

## Criminal Liability of Fintech Company for Spreading Personal Data

M. Imam Rosada

Universitas Islam Bandung, Indonesia

Correspondence: imamrosada99@gmail.com

Artikel	Abstract
<p><b>Keywords:</b> law enforcement; fintech and dissemination of personal data</p> <p><b>Artikel History:</b> Submission: 2023-02-13 Accepted: 2023-04-29 Published: 2023-04-29</p> <p><b>DOI:</b> 10.30999/jph.v5i2.2493</p>	<p>Globally, information technology has altered human behavior and way of life. The world has no borders now that information technology has advanced. Information technology has now evolved into a double-edged sword because, in addition to advancing human civilization and welfare, it also provides effective means for criminals to commit crimes, such as the dissemination of personal data by fintech (pinjol). As a result, laws that punish online lenders (pinjol) who spread personal data are now necessary. The purpose of this study is to identify criminal liability for the fintech (pinjol) conduct of disclosing personal information and to identify law enforcement. An strategy that is normatively legal is used in this study. In addition, this study employs primary law, secondary legal materials, and tertiary legal materials in a descriptive-analytical manner. The descriptive-analytical research methodology utilized in this study describes the applicable laws and rules connected to legal theories and the practice of enforcing positive legislation. According to the criminal liability view of criminal responsibility considered from the repercussions it can do harm to others, both physically and mentally, fintech (pinjol) is responsible for the act of disclosing personal data. It is reasonable that the act of disseminating personal data might be subject to the threat of penalty as defined in the ITE Constitution and the Dissemination of Personal Data Law since those who commit crimes are considered to have done so intentionally (Opzet) with a goal. Law enforcement's ability to prevent the dissemination of personal data is currently limited and challenging due to the difficulty of enforcing the legality standard. As a result, the ratification of the Dissemination of Personal Data Regulation was a breath of fresh air for law enforcement.</p>
Abstrak	
<p><b>Kata Kunci:</b> penegakan hukum, fintech, penyebaran data pribadi</p>	<p>Teknologi informasi telah mengubah perilaku dan pola hidup masyarakat secara global. Perkembangan teknologi informasi telah menyebabkan dunia menjadi tanpa batas (<i>borderless</i>). Teknologi informasi saat ini telah menjadi pedang bermata dua, karena selain memberikan kontribusi bagi peningkatan kesejahteraan, kemajuan dalam peradaban manusia, sekaligus menjadi sarana efektif untuk para pelaku melakukan tindak pidana, seperti Penyebaran data pribadi yang dilakukan oleh</p>

perusahaan *fintech* (pinjol), sehingga perlunya penegakan hukum terhadap pelaku pinjaman online (pinjol) yang menyebarkan data pribadi. Penelitian ini bertujuan Untuk mengetahui tanggung jawab pidana atas tindakan penyebaran data pribadi yang dilakukan oleh perusahaan *fintech* (pinjol) serta Untuk mengetahui penegakan hukumnya. Penelitian ini menggunakan metode pendekatan yuridis normatif, Penelitian ini juga dilakukan dengan cara deskriptif analitis yaitu menggunakan hukum primer, bahan hukum sekunder dan bahan hukum tersier. Metode yang digunakan dalam penelitian ini adalah bersifat deskriptif analitis, yaitu menggambarkan peraturan perundang-undangan yang berlaku dikaitkan dengan teori-teori hukum dan praktek pelaksanaan hukum positif. Tanggung jawab pidana atas tindakan penyebaran data pribadi yang dilakukan oleh perusahaan *fintech* (Pinjol) dalam pandangan pertanggungjawaban pidana dilihat dari akibat yang ditimbulkannya dapat merugikan orang lain, baik secara lahir maupun secara batin. Pelaku tindak pidana yang menyebarkan data pribadi dikategorikan sebagai Kesengajaan (Opzet) yang bersifat tujuan, sehingga patutlah tindakan penyebaran data pribadi dapat dikenakan ancaman hukuman sebagaimana diatur dalam UUD ITE maupun UU PDP. Penegakan hukumnya terhadap tindakan penyebaran data pribadi sampai saat ini sangatlah minim serta sulit dilakukan, asas legalitas menjadi permasalahan dalam penegakan hukumnya, sehingga setelah disahkannya UU PDP menjadi angin segar bagi para penegak hukum yang karenanya penegakan hukum atas penyebaran data pribadi memiliki dasar hukum yang kuat.

© 2023 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).

## Introduction

The development of Information and Communication Technology (ICT) has brought significant changes in many aspects of life, even its presence has brought changes in the periodisation of the history of human civilisation. Postindustrial society has emerged because of the shift in technology that has become the mainstay of human life. The change from mechanisation to massive digitalisation. This is what is called the epochal shift in human civilisation..<sup>1</sup>

Information technology has changed the behaviour and lifestyle of people globally. The development of information technology has caused the world to become borderless and caused significant social, cultural, economic and law enforcement patterns to change rapidly. Technological developments, starting from the first wave to the most recent wave, are always followed by supporting legal instruments. Moreover, information technology has now become a double-edged sword, because in addition to contributing to the improvement of welfare,

---

<sup>1</sup> [https://www.bphn.go.id/data/documents/pphn\\_bid\\_informasi\\_dan\\_teknologi.pdf](https://www.bphn.go.id/data/documents/pphn_bid_informasi_dan_teknologi.pdf) diakses pada tanggal 11 Desember 2020, Pukul. 20:48 WIB

progress in human civilisation, it is also an effective means for perpetrators to commit unlawful acts.<sup>2</sup>

The presence of globalisation in this millennium era has had a major impact on all sectors of human life, one of which is technology and the internet. Technology and the internet have a huge role in supporting all activities of human life. The huge utilisation of digital technology in Indonesia certainly has an impact on several sectors, one of which is the business sector or business industry. The rapid development of technology and the internet has not only penetrated the trade industry, but also the Indonesian financial industry. This is characterised by the presence of financial technology (fintech).<sup>3</sup>

Fintech comes from the term financial technology. According to The National Digital Research Centre (NDRC), in Dublin, Ireland, defines fintech as "innovation in financial services" which is an innovation in the financial sector that is touched by modern technology. Financial transactions through fintech include payments, investments, loans, transfers, financial planning and comparing financial products.<sup>4</sup> Fintech which is one of the technological advances that is in great demand by the public at this time with the existence of Fintech engaged in financial services the community can easily carry out transactions, lending and borrowing, instalments and so on without any space and time limits, Fintech which provides various kinds of financial services using the "peer to peer lending" system, namely the implementation of a lending and borrowing agreement that brings together lenders and loan recipients through the internet network.<sup>5</sup>

The presence of peer to peer lending systems in Indonesia can certainly have a positive impact, namely some residents who live in remote areas or remote areas can easily carry out the process of borrowing money.<sup>6</sup> The implementation of granting credit can be carried out quickly, besides that lending can be given without collateral, unlike the case with banks which juridically state that KTA is impossible, and even though banks provide credit without special collateral.<sup>7</sup>

However, on the other hand, there is also a negative impact of online transactions without collateral, because borrowers and lenders do not meet face-to-face or interact directly, it is very easy to commit crimes such as manipulation

---

<sup>2</sup> *Ibid*

<sup>3</sup> Ernama, Budiharto, Hendro S., "Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology (Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016)," *Diponegoro Law Journal*, Vol. 6, No.3, (2017), hlm. 1-2

<sup>4</sup> *Ibid.*, hlm.2

<sup>5</sup> Alfhica Rezita Sari, "Perlindungan Hukum Bagi Pemberi Pinjaman Dalam Penyelenggaraan Financial Technology Berbasis Peer To Peer Lending Di Indonesia", *Skripsi Program Studi (S1) Ilmu Hukum Fakultas Hukum Universitas Islam Indonesia*, Yogyakarta, 2018, hlm. 97.

<sup>6</sup> *Ibid.*

<sup>7</sup> Djoni S. Gozali dan Rachmadi Usman, *Hukum Perbankan, cet. II*, Sinar Grafika, Jakarta, 2012, hlm. 286.

of information and the risk of borrowers' personal data being vulnerable to being spread by lenders. Therefore, the right to information with rules that can protect the right to information in electronic transaction-based transactions is important so that people get legal protection.

Fintech engaged in financial services (Online lending (Pinjol)) does make it easier for people to make transactions anywhere and anytime but Fintech engaged in Pinjol financial services can also have negative consequences, one of which is the dissemination of personal data by unscrupulous Fintech Pinjol against people who cannot pay for loans made, although many people have been harmed by data disseminated by unscrupulous Fintech, namely perpetrators who disseminate personal data, but the prosecution of these individuals is suspected that many have not yet reached the realm of law.

The incident was caused by several factors, one of which was the victims who were reluctant to report to the authorities or to law enforcement due to the psychological pressure experienced by the victims as a result of the dissemination of personal data, Andi Hamzah said that "Law is the overall rule of behaviour that applies in a common life, which can be enforced with a sanction. The implementation of the law can take place formally and peacefully but it can also occur because violations of the law must be enforced".<sup>8</sup>

The rise of Pinjol cases in Indonesia, especially in the city of Bandung since 2018, 2019 to 2020, has claimed many victims, following the data that the author obtained as follows:

**Table 1.1**  
**Number of Online Loan Victim Reports (Pinjol) Received by the Bandung City Anti-Vendor Task Force**

Tahun	2018	2019	2020	2021
<b>Advokasi</b>	134	130	86	124
<b>Reject</b>	12	44	20	24
<b>Partner Disposition</b>	3	18	10	11
<b>Independent Settlement</b>	924	1777	2403	3051
	<b>1171</b>	<b>2030</b>	<b>2519</b>	<b>3210</b>
<b>TOTAL</b>			<b>8930</b>	

Source: *Satgas Anti Rentenir Kota Bandung*

The data above is data on victims of pinjol in Indonesia who have consulted the Bandung city anti loan shark task force online via whatsapp and the people of Bandung City who request legal protection directly. The amount of data above is the number of cases from 2018 to 2021, the data above is always increasing every year, so it is necessary to enforce the law more strictly against

<sup>8</sup> Andi Hamzah, *Hukum Acara Pidana Indonesia*, Saptartha Jaya, Jakarta, 1996. hlm.30

pinjol perpetrators who spread personal data, starting from the case data above, it can be understood that the law should be a shield to protect the public from criminal acts committed by criminals so that every year the crime rate does not continue to increase;

Based on the problems arising in Fintech law enforcement described above, the author is interested in examining in more detail the criminal liability of fintech companies for the dissemination of personal data. In addition, it is also necessary to know the law enforcement against the perpetrators of the spread of personal data. The number of people who are victims of the spread of personal data raises problems that must be discussed in more depth, especially in tackling and prosecuting the perpetrators of the spread of personal data, so as to further reduce the number of victims of the spread of personal data among the community, especially in Bandung.

Previous research conducted by Rama Putra Perdana and Sri Ratna Sumirna (2021) in their research entitled "Creditor Responsibility for the Dissemination of Customer Data in Online Loans (Fintech) reviewed from Book III of the Civil Code in connection with Law Number 19 of 2016 concerning Electronic Information and Transactions". This type of research is descriptive research, using a qualitative approach method.

The equation of previous research with this research is that the objects studied are both the dissemination of personal data. The type and method of research approach used both use qualitative descriptive methods; While the difference between previous research and this study is that the subject in previous studies focused more on the perpetrators who spread personal data, namely third parties, while in this study it focuses more on the responsibility of Fintech companies for the act of spreading personal data. The previous research material did not use the data of the victim whose personal data was disseminated but only used library materials and related laws and regulations, while in this study it used it. Previous research conducted by Wening Novridasati (2020) in her research entitled "Criminal Liability of Illegal Fintech Desk Collectors and Protection of Victims". This type of research is descriptive research, using a qualitative approach method. The equation of previous research with this research is that the objects studied are both the dissemination of personal data. The type and method of research approach used both use qualitative descriptive methods;

The novelty of this research is that it focuses directly on the liability of legal Fintech companies for the dissemination of personal data. The previous research material only used data from one of the victim reports that shared personal data, while in this study it used data on the number of victims whose personal data was shared by Fintech companies. The object of previous research to illegal Fintech while in this study, the object of research is legal Fintech.

## **Research Methods**

The author uses the normative juridical method in this research, namely looking at the rules relating to the dissemination of personal data on social media as regulated in Law Number 19 of 2016 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning Personal Data Protection using primary and secondary data which are analysed qualitatively. To complete this research data, the author conducts literature studies as well as field studies to obtain answers to be analysed with theories relevant to the author's research in order to obtain the expected research results.

## **Results and Discussion**

### **Criminal Liability of Fintech Company for Sharing Personal Data**

Criminal liability means that every person who violates the law, as defined by the law, should be held accountable for the act in proportion to his guilt; in other words, a person who commits a crime will be held accountable for the act with punishment if he makes a mistake. A person makes a mistake if, at the time of the act, society exhibits a normative view of the mistake that has been committed.<sup>9</sup>

Criminal responsibility refers to behavior that violates the law as well as moral principles or standards of decency that a community or some segments of society have established. This is done in order to satisfy a feeling of justice and acquire criminal responsibility.<sup>10</sup> Determine if a suspect or defendant is accountable for a criminal offense by looking at their criminal responsibility. To put it another way, criminal responsibility is a factor in deciding whether a defendant is found guilty or innocent.

According to Roeslan Saleh, the continuation of the objective reproach present in the illegal act and the subjective qualification to face punishment for his conduct constitute criminal culpability.<sup>11</sup> What is meant by "objective reproach" is a person's commission of an unlawful conduct; the unlawful act in question is one that is against or forbidden by law, both formal law and material law. The individual who does the unlawful or illegal act is referred to as the subject of the subjective reproach, or it might be claimed that the subject of the subjective reproach is the subject of the unlawful or illegal act.

The basis for the existence of a criminal offence is the principle of legality, while the basis for the punishment of the perpetrator is the principle of guilt. This shows that the perpetrator of a criminal offence will only be punished if he/she is guilty of committing the criminal offence. In order to be held criminally

---

<sup>9</sup> Moeljatno, *Perbuatan Pidana dan Pertanggungjawaban Dalam Hukum Pidana*, Bina Aksara, Jakarta, 1983, hlm. 41.

<sup>10</sup> Hanafi, Mahrus, *Sistem Pertanggungjawaban Pidana, Cetakan pertama*, Rajawali Pers, Jakarta, 2015, hlm. 16

<sup>11</sup> Roeslan saleh, *Pikiran-Pikiran Tentang Pertanggung Jawaban Pidana, Cetakan Pertama*, Ghalia Indonesia, Jakarta, 1982, hlm. 33

responsible, an act must contain an element of fault, of which there are two types, namely intent (*opzet*) and negligence (*culpa*).<sup>12</sup>

The ability to be responsible is the basis for determining the punishment of the perpetrator of a criminal offence. This ability to be responsible must be proven by the judge, because if a person is proven not to have the ability to be responsible, this is the basis for not being held responsible for a criminal act. This means that a criminal act cannot be convicted or an incident of a criminal offence. The Criminal Code does not regulate the ability to be held responsible, but what is regulated in the Criminal Code is those who do not have the ability to be held responsible, such as Article 44 of the Criminal Code which regulates the opposite of the ability to be held responsible.

The dissemination of personal data carried out by fintech companies or called Pinjol when viewed from the theory of criminal liability can be categorised as an act that causes a negative impact on the interests of others, before the enactment of the PDP Law the actions taken by pinjol were difficult to reach by law, meaning that the act of dissemination carried out was difficult to prevent by law enforcement so that it had a negative impact on victims whose personal data was disseminated through information technology (online media).

The development of technology in everyday life can be felt in various activities, especially in a Covid 19 pandemic situation that cannot be separated from technology, so legal protection of personal data in the digital world is very important because since the Covid 19 pandemic the use of electronic documents and internet networks has increased and almost everyone who works, studies, transacts and so on is done at home using the internet network.<sup>13</sup>

What is meant by "objective reproach" is a person's commission of an unlawful conduct; the unlawful act in question is one that is against or forbidden by law, both formal law and material law. The individual who does the unlawful or illegal act is referred to as the subject of the subjective reproach, or it might be claimed that the subject of the subjective reproach is the subject of the unlawful or illegal act.<sup>14</sup>

In an article titled "The Right to Privacy" or "The Right Not to Be Disturbed" published in the Harvard University Law School scientific journal, Warren and Brandheis introduced the idea of privacy for the first time. According to Warren and Brandheis, as technology developed and advanced, the public became more aware of a person's right to enjoy life.<sup>15</sup>

---

<sup>12</sup> Moeljatno, *Perbuatan Pidana dan Pertanggungjawaban Dalam Hukum Pidana*, Bina Aksara, Jakarta, 1983, hlm. 46.

<sup>13</sup> Sahat Maruli Tua Situmeang, Penyalahgunaan Data Pribadi sebagai bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber, *Jurnal Sasi*, Volume 27 Nomor 1, Januari-Maret 2021, hlm. 38

<sup>14</sup> *Ibid*,

<sup>15</sup> Latumahina, RE, "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya", *Jurnal Gema Aktualita*, Vol.3, No. 2, 2014, hlm. 14-25

One of everyone's fundamental rights is the one to privacy. Every person has a right to dignity, and that dignity must be upheld. Personal information includes a person's name, age, gender, education, occupation, address, and place in the family.<sup>16</sup> Everyone owns sensitive personal information. A person's right to privacy, which includes personal data, must be respected in all spheres of life.

The idea of personal data protection emphasizes that each person has the freedom to choose his or her behavior and whether to share data with others. If a person chooses to share data, that person also has the freedom to choose the requirements that must be followed in order to prevent harm to the parties.<sup>17</sup>

Based on the results of the author's interview with the Chairperson of the Bandung City Anti Loan Shark Task Force, Mr Saji Sonjaya, all people who have problems with loan sharks, almost all of them get the same actions, namely, intimidation, dissemination of personal data that is included with the personal photos of the people being disseminated, and even the spread of slander carried out by loan shark collectors. The form of slander carried out is that collectors who spread personal data along with photos of the victims spread slander that the victim made the number addressed by the collector as an emergency contact even though in reality this was not the case, so that collectors can intimidate the number addressed by the collector to pressure victims to make debt payments.<sup>18</sup>

As a result, many people are disturbed, both socially and mentally as a result of the actions taken by pinjol collectors against people who have debts to the Pinjol, even though in the rules personal data is something that must be protected as in the ITE Law, one of them, but in reality many collectors from fintech companies (pinjol) have committed acts of spreading personal data and even spreading false news (slander).<sup>19</sup>

The act of disseminating personal data without the consent of the person concerned is one of the ITE criminal offences that should be charged as Article 26 paragraph (1) of the ITE Law and the act of disseminating personal data that is intended to cause hatred or hostility between individuals or groups (slander) as contained in Article 28 paragraph (2) of the ITE Law can be punished as Article 45 paragraph (2) of the ITE Law, but in reality these efforts are very difficult to do by the victims of pinjol who have their personal data disseminated. This is due to the excessive concern of the community who get strong intimidation from loan collectors so that the majority of people who are victims are reluctant to report to the Indonesian National Police.

---

<sup>16</sup> Mahira, DF, Emilda Y Lisa NA, "Consumer Protection System (CPS): Siste, Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept", *Jurnal Legislatif*, Vol.3 No.2, 2020, hlm.287-302

<sup>17</sup> Fanny, P, "Perlindungan Privasi data Pribadi Perspektif Perbandingan Hukum", *Jurnal Jatismara*, Vol.34 No.3, 2019, hlm. 239-249

<sup>18</sup> Hasil Wawancara Penulis dengan Ketua Satgas Anti Rentenir Kota Bandung Bapak Saji Sonjaya, S.H., M.H.Kes., C.L.I. pada tanggal 20 Desember 2021 pukul 13.30 WIB.

<sup>19</sup> *Ibid.*



## Law Enforcement Against Fintech Companies that Disseminate Personal Data

Along with the rapid development of information and technology in the business world, online lending in particular, is not free from problems, especially regarding personal data protection. Unwitting misuse of personal data can occur because it is the negligence of the potential victim (community) itself. For example, without the potential victims (the community) themselves realising that when making a money lending transaction through the application (Pinjol) then registering by attaching personal data to the platform or form and so on that without being aware of the potential victims (the community) the personal data entered into the application can be misused by pinjol and can potentially cause harm to the data owner.

In addition, as a result of the rapid development of science and technology today, big data is popularly used. Big data is considered a promising solution in processing data because it is able to process large and varied data and can make accurate attachments, thus making big data not only used by the government but also used by the private sector. Large companies that use it as an effort to study consumer behaviour, such as loyalty, visit patterns, purchase history and others, so that they are effective in marketing their products or services. However, on the other hand, it is undeniable that the misuse of big data can also threaten a person's privacy.<sup>20</sup>

Personal data is a very sensitive and private matter so that its protection is needed, both by the government and non-government as well as law enforcers. In an effort to realise expediency, justice and legal certainty in an effort to fortify themselves from data misuse, the community is also required to have high integrity so that they can collaborate with the government and law enforcement in realising it. Each country has a different term in using the term personal data such as in the United States, Canada and Australia using the term personal information while in European Union countries and Indonesia using the term personal data.<sup>21</sup>

If the current legislation do not specifically address the misuse of personal data, then self-regulation or preventative measures can be used to provide legal protection against it.<sup>22</sup> Since many other nations have enacted laws governing the protection of personal data, the Draft Law (RUU) on Personal Data Protection must be created and passed as soon as possible. For comparison, the UK's Data Protection Act of 1998, whose implementation body is known as the data protection commissioner, has been in place since 2000 and regulates the

---

<sup>20</sup> Sahat Maruli Tua Situmenang, Penyalahgunaan Data Pribadi sebagai bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber, *Jurnal Sasi* Vol. 27, No.1 Januari, 2021, hlm. 41

<sup>21</sup> Latumahina, R. E, Aspek Hukum Perlindungan Data Pribadi di Dunia Maya. *Jurnal Gema Aktualita*, Vol. 3, No. 2, Desember 2014, hlm. 14-25

<sup>22</sup> Salam, M. F, *Peradilan Militer Indonesia*, Mandar Maju, Bandung, 1994, hlm. 100

protection of a person's personal data. The data protection commissioner is tasked with monitoring any individual or organization that uses a person's personal data.

In Malaysia, the Personal Data Protection Act (PDPA) 2010 governs the processing of personal data by data users in the context of commercial transactions with the goal of protecting the interests of the data subject. Malaysia is one of the countries, along with the UK, that has regulated the protection of personal data. There are privacy and personal data principles that are accepted globally. Modern national data protection regulations are built on these tenets. The Organisation for Economic Co-operation and Development (OECD) published one of the international laws safeguarding personal information and privacy. Additionally, the European Convention for the Protection of Human Rights (ECHR) was established by the Council of Europe (CoE) in 1950.<sup>23</sup>

Similar to other nations, Indonesia still has issues with the enforcement of laws governing the protection of personal data. So it makes sense to compare this to other nations that have laws governing the protection of personal data used for cybercrime.

According to Sudikno Mertokusumo, the law serves as an instrument to safeguard the rights of people. According to Philipus M. Hadjon, the basic goal of the rule of law is to give its citizens legal protection. Two concepts, namely the principle of human rights and the principle of the rule of law, serve as the foundation for the legal protection of the populace against governmental activities.<sup>24</sup> Fundamental rights are those that are acknowledged as being inalienable to humans due to their nature. The right to freedom is one of the liberties that is seen as being highly fundamental. Humans cannot reach their full potential as people in their complete quality without the right to freedom.<sup>25</sup>

Regulations pertaining to the right to the privacy of personal information are an example of how fundamental human rights are acknowledged and safeguarded. As a result, the writing of the Personal Data Protection Draft Law has a solid and responsible philosophical basis. Pancasila, which is the rechtsidee (legal ideals) and the notion of bringing the law to what is desired, is the philosophical underpinning in question. According to Sunaryati Hartono, consideration must be given to the suitability of the national legal system (in a wide sense) that governs society, the country, and the state, particularly the Indonesian legal system, for the following purposes:<sup>26</sup> (a) Social values (whether

---

<sup>23</sup> Rosadi, S. D., & Pratama, G. G, Urgensi Perlindungan data Privasi dalam Era Ekonomi Digital Di Indonesia, *Veritas et Justitia*, Volume. 4, No.1, 2018, hlm. 104.

<sup>24</sup> Setiadi, H. E, *Sistem Peradilan Pidana Terpadu dan Sistem Penegakan Hukum di Indonesia*, Prenada Media, Jakarta, 2017, hlm. 272

<sup>25</sup> Akub, M. S dan M Ilyas, *Wawasan Due Process Of Law Dalam Sistem Peradilan Pidana*, Rangkang Education, Yogyakarta, hlm. 79.

<sup>26</sup> Gunawan & Kristian, *Perkembangan Konsep Negara Hukum Dan Negara Hukum Pancasila*, Refika Aditama, Bandung, 2015, hlm. 15.

the national legal system is in line with social values); (b) Legal philosophy (whether the national legal system is in line with Indonesia's legal philosophy); (c) Legal norms; (d) Legal institutions; (e) Processes and procedures to be applied in a national legal system; (f) Human resources in implementing an adopted legal system; and (g) Educational institutions and the legal education system.

Regarding the aforementioned, Article 28G of the Republic of Indonesia's 1945 Constitution serves as the legal foundation for personal data protection. Personal data protection is a way of implementing the constitutional requirement and must be governed by law. Every person has the right to the security and protection from the threat of fear of engaging in or refraining from engaging in behavior that is protected by human rights, according to Article 28G of the Fourth Amendment to the Republic of Indonesia's 1945 Constitution. This article conveys the significance of passing legislation and rules to safeguard personal information.

The many individuals who are committing the crime of disseminating personal data and are out and about doing it are inextricably linked to Indonesia's adoption of the Personal Data Protection Law (UU PDP) on Tuesday, September 20, 2022. This is especially true of the actions taken by several sizable fintech companies, also known as online loans (PINJOL), which are widely used to spread personal data. Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) was also passed with the support of numerous groups, and its ratification represents a step toward legal reform in Indonesia, particularly with regard to the rule of law "as a tool of social engineering".

According to Article 1 Point 2 of the PDP Law, "personal data protection" is defined as "the whole endeavor to protect personal data during personal data processing in order to ensure the constitutional rights of personal subjects, There are personal data controllers and personal data processors in the PDP Law. Any individual, group of individuals, or international organization that decides how to use personal data and exercises control over how it is processed is considered a personal data controller. A personal data processor, meantime, is any individual, group of individuals, or international organization operating alone or collaboratively to handle personal data on behalf of a personal data controller."<sup>27</sup>

Before the PDP Law was passed, it was frequently difficult for law enforcement to crack down on crimes involving the transmission of personal data, especially when they involved fintech firms or so-called Pinjol. This is because the prior legislative framework—Law Number 19 of 2016 Concerning Amendments to Law Number 11 of 2008 Concerning Electronic Information and Transactions (ITE Law)—used in efforts to enforce the illegal crime of disseminating personal data was inadequate.

---

<sup>27</sup> Rizky P.P dan Karo Karo, *Perlindungan Hukum atas Privasi dan Data Pribadi Masyarakat*, Artikel, dipublikasikan pada Selasa, 8 Oktober 2019

The Indonesian National Police (POLRI), in particular, implements law enforcement only based on the ITE Law, which explains that it does not specifically regulate the protection of personal data but rather the abuse of information systems and electronic transactions, such as cybercrime in the form of Illegal Content, Unauthorized Access to Computer System and Service, and Infringement of Intellectual Property Rights.

Law enforcement officials' efforts to enforce the law are closely tied to efforts to protect personal data because, if law enforcement can be carried out as effectively as possible against those who disseminate personal data, it is likely that personal data can be protected. Respecting the right to privacy includes protecting personal information, which must start by establishing legal certainty. In order to give enforcement against those who disseminate personal data legal certainty in its application, the guarantee of legal protection of personal data must be included in the constitution, a legal instrument with the greatest authority.

The numerous public complaints to the anti-loan shark task force of the city of Bandung as a victim of pinjol whose personal data is disseminated due to a lack of security and supervision of data users show that law enforcement against the dissemination of personal data in Indonesia generally and particularly in the city of Bandung is still considered to be subpar. Due to the fact that the enforcement took place before to the PDP Law's passage, it continues to be based on Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Although wiretapping is prohibited except by organizations with the legal authority to do so in the course of legal actions, the ITE Law has regulated data protection including wiretapping.

Given the rapid development of technology and information, the Personal Data Protection Law (PDP Law) must be implemented as much as possible in the future to protect the right to protection of one's self, family, honor, dignity, and property under their control, as stated in Article 28 of the 1945 Constitution. This will give the protection of personal data legal certainty. In order to enforce the law on the dissemination of personal data, law enforcers must take an active and responsible role in preventing and helping people who are victims of the criminal act of spreading personal data. Law enforcers have the authority to find, prevent, restore, and punish or take action against violators of laws in force in Indonesia.

## **Conclusion**

The criminal liability of fintech businesses or Pinjol for the act of disclosing personal information is included in the area of conduct for which there must be criminal liability. Others may suffer socially and psychologically as a result. It is reasonable that the act of distributing personal data can be punishable as provided for in the ITE Constitution and the PDP Law since those who commit crimes that disseminate personal data are classified as intentional (Opzet), which

is purposeful. Even a few of the perpetrators of spreading personal data reached the point of being tried in court, despite the fact that the primary goal of law enforcement is to promote safety, comfort, and peace in society. Prior to the passing of the PDP Law, enforcement against fintech companies or Pinjol that spread personal data was very weak and difficult to implement. The PDP Law's passage is a breath of fresh air for law enforcement since it gives law enforcement's use of personal data a solid legal foundation. The notion of legality is an issue in law enforcement.

## References

- Akub, M. S dan M Ilyas, *Wawasan Due Process Of Law Dalam Sistem Peradilan Pidana*, Rangkang Education, Yogyakarta.
- Alfhica Rezita Sari, *“Perlindungan Hukum Bagi Pemberi Pinjaman Dalam Penyelenggaraan Financial Technology Berbasis Peer To Peer Lending Di Indonesia”*, Skripsi Program Studi (S1) Ilmu Hukum Fakultas Hukum Universitas Islam Indonesia, Yogyakarta, 2018.
- Andi Hamzah, *Hukum Acara Pidana Indonesia*, Saptia Artha Jaya, Jakarta, 1996.
- Dewi, S. *Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia*, Yustisia Jurnal Hukum, Vol.5, No.1. 2016.
- Djoni S. Gozali dan Rachmadi Usman, *Hukum Perbankan, cet. II*, Sinar Grafika, Jakarta, 2012.
- Ernama, Budiharto, Hendro S., *“Pengawasan Otoritas Jasa Keuangan Terhadap Financial Technology (Peraturan Otoritas Jasa Keuangan Nomor 77/POJK.01/2016)”*, Diponegoro Law Journal, Vol. 6, No.3, 2017.
- Fanny, P, *“Perlindungan Privasi data Pribadi Perspektif Perbandingan Hukum”*, Jurnal Jatiswara, Volume 34 Nonor 3, 2019.
- Gunawan & Kristian, *Perkembangan Konsep Negara Hukum Dan Negara Hukum Pancasila*, Refika Aditama, Bandung, 2015.
- Hanafi, Mahrus, *Sistem Pertanggung Jawaban Pidana, Cetakan pertama*, Rajawali Pers, Jakarta, 2015.
- Latumahina, R. E, *Aspek Hukum Perlindungan Data Pribadi di Dunia Maya*. Jurnal Gema Aktualita, Volume 3, Nomor 2, Desember 2014.
- Mahira, DF, Emilda Y Lisa NA, *“Consumer Protection System (CPS): Siste, Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept”*, Jurnal Legislatif, Volume 3 Nomor 2, 2020.
- Moeljatno, *Perbuatan Pidana dan Pertanggungjawaban dalam Hukum Pidana*, Bina Aksara, Jakarta, 1983.
- Natamiharja, R., & Mindoria, S, *Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN*, Fakultas Hukum Lampung, Lampung, 2019.

- Roeslan saleh, *Pikiran-Pikiran Tentang Pertanggung Jawaban Pidana, Cetakan Pertama*, Ghalia Indonesia, Jakarta, 1982.
- Salam, M. F, *Peradilan Militer Indonesia*, Mandar Maju, Bandung, 1994.
- Setiadi, H. E, *Sistem Peradilan Pidana Terpadu dan Sistem Penegakan Hukum di Indonesia*, Prenada Media, Jakarta, 2017.
- Rosadi, S. D., & Pratama, G. G, *Urgensi Perlindungan data Privasi dalam Era Ekonomi Digital Di Indonesia*, Veritas et Justitia, Volume. 4, Nomor. 1, 2018.
- Rizky P.P dan Karo Karo, *Perlindungan Hukum atas Privasi dan Data Pribadi Masyarakat*, Artikel, dipublikasikan pada Selasa, 8 Oktober 2019
- Sahat Maruli Tua Situmeang, *Penyalahgunaan Data Pribadi sebagai bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber*, Jurnal Sasi, Volume 27 Nomor 1, Januari-Maret 2021.
- [https://www.bphn.go.id/data/documents/pphn\\_bid\\_informasi\\_dan\\_teknologi.pdf](https://www.bphn.go.id/data/documents/pphn_bid_informasi_dan_teknologi.pdf) diakses pada tanggal 11 Desember 2020, Pukul. 20:48 WIB
- Undang-Undang Dasar 1945
- Kitab Undang-Undang Hukum Pidana
- Undang-Undang Nomor 19 tahun 2016 Tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi