi, Pinjaman Top, Pinjaman Sigap, Uang Cepat, Dompet Emas and Kotak Rupiah.

The perpetrators were then arrested under Article 27 § 1 jo, Article 45 §1 and/or Article 27 §4 jo, Article 45 §4 of Law No 19 of 2016 amending Law No11 of 2008 concerning Electronic Information and Transactions or ITE.

All suspects are punished with a minimum sentence of imprisonment for a maximum of 10 (ten) years and a fine of at least Rp. 700 million, or a maximum of Rp.10 Billion [7].

Analysis of Pinjol Cases Based on ITE Law & PDP. The three cases above illustrate the use of doxing provisions in tackling crimes of leaking, defamation, and the use of personal data without the owner's permission. All three tell how debt collectors have comprehensive access to customers' data.

1) Lessons Learned in the Three Cases of *Pinjol.* Customers usually fill out a registration form using an online money lending application. This form aims to record the seriousness and authenticity of the identity of the person who will borrow money from the application. Financial applications here are online loans and many applications that require similar data to determine the borrower's credibility. Examples are Go-Pay Lat-

er accounts, Shopee Pay Later, and applications requiring similar data.

The form is usually formatted to ask for a photo of the prospective customer's face, then a picture of their ID and occupation. They call this stage the "Verification" stage, where the lenders determine whether the borrower can repay their debts. At this stage, the lender can cancel or confirm the borrower's loan status eligibility. However, this is the red line between the customer and the lender.

The data sent by the customer is indeed recorded in the "data bank" or data vault owned by *Pinjol*, here in the form of electronic document data stored on internet-based storage (Cloud). As a society, we must be careful when placing our data. Of course, we must also look at the credibility of the *Pinjol* application, which we will later use. To reduce the chance of data leakage, prospective customers should use a loan application approved by the Financial Services Authority (OJK).

In this case, if OJK does not approve the application, then the status of the application is illegal. Doxing cases carried out by debt collectors, such as the example above, usually come from applications that the OJK does not monitor, so they can freely act when operating the *Pinjol* application.

The recent eradication of illegal *Pinjol* companies has been a breath of fresh air for people accustomed to using these applications. However, incidents like this still occur due to other factors.

2) Analysis of *Pinjol* Cases. The resolution of doxing cases committed by unscrupulous debt collectors can be resolved using the ITE Law and the Criminal Code that applies to this matter. For example, in the case of the arrest of five *Pinjol* employees who leaked data and threatened their customers, the following articles were charged; "

Article 27 § 1 jo, Article 45 § 1 of the ITE Law. Article 27 of the ITE Law is a type of crime committed because the perpetrator distributes, transmits, or can access electronic documents, which, if this happens, can cause embarrassment to the victim. At the same time, Article 45 describes the punishment imposed on the perpetrator. At the very least, the perpetrator will be subject to a maximum imprisonment of six years and a maximum fine of one billion.

Article 27 § 4 jo, Article 45 § 4 of the ITE Law. The provision in Article 27 § 4 of the ITE Law involves extortion in the actions carried out by the suspect so that the suspect can get a sentence of imprisonment for six years and a maximum fine of one billion."

If using Differential Association Theory, in the case of *Pinjol*, debt collectors in this case have the same tendency to carry out their actions. They do similar things, such as the action already having a template.

The actions of debt collectors in carrying out their actions are as follows:"

a) They are terrorizing the lineage if the debt is paid late.

b) If the customer refuses to pay, the collector will send a fictitious order to the customer.

c) If the customer still does not pay, the debt collector will contact the customer's contacts and dox them by sharing information about the debt.

d) The next threat will affect the workplace if you do not want to pay.

e) This process continues until the victim pays the debt. No matter who will be affected, even the bills will go to family contacts."

The differential association theory explains that evil actions do not result from parental inheritance, but the surrounding environment learns them. In the case of *Pinjol*, the actions they take are a methodology of learning from the environment. They study the characteristics of customers and find out what methods are most effective in collecting debts even though it makes customers depressed and contrary to morality.

In Sutherland's opinion, if criminal behaviour is something that individuals learn from the behaviour of a social relationship, sustainable traits and behaviour are the basis for what is learned.

The theory of crime prevention efforts explains that preventive action is divided into two parts of policy regulations: legal (penal) and non-penal methods.

Considering that the Personal Data Protection Law was still not active when writing this journal, the author argues that the PDP Law will also strengthen the legal umbrella in tackling the criminal act of doxing in Indonesia. The use of Article 65 of the PDP Law contains "Prohibition in the Use of Personal Data". The PDP Law was made to protect citizens' data when operating e-commerce.

As written in Article 4 § 3 regarding the general types of personal data: "*Full Name, Gender, Citizenship, Religion, Marital status, Personal Data that is combined to identify an individual".*

This data is commonly used in the 'Verification' stage of using financial apps.

Article 1 § 6 to 8 explains: "1) Personal Data Subject is an individual to whom Personal Data is attached; 2) Every person is an individual or corporation; 3) A corporation is an organized group of people and/or wealth, whether incorporated or unincorporated".

Continued in Article 2 of the PDP Law:

"1) This Law applies to every Person, Public Body, and International Organization that performs legal acts as regulated in this law:

a. That is located in the jurisdiction of the Republic of Indonesia; and

b. Outside the jurisdiction of the Republic of Indonesia: In the jurisdiction of the Republic of Indonesia and/or For Personal Data Subjects of Indonesian citizens outside the jurisdiction of the Republic of Indonesia.

2) This Law does not apply to the processing of Personal Data by natural persons in private or household activities".

This law protects the rights of citizens, corporations, and every group protected by the PDP law. However, a necessary explanation is listed in Article 2 § 2 regarding the inapplicability of this PDP Law.

The Personal Data Protection Law does not apply to issues in personal or household activities. Following the explanation of the PDP Law formulated in its formulation: "The formulation of rules on Personal Data Protection can be understood due to the need to protect individual rights in society in connection with processing Personal Data electronically and non-electronically using data processing devices. Adequate protection of Personal Data will be able to provide public confidence to provide Personal Data for various greater public interests without being misused or violating their rights. Thus, this regulation will balance the rights of individuals and communities whose interests are represented by the state. This Personal Data Protection regulation will greatly contribute to creating order and progress in the information society."

This explanation provides information that the PDP Law was deliberately made for the sake of the modernization process of society, which encouraged the use of electronic devices that can modernize life in society and the state. As described above, "Personal Data will be able to give the public confidence to provide Personal Data for various greater public interests without being misused or violating their rights". This context reflects that the government encourages and protects community activities using online services.

Based on the explanation above it is then corroborated by a further explanation in the PDP Law as follows: "To reduce overlapping provisions on Personal Data Protection, basically the provisions in this law are standards for Personal Data Protection in general, whether processed as a whole or by electronic and non-electronic means, where each sector can apply for Personal Data Protection according to the characteristics of the sector concerned. The regulation of Personal Data Protection aims to, among others, protect and guarantee the basic rights of citizens related to personal protection, guarantee the public to get services from Corporations, Public Bodies, International Organizations, and the Government, encourage the growth of the digital economy and the information and communication technology industry, and support the improvement of the competitiveness of the domestic industry."

It is clear that this PDP Law, in the future, will become a standardization in Personal Data Protection, which if in the future there is a conflict between ITE Law and PDP Law, then the PDP Law will be put forward first because it becomes the basis and standardization in Personal Data Protection and Consumer rights.

Thus, if a case of doxing occurs and the PDP Law is already active in the future, then the PDP Law is the primary one to use. Then, suppose there is no conflict in the legislation. In that case, the ITE Law will be side by side as a complement to the PDP Law by the explanation of the PDP Law in the "Transitional Provisions" Chapter listed in Article 75 of the PDP Law: "When this Law comes into force, Personal Data Controllers, Personal Data Processors, and other parties related to the processing of Personal Data must adjust to the provisions of Personal Data processing under this Law".

Furthermore, in tackling similar *Pinjol* cases, based on the theory of Crime Prevention Efforts

and non-penal policies that can be carried out in social defence actions, the government has made several arrests of illegal *Pinjol* elements. Most recently, due to *Pinjol*'s interest being too high, the OJK has been trying to make new regulations to curb Pinjol's high interest rates, to the point that customers cannot repay their loans because the interest never runs out.

Influencer Doxing & Cyber Bullying Cases. If we discussed cases between individuals and companies in the previous section, then this time, the case to be addressed is between individuals and individuals.

Vtuber Case. Back to clarify a little about what a Vtuber is. In the world of content creation, many people can become famous instantly. Those who have become well-known and influential are often called "Influencers".

Everyone considered an influencer is usually famous because of the content they bring to social media platforms such as YouTube, Twitch, Instagram, TikTok, and many others. Regarding live streaming or live broadcasting, content creators in these fields often refer to themselves as streamers whose daily lives are looking for profits by making live broadcasts on internet services using video-based social media.

Video-based social media, currently the most popular worldwide, is on two platforms. The first is YouTube, and the second is Twitch. For this writing, we will focus on the Youtube channel. Those who work in creating content on the YouTube channel are nicknamed Youtubers or people who make creations on the YouTube channel professionally.

On the YouTube channel, the creator's content is divided into two parts: the first is a Youtuber who makes video documentation, and then there are Youtubers who carry out their creative content activities by live streaming. The scope of live streaming is carried out on YouTube channels and then developed in various lines. There are live-streaming games, those that bring cooking content, and those that discuss sports impressions. All of that is done live on the YouTube channel.

Recently, around 2020, a group of YouTube streamers called themselves Vtubers. Vtuber means Virtual Youtuber, which means that they are influencers who use animated avatars, and their identities are biased in hiding their respective personal data. The purpose of these Vtubers working on YouTube varies and is similar to that of traditional Youtubers. However, what is unique to these Vtubers is that they wear animated characters that can move using a program embedded in a smartphone, a "face tracking program".

The use of animated characters played professionally by these Vtubers - each person makes their personality a marketing tool with a variety of uniqueness and unique voices owned by each member. The creation of this atmosphere is what supports these Vtubers in entertaining and marketing themselves to viewers of Vtuber content.

The character used as a Vtuber is a character in the form of two-dimensional animation, or what is referred to as "Live2D Animation Character". What does Live2D mean? The sentence means two-dimensional animation that can live in cyberspace because voice actors play it. The voice actor is called a "Vtuber", and the animated character is called a "Live2D Model".

Live2D characters are Vtubers' main asset in their online activities. Whether it is live streaming, creating content, or promoting the merchandise advertised by each cast. Thus, in the marketing and branding actions of Vtubers who are already famous and have become influencers, behind them, there are usually companies that become the umbrella for each Vtuber activist.

It costs a lot of money for a company to create a Live2D animated character that its voice actors will later use. Usually, one Live2D character can be worth hundreds or even hundreds of millions to produce a character that can move like a natural person. Usually, a Vtuber company agency can spend tens or even hundreds of millions to create a set of Vtuber streamer groups, which will become the main asset in running the company's economic turnover and attracting investors' attention to the Vtuber agency.

As discussed earlier, the selling point of a Vtuber is the voice and how interesting the voice actor plays the character. Therefore, every cast of Vtuber characters is very vulnerable to doxing. Just imagine if there were a Vtuber who had an exciting voice and character acting. Still, one day, someone shares the person's data and displays the natural face of the Vtuber's actor, and the Vtuber's appearance does not match his fans' expectations. Essentially, those who want to leak

the secrets of the character's voice actor to find out who is the actor behind their idol. What will happen to the Vtuber in the future? Can he maintain his current situation? In addition to being detrimental to the individual Vtuber, this action can undoubtedly hurt the agency that employs the Vtuber. The occurrence of doxing can potentially harm the condition of the agency company where the Vtuber works.

Kureiji Ollie Case Position. In a case that occurred in Indonesia. This incident happened some time ago and involved one of the largest Vtuber agencies in the world, Hololive ID. This agency is a subsidiary of Vtuber from Japan. The core company of Hololive is Cover Corp. This company houses Vtuber agencies such as Holostar (Male Vtuber), Hololive ID (Vtuber Branch based in Indonesia), Holo EN (International Branch), and many more. The history of Cover Corp is that it is a mobile science and technology company focused on creating software capable of tracing a person's face. Cover Corp has become a global entertainment enterprise as the company grows.

The case originated from the live-streaming video of one Hololive ID Vtuber named Kureiji Ollie. A zombie-themed Vtuber with a unique character design, like a female zombie with a teenage high school student background. Ollie is one of the Vtubers whose subscriber growth was growing fastest globally. Several internationally renowned influencers and Youtubers even highly idolize him because of his excellent English and communication skills when collaborating with many Youtubers, Vtubers, and influencers.

Figure 5 – Case excerpt from the Topic Area page (in Indonesian)

This made Ollie a crucial Vtuber asset for the Hololive ID agency at the time. Until recently, there was an unrecorded rule for Vtuber fans. This rule was "no individual is allowed to disseminate personal information or data of their favourite Vtuber member". Anyone with information about a Vtuber voice actor's private data is prohibited from sharing it.

Legally speaking, as long as it does not harm the parties involved, it is perfectly legal. This is referred to as "soft doxing" or mild doxing. Therefore, searching for information is taboo to find out who the actor behind Vtuber's voice actor is, and if they already know a lot of information about the Vtuber's identity, then this action is referred to as a "Rabbit Hole" or people who have fallen into the rabbit hole, usually those who have entered the realm, it will be challenging to get out.

The information holder of a Vtuber voice actor is very vulnerable in keeping the secret. If they are impatiently typing on social media, they could be doxed. However, as long as they are not triggered, usually the fans, they can keep the secret. However, this case occurred because the trigger for the information leak eventually leaked to social media. The beginning of this information leak came from one of the streams that Kureiji Ollie did when he had just received an award from the YouTube channel in the form of a "Golden Play Button". This award can be obtained if a person who works on YouTube can get 1 million subscribers. However, what triggered this case was the golden play button.

On the golden play button, there is a material that can reflect images like a mirror, and the unwanted incident at that time occurred, where the natural face of the cast of Kureiji Ollie, was reflected in the mirror part of the golden play button.

Figure 6 – Illustration when Ollie's face is reflected (in Indonesian)

After the incident, Ollie immediately stopped his broadcast and privatized his live broadcast video. However, when Ollie ended his live streaming on the social media channels Facebook and X (Twitter), it turned out that many people had provided and disseminated information on Ollie's face in the form of snippets of images taken unilaterally by Ollie's audience when the incident took place.

As a result of the incident, many blasphemed Ollie because the person behind the character Kureiji Ollie was not what they had imagined. The trigger for why many people blasphemed Ollie at that time was not because Ollie's face was exposed on the golden play button. Still, the incident after the tragedy of the spread of pieces of the natural face of the Kureiji Ollie cast spread on social media.

After the photo spread on social media, many netizens matched the data and information they collected when they went into the "Rabbit Hole". Discussions about the identity behind Ollie's character emerged, and people shared information on Discord, Facebook, and other social media channels.

Unconsciously, the cyberspace community at that time had committed the crime of doxing, which could be charged with the ITE Law regarding defamation and dissemination of electronic information and documents. In addition, they had also insulted someone's physique (Body Shaming). However, the basis of the ITE Law is a complaint offence, where the character Kureiji Ollie is unlikely to make a report to the authorities because he must report the case in real life and cannot be anonymous. If the case goes to court, then Ollie's name and identity will be revealed, and if this happens, the company and its Vtuber members will suffer even more significant losses.

Back to the case of Kureiji Ollie. After that incident, many people left Ollie because curiosity had disappeared from their minds. Ollie's viewership decreased until Ollie's subscriber growth was finally stuck at (1.31 Million) Subscribers. Due to the incident, the Hololive ID agency also suffered losses. The primary source of income for the Hololive agency was donations from viewers. Therefore, when the audience decreases, the donations received will also decrease.

But it doesn't end there. This case also affected other Vtuber Hololive members. Many people were also curious about who the actors behind the other members were, where the Vtuber character actors were also friends and coworkers of Kureiji Ollie.

The Kureiji Ollie case that went viral in the Vtuber community some time ago, as explained in the case above, the doxing actions taken by netizens in Ollie's case can be charged with ITE Law Article 27 § 3, which contains defamation. Indeed, in Ollie's case, it is not only Ollie who is harmed, but the Vtuber agency where Ollie works is also harmed.

Due to the ITE Law, which other people cannot represent in reporting it, the doxing committed by netizens cannot be prosecuted. Furthermore, can the PDP Law protect this in handling doxing cases against the background of leaking personal data of Vtuber members? However, a further question arises regarding whether this case can be reported. If actionable, who should be blamed in this doxing case?

Doxing & Cyber Bullying Case Study based on ITE Law & PDP. From a legal perspective, the Vtuber Kureiji Ollie case is rare in Indonesian legislation. The aspects inherent in this type of case are pretty abstract. Here is why this is the case:

1. Ollie's case involves the confidentiality of the reporter's identity. If the case is reported to the police, can the alias (Kureiji Ollie) still be used as the reporter's name?

2. If you cannot use an alias, can the reporter be represented on behalf of the company or the reporter's attorney?

3. If you can use an alias and the police start investigating, how do you identify a suspect who is also anonymous?

Based on the UPK theory, penal and non-penal policies are needed to tackle the criminal act of doxing Vtuber. In Ollie's case, the use of penal methods is as follows.

Based on the Criminal Procedure Code, it is clear that a person is not required to include the reporter's name and the suspect (according to the KTP). However, after making a report, whether verbally or in writing, the reporter must use his/her real name in signing the report, so it is an obligation to use the actual name when he/she wants to investigate the report [7]. Sometimes, one can use an alias if the reporter does not know the suspect's identity.

This can happen if the investigation clearly states that the suspect is anonymous. Therefore, the authorities must track and find out and collect

data on the suspect's identity. If, at the investigation level, the suspect's identity is still unknown, then the possibility of the case being processed legally can be reached. All of this goes back to the level of difficulty of the case that can be handled by the police [7]. However, let's look at the guidelines of the three ministerial agreements involving defamation. It must be the person concerned who can make a police report without being represented - because this offence is a complaint offence.

In terms of tracking people, currently, the Cyber Criminal Police Directorate must have specific methods to track suspects. Thus, in the case of Vtuber doxing, the only obstacle is whether or not the use of a pseudonym or alias is allowed in reporting it. Or can the report be represented by the company? So, if the doxer is a community, who is entitled to be rewarded as the perpetrator of the doxing crime? Those who deserve to be considered doxing suspects openly share the document with the public. So, if the source is one person, that person can be charged with anti-doxing. However, suppose the information has fallen into a community, and the community as a whole participates in spreading it. In that case, all community members who spread the information can also be charged with articles regarding disseminating personal data.

The use of non-punitive methods in the Vtuber doxing case can be done by educating the public about the doxing laws in the current ITE Law. As long as there are still people who do not know the context of the ITE Law, the criminal act of doxing will continue to occur and even develop.

As discussed earlier, it is not the bloodline that makes a person evil, but rather the environment in which they carry out their daily activities.

Analysis of the Kureiji Ollie case

In Ollie's case, the aggrieved subject here is like two sides of a coin: one is the Vtuber, and the other side is the Vtuber's agency. The suspect will be subject to civil articles if the reporting party is the company. Thus, the case can be processed legally.

The community that doxed Ollie was the first to communicate with each other about who the actor behind Ollie's voice actor was. The characteristics of people who are doxing in the realm of information dissemination and electronic documents are usually members of a community who often discuss these specific things. Finally, this incident occurs; according to Sutherland's statement, patterns of malicious behaviour are traits that individuals learn from the behaviour of a relationship between familiar social.

In Ollie's case, the only law that can be used is the ITE Law because what is attacked is privacy in the form of electronic documents. The use of the PDP Law as a legal umbrella in handling the Vtuber doxing case can be used if it fits the criteria of personal data in the PDP Law, which is divided into general and specific.

According to the PDP Law, article 4, paragraphs 2 and 3 explain:

"2) Specific personal data, as referred to in § 1, letter a, includes health data and information; biometric data; genetic data; criminal record; child data; personal financial data and/or other data based on the provisions of laws and regulations.

3). General Personal Data, as referred to in § 1 letter b, includes full name; gender; nationality; religion; marital status; Personal Data combined to identify an individual."

Based on the above criteria, the PDP Law can only be used when formal personal data is involved, while electronic documents such as photos and so on can only be charged with the ITE Law.

Data on Cybercrime Cases in Indonesia

The Substance of Law Enforcement Apparatus and Means. Law enforcement is an obligation for everyone living in Indonesia, requiring everyone to know all their rights and responsibilities. Regarding the issue of law enforcement in cybercrime in Indonesia, POLRI agencies are among those who handle cybercrime cases. In this case, applying the POLRI forensic laboratory as a support for scientific investigators in the Indonesian criminal justice system is needed.

Investigator Aspect. The presence of a 'Cyber Patrol' unit within the police shows the importance of specialized investigators in addressing cyberspace issues - skills in technology and information are needed to detect cybercrime. In this regard, police investigators play a significant role in cybercrime control efforts. The ability and quality of investigators to explore and master computer expertise must be adequate because it is a consideration in uncovering cybercrime cases reported by the public [8].

The obstacle to the quality of investigators appears to be the strength and capability of the POLRI cybercrime unit [8]. Investigators' ability to handle cyber cases must have skills in English, forensic computer skills, mobile forensic skills, and an understanding of cyber law. Each Polda should have an adequate quantity/number of investigators so that the cyber unit in each Polda can overcome the problems present in proportion to the number of reports or complaints coming from the public. Of course, in this case, the impact can strengthen and accelerate the service and handling of cybercrime by the police.

For this reason, POLRI annually recruits investigators with abilities that match the skills needed. Undergraduate schools are open every year to fill the needs of POLRI in handling cyber cases and other fields. The cybercrime unit currently requires a lot of personnel, so all police chiefs have a cyber unit that can hold public reports based on the report date, not based on the priority of which problems have more losses [8].

Aspects of Evidence. Electronic systems or data connected to the internet are the target media for cybercrime. Because of the many computer café facilities (internet cafes) and other public facilities that can be used for free, presenting evidence in handling cybercrime cases differs from proving in ordinary crime cases. The obstacles that cyber investigators must face start from digital evidence because of the ease of destroying evidence. In fact, with one press, the evidence can be lost. This is evidence of cybercrime - if not handled quickly, accurately, professionally and effectively, public facilities can commit cybercrime in such a short time. The explanation is as follows [8].

a. Digital Evidence is Easily Disposed of. Evidence in cybercrime is usually digital or data-based, as cybercrime targets electronic systems based on data and information. In practice, such as in cases of hacking, online fraud, doxing and defamation, or other issues, the instruments used are computer-based and connected to the internet system. The ease of deleting data and hiding evidence makes the collection of evidence in cybercrime more difficult than in conventional crime.

b. Use of Public Facilities in Committing Cybercrime. In cybercrime, many perpetrators use public facilities to carry out their actions, such as using electronic media connected to public Internet networks, Internet Café facilities, or Internet cafes. In investigating cybercrimes, police use computers to track the perpetrators through websites or IP addresses where the perpetrators use their electronic devices to surf the internet. This has become a common practice, although sometimes it is a challenge.

c. Witness locations that are not the same as the victim and perpetrator. Information provided by witnesses is a determining factor in the legal process, especially in cyber cases, including evidence, is a determining part. Cyber cases are quite different from criminal cases in general; therefore, cybercrime is included in particular crimes requiring special tools such as computers. In cyber cases, witnesses are not always in a position or location close to the perpetrator or victim - witnesses and victims in cyber cases have such an important role. In practice, there are rarely witnesses in cyber cases because the victim witness may be outside the region or the country. These difficulties make investigators work harder because examining witnesses and filing investigation results must also be done on witnesses [8].

In cyber cases, the public prosecutor will not accept the case file if it is not complete with the minutes of the witness examination. Sworn testimonies must accompany victim and witness testimonies because most witnesses usually do not attend the trial due to the remoteness of the location where they live - this can lead to incomplete legal evidence, in the condition of an incomplete case file, when submitted to the court, it can result in a lack of evidence and the defendant is at risk of being acquitted. The police, in this case, cyber investigators, can also experience similar difficulties when processing cyber criminal cases. Obstacles can be obtained due to a lack of evidence, but if lucky, the police can conduct a sting operation when the cyber perpetrator is arrested while acting. The perpetrator's presence at the scene can shorten the evidence collection directly; the officer can simultaneously secure evidence, and thus, witnesses are not needed in these conditions [8].

Support Facilities. Facilities that can assist police performance in handling cyber cases are needed, such as the presence of a computer forensics laboratory that is intended to reveal digital data and record and store evidence in the form of soft copies, such as images, sound, video, programs, html, and so on. Computer forensics in the cyber unit within POLRI, or digital forensics, is to collect and evaluate digital evidence and various ob-

jective facts after an incident or violation of information system security occurs. The facts will then be used as evidence in court [8]. Investigators can use internet forensic data to determine who sent the email, when it was sent, and where the sender is located based on the sender's server.

POLRI can also identify website visitors by looking at the IP addresses of website users, the electronic devices they use, their movements and activities, and their steps in using the website [8].

The following is a table of Digital Forensic facilities owned by POLRI based on the regions with Digital Laboratories" [8].

Table 1 – List of POLDAs that have a Digital Forensic Laboratory

No	Police Name	Information	Type / Classification
1	METROJAYA	Having a digital forensic laboratory helps POLDAs that do not yet have one.	A+ (A Specific) ISO 17025
2	SUMSEL	Helping police stations around the Sumatra region.	A
3	BALI	One of the police stations that has an accredited Digital Forensic Laboratory.	A
4	NTB	POLDAs that have an accredited Digital Forensic Laboratory	A
5	PAPUA	Police who received LABDIGFOR equipment grants	A
6	SUMUT	Police who received LABDIGFOR equipment grants	A
7	JATIM	Police who received LABDIGFOR equipment grants	A
8	JABAR	Police who received LABDIGFOR equipment grants	A
9	SULAWESI TENGAH	Police who received LABDIGFOR equipment grants	A
10	KALIMANTAN TIMUR	Police who received LABDIGFOR equipment grants	A
11	JAWA TENGAH	Police who received a LABDIGFOR equipment grant	A

From the table above, we can measure the ability of each POLDA in Indonesia to handle cybercrime cases, especially cases that require special handling, by using a digital forensic laboratory in the process of investigating cybercrime. Currently, ten POLDAs have Digital Forensic Laboratories and other laboratories will continue to be built in various parts of Indonesia.

In addition to the digital forensic laboratory owned by POLRI investigators in investigating cybercrime, currently, investigators also have facilities to deal with cyber cases, such as the Cybercrime Investigation Satellite Office (CCISO) and Strategic Information and Tactical Operation Center (SITOIC), which include the following:

"A. Cybercrime Investigation Satellite Office (CCISO) laboratory consisting of a Computer Forensics Laboratory; Mobile Phone Forensics Laboratory; Forensic Audio Video Laboratory.

B. Strategic Information and Tactical Operation Center (STOIC) Laboratory consists of Analysis Communication Laboratory; Financial Analysis Laboratory; Command Center Laboratory".

Other supporting equipment police investigators use include a mobile direction finder, Cellebrite UFED Touch, check post, CDR, monitoring centre / social media monitoring, and so on. These supporting tools and their laboratories are infrastructure facilities that require accreditation to examine digital evidence.

Unfortunately, not all regional POLRI cyber units have this equipment. Each POLDA must cooperate with POLDAs with more complete equipment. It is hoped that in the future, POLRI will have the infrastructure of cyber units in all POLDAs for smoothness in taking action against cybercrimes so as not to accumulate in one police station or even be transferred to POLRI Headquarters.

Cyber Case Data Report for the Last 3 Years. Based on data obtained by the author from DITTIPIDSIBER BARESKRIM POLRI, based on cases of threats made by debt collectors to terrorize customers in the form of threats through fictitious Go-food orders or threats to spread their data, the following are the data results:

Table 2 – Cyber Case Data Report for the Last 3 Years

Period of the year	Threatening
2020	36
2021	131
2022	219

The table above shows that the number of threatening cases increases yearly. In handling cybercrime cases, the following is the number of cyber cases based on data obtained from DITTIPIDSIBER BARESKRIM POLRI.

Based on the increase in case settlement in the table above, it can be said that the number of cybercrimes in Indonesia fluctuates every year. The table above shows an increase in the number of cases resolved, which shows the quality of investigators who solve cases. The results from Table 3 show the percentage of case completion.

Table 3 – Number of Case Increase

Period of the year	CT	CC
2020	4790	1283
2021	3270	1780
2022	4860	2720

Data on cybercrime that has occurred in recent years, in the case of:

Table 4 – Data on cybercrime

Case	2022	2021	2020
a. Online gambling	322	54	82
b. Online-based fraud	1.322	864	1.319
c. Extortion	42	14	37
d. Threatening	219	131	36

Table 5 – Percentage of resolved, unresolved, and in-process cases of Cyber TP Case database for 2022

Number of Crimes (CT)	Number of Crime Settlements (CC)	%
4860	2720	55.97

It should be understood that there are no unresolved cases in case of resolution, only crime total (CT) and crime clearance (CC) because unresolved cases = are still in the investigation process.

Table 6 – The level of cyber case handling in Indonesia, whether it is getting better or worse

Period of the year	CT	CC	Percentage
2020	4790	1283	26.78
2021	3270	1780	54.43
2022	4860	2720	55.97

Based on the increase in case resolution in the table above, DITTIPIDSIBER BARESKRIM POLRI said that handling cybercrime cases in Indonesia is improving yearly.

The results of interviews with resource persons provide insight into eradicating cybercrime in Indonesia. In the case of spreading personal data, *Pinjol* cases involving acts of threatening through fictitious orders and threatening the spread of personal data are increasing every year. However, the increase in cyber instances does not mean that law enforcement in Indonesia is weakening. Still, the table above illustrates how vigorous law enforcement has been in recent years.

If a crime increases, then we must also look at how successful the number of cases resolved, for example, cyber cases that occurred in 2022, where there were around 4860 (four thousand eight hundred and sixty) cases recorded in the total crime in the cyber scope that occurred in Indonesia. However, the number of settlements also reached 2720 cases that law enforcement officials successfully resolved. This number is based on the opinion of the source that in 2022, the success rate of the police in cracking down on cybercrime amounted to 55.97%. What causes the crime rate in the cyber sphere to increase? Does not the success in solving the case mean that the number of people who want to commit similar crimes will decrease? According to differential association theory, the environment triggers people to commit crimes. This agrees with what the informant said.

The cause of people committing cyber offences, which is the biggest trigger in cybercrime, according to the source, "from the cases that have been handled to date, the majority of the motivation of cyber criminals is to gain profit in the form of money / gain personal wealth; and a small part because of a sense of revenge/disappointment / want to get recognition from certain communities." When viewed from the ITE and PDP Law, the protection provided by the two laws is very targeted in tackling criminal acts related to a person's data. The ITE Law pro-

tects a person's rights from being misused, and the PDP Law protects personal data from being spread outside for interests the data owner disapproves of. The grudge that a person feels can make him darken his eyes and do things not allowed by law.

Based on the interview results, a report from the National Cyber Security Index (NCSI) provides a record of the cybersecurity index score in Indonesia of 38.96 points out of 100. This occurred in 2022. This figure makes Indonesia ranked third lowest among the G20 countries. Indonesia is ranked 83rd out of 160 countries globally in the report's list. This picture provides information if the law applied in Indonesia, in this case, the ITE Law, which is currently still actively used, can overcome cybercrime, with the hope that when the PDP Law has been implemented in Indonesia, the lift will further decrease and make Indonesia safe from cybercrime.

Cybercrime is a particular crime, so special competence is required to handle these cases. In preventing cybercrime, the ITE Law and PDP act as a legal umbrella to deter people from violating them. In terms of preventing and taking action directly, according to the resource person, there are two ways that the police can do, in this case:

1) Repressively, where the police enforce the law or handle cases based on LP or report letters to suppress criminal acts.

2) Preventively, POLRI conducts prevention campaigns through educational efforts through online and offline media, counselling, seminars, coaching, and so on by functions other than detection.

The following question is, what happens if someone hides their identity or remains anonymous? The police have their undisclosed methods to handle such situations. Additionally, in the case of Vtubers, is it permissible for the reporter to have legal representation or for the company to create an LP, with the victim's permission, according to the ITE Law and the Criminal Procedure Code? The speaker suggested that based on the three Ministers' agreement guidelines on defamation cases, the individual involved must file a police report without legal representation, as it is connected to the offence of complaint.

The Electronic Information and Transaction Law and the Personal Data Protection Law are regulations created to prevent individuals from engaging in ITE and PDP crimes. However, the occurrence of these crimes can vary due to factors such as economic conditions, resentment, community environment, low education levels, and more. Therefore, the ITE and PDP Laws aim to ensure the peace of Indonesian people while using social media and browsing the internet.

CONCLUSIONS

The comparison between the Republic of Indonesia ITE Law Number 19 of 2016 and Personal Data Protection Law Number 27 of 2022, in response to doxing *Pinjol* and cyberbullying, has similarities and differences. The similarity between the two laws is to protect a person's right to privacy against doxing that can occur at any time. The difference between the two laws is that if the ITE law protects electronic documents such as photos, sounds, and so on by the explanation of the ITE Law, the discussion of the Personal Data Protection Law explains that what is protected in this law is personal data in the form of addresses, medical history, debts, marital status, and so on concerned by the explanation of the PDP Law. Furthermore, if the suspect is anonymous, the authorities will track the person with all the capabilities and technology owned by the authorized agency until it is known who is behind the anonymous account and to get the appropriate punishment. Conclusion The current legal position of doxing victims, with ITE Law No19 of 2016, is beneficial and can provide people with security and comfort from doxing attacks. The issuance of the Personal Data Protection law is a complement to the ITE Law when the PDP Law is active, so, later, if there are cases related to doxing or outside of it involving the ITE Law and PDP, then, in the author's opinion, the ITE Law and PDP Law will be sustainable and complementary, as long as the existing articles do not conflict with the PDP Law. The presence of laws that protect against doxing attacks has so far been able to tackle cybercrime and protect the public from these crimes. Thus, the presence of the ITE Law is complementary in preserving a person's right to ownership of electronic document data and the presence of the PDP Law, which focuses on personal data. The two laws look strong and complement each other if the other law cannot handle existing cybercrime cases.

People want their identities to be kept secret for many reasons. In the case of criminal doxing, it will be tough to be prosecuted if the person's sta-

tus is anonymous because to make a report to the authorities requires real identity such as name, address, and signature, all of which require factual identity and cannot be anonymous. If an anonymous person wants to make a report, they must provide data about their real identity (KTP identity) in the form of signatures and so on. If that is done, then the anonymous identity is threatened there. Therefore, it will be difficult for a Vtuber / Anonymous who wants to report a doxing case to the authorities. Thus, one of the suggestions that the author can convey is to allow Anonymous to permit people he trusts to submit reports using a power of attorney so that the police can accept reports regarding doxing crimes aimed at the person concerned. UU ITE and UU PDP are laws that protect the right to personal data owned by every citizen. As explained above, people want to keep their identities a secret for many reasons. It could be that someone feels that if he later reports his complaint to the police, the reported suspect will commit a revenge crime. Or, like the Vtuber case above, keeping the identity secret is an absolute thing to do in the entertainment business. In the author's opinion, if the identity of the reporter is needed, then only the recipient of the report is obliged to know the identity of the person to clarify the credibility of the reporter so that if it is true that the case happened to him, then the investigation can be continued and continued in the investigation, after that, all the contents of the report format will contain alias data from the original person behind the doxing case reporter. The police must be able to protect the rights of citizens so that they can feel safe and comfortable reporting anonymous cases.

For this reason, the author argues that a new law should be made that protects the rights of citizens whose identity confidentiality is considered. In protecting cybercrime cases, especially in doxing instances, the author feels that the ITE and PDP laws are good enough to tackle and take action against cybercrime in Indonesia. The authorities also know their competence and have established human resources to control and reduce the number of cybercrime crimes worldwide. The community's sensitivity to criminality in the cybercriminal world must be considered here. Examples include piracy, online gambling, pornography, doxing, cyberbullying, internet terror, and so on. Currently, legal control can be relied upon, but people still do not understand that the components of their lives could be part of cybercrime.

For this reason, the author suggests socializing all types of activities considered cybercrimes to the Indonesian people. It can be through social media, podcasts, or even television channel broadcasts so that people know if what they are doing violates the law and does not approach it. Following the Differential Association theory, crime does not grow from parents but is obtained from the environment that is learned. Breaking the chain of crime is one of the best non-penal methods of tackling crime.

REFERENCES

1. Dian, U., Bagos, B., Fajar, F., & Noerma, K. (2024). Perlindungan Hukum Terhadap Kekayaan Intelektual Dalam Era Digital Di Indonesia [Legal Protection of Intellectual Property in the Digital Age in Indonesia]. *TERANG, 1*(1).

2. Putra, Pratama, A., & Pradnya, Y. D. G. (2022). Analyzing Trials Through Online Media During The Covid-19 Pandemic in Indonesia. Policy, Law, Notary and Regulatory Issues (POLRI), 1(1), 8–15. doi: 10.55047/polri.v1i1.22

3. Halif, H., Azizah, A., & Ratrini, P. D. (2023). Regulating Doxing and Personal Data Dissemination in Indonesia. *Jurnal Kajian Pembaruan Hukum, 3*(1), 61. doi: 10.19184/jkph.v3i1.33938

4. BBC News Indonesia. (2023, September 22). *Pinjol AdaKami diduga teror nasabah karena terlambat bayar cicilan - "Saya dibilang anak haram, orangtua dimaki dengan kasar"* [Pinjol AdaKami allegedly terrorises customers for late repayments - 'I was called an illegitimate child, my parents were abused']. Retrieved from https://www.bbc.com/indonesia/articles/cz986dygeeyo (in Indonesian).

5. Prihatini, Z., & Maullana, I. (2022, November 11). *Sidang Kasus Pria Ancam Korban Pinjol Digelar di PN Jakarta Utara* [Trial of man who threatened loan shark victim held at North Jakarta District

Court]. Retrieved from https://megapolitan.kompas.com/read/2022/11/18/14223061/sidang-kasus-pria-ancam-korban-pinjol-digelar-di-pn-jakarta-utara#google_vignette (in Indonesian).

6. Raharjo, A. (2022, June 15). *Lima Karyawan Pinjol Ditangkap Atas Dugaan Penyebaran Data* [Five loan shark employees arrested on suspicion of spreading data]. Retrieved from https://www.antaranews.com/berita/2941341/lima-karyawan-pinjol-ditangkap-polisi-atas-dugaan-penyebaran-data (in Indonesian).

7. Jayanti, D. (2022, December 13). *Jerat Hukum Mencatut Nama Orang Lain dalam Dokumen* [The Legal Snares of Using Other People's Names in Documents]. Retrieved from https://www.hukumonline.com/klinik/a/jerat-hukum-mencatut-nama-orang-lain-dalam-dokumen-lt569eee7a6efaa/ (in Indonesian).

8. Sarkar, G., & Shukla, S. K. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology, 2*, 100034. doi: 10.1016/j.jeconc.2023.100034