Jurnal Komunikasi Indonesia

Volume 13 | Number 2 Article 7

8-30-2024

Cyber Crime Against Women's Personal Data on Online Platforms and The Role of PDP Laws

Ambar Alimatur Rosyidah
Faculty of Social and Political Sciences, Universitas Gadjah Mada, Yogyakarta

Farah Fajriyah
Faculty of Social and Political Sciences, Universitas Gadjah Mada, Yogyakarta,

Rahayu Rahayu
Faculty of Social and Political Sciences, Universitas Gadjah Mada, Yogyakarta,

Recommended Citation

Rosyidah, Ambar Alimatur; Fajriyah, Farah; and Rahayu, Rahayu (2024) "Cyber Crime Against Women's Personal Data on Online Platforms and The Role of PDP Laws," *Jurnal Komunikasi Indonesia*: Vol. 13: No. 2, Article 7.
DOI: 10.7454/jkmi.v13i2.1229
Available at: https://scholarhub.ui.ac.id/jkmi/vol13/iss2/7

Volume 13
Issue 2
Augusts 2024
ISSN 2615-2894

JURNAL KOMUNIKASI INDONESIA

Cyber Crime Against Women's Personal Data on Online Platforms and The Role of PDP Laws

Ambar Alimatur Rosyidah*, Farah Fajriyah, Rahayu

Faculty of Social and Political Sciences, Universitas Gadjah Mada, Yogyakarta, 12920, Indonesia

**Email: ambaralimaturrosyidah@mail.ugm.ac.id*

Article Information
Received
23/11/2023
Received in revised form
03/03/2024
Accepted
19/07/2024
Available online
30/08/2024
DOI:
10.7454/jkmi.v13i2.1229

Keywords
Data privacy, women's vulnerability, PDP Law, Tripartite Cybercrime Framework

Abstract

The presence of online platforms such as financial technology lending platforms is like a double-edged knife for women. These platforms pave the way for restrictions on women accessing loans. However, the use of fintech poses risks to women. They become victims of cybercrime with the existence of desk collectors who collect online loans and the third party who use the women's data. This study aims to examine the cybercrime implications of using fintech experienced by women related to fintech lending and then explore the role, data protection, and scope of the Personal Data Protection Law as a solution. This study uses Qualitative Content Analysis (QCA) with the Tripartite Cybercrime Framework (TCF) to analyze the problem. The research data were women's complaint letters against fintech lending platforms that we obtained through the mediakonsumen.com website from 12 September 2020 to 8 November 2022. The PDP law, LBH reports, press releases, and relevant news media complement the data. These letters show five categories of women's experiences with online loan desk collector billing: online fraud, unauthorized transmission and use of personal data, identity theft, cyberbullying, and online harassment. This research also obtains socio-economic and psychosocial blending motives from online loan desk collectors. The core problem in online loan cases is ownership and access to personal data. Nevertheless, the PDP Law does not cover fundamental rights to data security, namely privacy rights and the victim's right to recovery.

Introduction

The presence of information and communication technology such as digital platforms have increased the risk of cybercrime for women (Kurnianingsih et al., 2022). As with finance, lending has been done online, known as Finance Technology or abbreviated as fintech (Lee et al., 2021). However, fintech peer-to-peer (P2P) lending platforms can be a two-edged sword for women. While these platforms contribute positively by

paving the way for restrictions on women accessing loans, they can also be harmful (Kurnianingsih et al., 2022; Ozili, 2018; Thakor, 2020). The Financial Services Authority (OJK) shows that the total outstanding online loans from women in Indonesia are higher than men, amounting to IDR 12.41 trillion and IDR 11.12 trillion, respectively, from January to October 2021 (Dihni, 2021). Women also dominate non-performing online loans, amounting to IDR 563 billion in the first semester of 2022 (Novia, 2022). This figure shows the vulnerability of women to becoming victims of cybercrime.

According to the National Commission on Violence Against Women (Komnas Perempuan), women as consumers often have negative experiences with debt collectors, especially in the digital space (Rahayu, 2021). Fintech lending uses debt collector services to collect the loan, by assigning desk collectors who remind debtors to pay debts using the ICT and field collectors who collect consumer payments in the field (Siagian et al., 2023). When the loan is collected, women experience intimidation, leading to financial status declines (Rahayu, 2021). The desk collectors of online loan providers often harass, terrorize, and scare consumers by targeting their co-workers, relationships, and even friendships (Rolobessy et al., 2023). This behavior falls under the cybercrime category, including cyberbullying and harassment or destruction (Reep-van den Bergh & Junger, 2018). The impact of cybercrimes can range from tangible injuries, such as data loss, to intangible losses, such as system crashes or loss of reputation, leading to financial losses (Chandra & Snowe, 2020).

The rise of internet and social media use has led to increased cybercrime that utilizes information and communication technology (Soomro & Hussain, 2019). Data from Komnas Perempuan reveals that there has been an 83% spike in the number of cases from 2020 to 2021, from 940 to 1721 cases (Shabrina, 2022). This type of cyber violence involves misusing personal data, which includes doxing, impersonation, and morphing. The issue of Cyber Gender-Based Violence is particularly concerning as it violates women's human rights and makes them feel unsafe as victims of violence (Komnas Perempuan, 2021).

Gender inequality plays a role in the vulnerability of women in terms of digital literacy status. In the 2021 Indonesia Digital Literacy Status report from the Ministry of Communication and Informatics and the Katadata Insight Center (KIC), where one of the indicators in this score is digital safety, women's average score is still below that of men (Ameliah et al., 2021). According to the report, 55% of male respondents' digital literacy scores were above the national average, while only 45% of women were above average (Mutiara, 2022). This score discrepancy indicates that women are more vulnerable in the digital world than men.

Research related to crimes against women in the media through messages shows some motives. A study in India mapped the forms of online violence experienced by women. The types of violence were dismissive insults, ethnoreligious slurs, and gendered sexual harassment (Kumar et al., 2021). These types of violence are related to how women's bodies are vulnerable in the digital space, so they often become targets of violence (Estrada, 2023). The message forms of harassment are placed on the media, showing empirically and conceptually how the experience of violence against women is also facilitated by digital technology (Henry et al., 2020). Existing studies are still mapping and showing empirical and conceptual data and have not resulted in policy recommendations. This research fills the gap by showing the implications of regulation, more specifically in the context of fintech-related crimes committed and explores how the media has power and contributes to violence.

Fintech as a media is increasingly becoming a part of our daily lives, and it is essential to address the gender issues that arise from its use. This article examines the risks of cybercrime resulting from the use of fintech lending platforms and how

the regulatory system addresses these issues. Specifically, we monitor grievances experienced by women as victims in the fintech industry using the Tripartite Cybercrime Framework (TCF) from Ibrahim (2016a) and Lazarus (2019). Using the Self-Determination Theory, we also delve deeper into the motivations of online loan platforms. Additionally, we explore the implications of the Personal Data Protection policy in Indonesia.

Self-Determination Theory (SDT) explains that humans have motives when accessing digital media. SDT, developed by Edward L. Deci and Richard M. Ryan, theorizes about human motivations. It is used in general and organizational psychology and was born out of an interest in studying intrinsically motivated behavior (Gagné & Deci, 2014). SDT assumes a dialectic between humans as an active organism with growth-oriented and the social context, which is the organism-environment that can influence this integrative growth or disrupt and impair the process (Deci & Ryan, 2015). This macro theory has five mini theories; one of the theories used in this research is the Organismic Integration Theory (OIT). This theory analyzes the reasons for a person's actions by placing the fundamental reasons from controlled (non-autonomous) to self-determined (autonomous) (Sheldon & Titova, 2023).

The relationship between Self Determination Theory and cybercrime is in the presence of the perpetrators' motivations. In Self Determination Theory, there are two extremes of motivation for someone to commit a crime: intrinsic and extrinsic, and in between is identified and introjected motivation (Deci & Ryan, 2015; Sheldon & Titova, 2023). Extrinsic motivation tends to carry out an activity solely to achieve different results, whereas intrinsic motivation is a demonstration of action that is inherent as a form of satisfaction for doing so (Ibrahim, 2016; Ryan, 2018). This motivation becomes different in cyberspace. Kshetri (in Ibrahim, 2016) describes cybercriminals and hackers as intrinsically motivated, which is considered to have a superior impact compared to extrinsic motivation.

Although there are no universally accepted definitions, cybercrime refers to the Internet and computer technology as the common denominator to perpetrate crimes impacting individuals, organizations, or governmental entities (Chandra & Snowe, 2020; Viano, 2017). In the modern view, cybercrime is borderless because there are no clear borderlines between the digital and the physical world (Chandra & Snowe, 2020; Europol, 2011; Viano, 2017). Perpetrators of cybercrime are motivated by three possible factors: socioeconomic, psychosocial, and geopolitical (Ibrahim, 2016). One of the causes is the lack of digital literacy skills that allow someone to become a victim of cybercrime (Sila & Taufik, 2023). When using digital media, a person unknowingly conveys their information through the user's data recorded by the system. Understanding the boundaries between important and unimportant data is part of digital literacy skills that concern modern society's ability amidst increasing communication and access to information through digital technology (Center for Digital Society, 2021).

Personal Data Protection in Indonesia and Content Moderation Platform

Fintech lending as a digital platform in the financial sector holds a large amount of data about bank accounts and identities of users which makes it necessary to develop methods of protection against cybercrime (Despotović et al., 2023). This technology is a relatively new component of the banking system and relies heavily on technologies prone to cybersecurity consequences, one of them is privacy issues (Despotović et al., 2023). Romansky (2019) broadens the definition of privacy as 'privacy in a digital environment (e-privacy),' which requires fulfilling the right to privacy. It must be seen as an independent right entitled to legal protection. Personal identity data is also

considered as privacy (Sim et al., 2019). Irresponsible dissemination of personal identity is prone to occur through online media. Potential crimes also vary; victims of cybercrime experience a similar range of emotional, psychological, and behavioral health consequences to the degree of suicidal ideation (Lazarus et al., 2022; Tan, 2018). In this case, the government should respond through policies where data protection laws produce a framework that can be applied to prevent information privacy (Tamò-Larrieux, 2018).

In Indonesia, the movement continues to mushroom, which is divided into e-commerce and fintech (Hiyanti et al., 2020). Loan service providers have many female consumers who are potential victims of data misuse (Sinombor, 2023). This research will look at the Personal Data Protection (PDP) Law ratified in 2022 and the potential for cybercrime. The PDP Law itself should be present to regulate data security, which was previously mentioned in the Article 26 of the Electronic Information and Transaction Law, known as ITE. However, the regulations that initially responded to online lending problems were deemed not to show different vulnerabilities and impacts between men and women due to personal data breaches (Shabrina, 2022).

Data protection is related to the content moderation policy contained in the ITE Law. Content moderation is widely discussed for social media platforms. It is defined by PR2Media (2023) as a 'process used by social media platforms to protect their users by evaluating, identifying, limiting, reducing traffic to, and/or deleting illegal and harmful content and/or the accounts that post said content' (p.6). Common (2020) explains three stages of content moderation: creation, which is the development of the rules; enforcement, which includes flagging content deemed problematic and taking action; and response, the internal processes of the platform and the methods of activists to change the platform from the outside. The problem is that the platform approach to the moderation of content is underdeveloped, which causes human rights issues (Common, 2020).

To see the motivation of perpetrators of Fintech platform cybercrime from a feminist perspective, we use the Tripartite Cybercrime Framework (TCF). TCF can facilitate this analysis because it is under a feminist crime epistemology that places gender at the heart of crime investigations and recognizes the sources of social gains and losses in society (Chesney-Lind, 2020; Lazarus et al., 2022). The Tripartite Cybercrime Framework (TCF), proposed by Ibrahim (2016b) and further developed by Lazarus (2019), is suitable for investigating the relationship between gender and cybercrime. TCF and feminist perspectives, according to Lazarus et al. (2022), both 'locate gender at the core of crime investigation and acknowledge that contextual cultures and nuances apply online as offline' (p.386). Feminist criminology, which emerged in the 1970s, is an approach to studying crimes with a feminist lens emphasis on gender, which includes women as victims, offenders, women working in the criminal justice system, and masculinities and crime (Lynch, 2018; Sharp, 2015).

TCF divides three motivations, which can be intrinsic and extrinsic, namely socioeconomic, psychosocial, and geopolitical (Ibrahim, 2016; Lazarus et al., 2022). According to Lazarus (2019), this TCF stands on the premise that perpetrators and victims from a broad spectrum of digital crimes have a unique relationship based on the perpetrator's main motivations and benefits and the primary victim's losses. Lazarus et al. (2022) investigate whether men and women hold different perceptions of digital crimes across these two dimensions, which are psychosocial (cyber fraud or online fraud) and socio-economic (cyberbullying, revenge porn, cyberstalking, and online harassment). The results exposed the women's vulnerability to psychosocial cybercrime. Psychosocial cybercrimes are more gendered than socio-economic (online fraud) cybercrime, which has no differences between men and women (Lazarus et al., 2022).

Table 1. Tripartite Cybercrime Framework (TCF)

No	Cybercrime categories	Definition	Types of Cybercrime
1	Socioeconomic cybercrime	*Cybercrime* can be defined as the computer or/and the acquisition of financial gain mediated by the internet.	False pretence, impersonation, manipulation, counterfeiting, forgery, or other fraudulent representations of facts, such as online fraud, credit card fraud, online embezzlement, and romance scams.
2	Psychosocial cybercrime	A digital crime is primarily psychologically driven to cause shock, distress, or harm to someone, where monetary gain is not the primary goal.	Cyber-stalking, cyberbullying, online-harassment
3	Geopolitical cybercrime	Cybercrimes are political and involve state agents (and non-state activists) and their representatives involved in the action	Cyber espionage or malware-based attacks disrupt the critical national infrastructure of a country.

Source: Ibrahim (2019) & Lazarus (2022)

Research Methods

This research uses a descriptive qualitative approach. The research data is the letters from women sent via mediakonsumen.com from September 2020 – December 11, 2022. Apart from being sent by women, the data should contain women's negative experiences with online loans related to their data. These letters were then analyzed using the Qualitative Content Analysis (QCA) method to summarize and explain key aspects of the data and explore the meaning individuals convey from their experiences (Schreier, 2012).

In the first stage, we sorted the data using the tag of '*pinjaman online'* (online loan) in *mediakonsumen.com*. After tag screening, we used the keywords '*data pribadi*' (personal data), '*intimidasi*' (intimidation), *'teror*' (terror), '*meneror*' (terrorize), *'melecehkan'* (harass), and *'pelecehan'* (harassment). The keywords extracted from the data of Komnas Perempuan and Legal Aid Institute (LBH) about women's experience in fintech lending. We get 16 letters from readers that match the criteria. In the next stage, we grouped experiences into five themes: online fraud, unauthorized transmission and use of personal data, identity theft, cyberbullying, and online harassment. These categories come from TCF and are suitable for investigating the relationship between gender and digital crime (Lazarus et al., 2022).

From those themes, we developed two codes: socio-economic and psychosocial motivations. Socio-economic motives are online fraud, identity theft, unauthorized transmission, and use of personal data, while psychosocial motives are cyberbullying and online harassment. In the final stage, this research examines the potential role and scope of Law No 27/2022 on Personal Data Protection (PDP) as a solution to the considerable risk of cybercrime problems against women caused by fintech platforms.

This analysis examines articles related to the PDP Law and presents related news, press releases, and reports of Komnas Perempuan and LBH.

Results

Cyber Crime Against Women in Fintech Lending: The Blending of Socioeconomic with Psychosocial

Based on reader letters sent to *mediakonsumen.com* from September 2020 - December 11, 2022, platforms that committed cybercrimes are both legal (registered by OJK) and illegal (unregistered). The perpetrators were the desk collectors and the third party who used the women's personal data. Several online loans with such collection methods in this cybercrime won the 2022 Top Brand Award, such as Kredivo and Akulaku.

Cybercrime can affect all women, both as borrowers in the application and those who are not. As borrowers, women often experience threats even though their loans are not yet due. Meanwhile, the data of non-borrowers are owned by the desk collector, such as identity card data. Women who are non-borrowers have previous experience as borrowers in other applications.

Lazarus (2022) showed different socioeconomic and psychosocial attributes as if there were strict boundaries between the two. Unlike online loans, the boundaries between socioeconomic and psychosocial motivations are fading. In cases of billing by online loan desk collectors, the primary motivation is socioeconomic. To get financial benefits; desk collectors carry out psychosocial attacks such as cyberbullying and online harassment. It is assumed that a psychological attack to the borrower would result in getting benefits from the loan interest.

Based on the desk collector's actions and the experiences of the victim, two simultaneous motives underlie the perpetrator's crime: socioeconomic and psychological. For instance, in the case of a woman identified as EK, desk collectors committed online fraud, unauthorized transmission, and use of personal data based on socioeconomic motives. They also performed cyberbullying and online harassment or based on the psychosocial motive. Deci & Ryan (2015) argued of controlled motivation, which 'comprises identified and integrated forms of extrinsic motivation, along with intrinsic motivation' (p.488).

Socioeconomic motivation as extrinsic motivation appears clear and active after external stimulation, such as an online loan platform. The stimulation is the pursuit of rewards such as money from their workplace (Deci & Ryan, 2015). The desk collector who carries out this task is equipped with a platform with the user's data along with the contacts. However, it turns out that DC also has psychosocial motives. This motive resides within the actor without stimulation and is more impactful than the extrinsic motive. The harassment causes victims, fear to a certain extent, and can results in fatalities.

Table 2. Research Findings on Types of Cyber Crime

No	Victims	Date	Types of Cybercrime
1	NR	Sept. 19, 2022	Cyberbullying, unauthorized transmission, and use of personal data, online harassment
2	IU	Apr. 21, 2022	Online fraud, unauthorized transmission, and use of personal data

No	Victims	Date	Types of Cybercrime
3	IP	Nov. 16, 2021	Cyberbullying, unauthorized transmission, and use of personal data
4	SA	May. 20, 2021	Cyberbullying, unauthorized transmission, and use of personal data, online harassment
5	PA	Oct. 1, 2021	Cyberbullying, unauthorized transmission, and use of personal data, online harassment
6	SR	Dec. 30, 2020	Cyberbullying, online fraud, unauthorized transmission, and use of personal data
7	ET	Nov. 8, 2022	Cyberbullying, unauthorized transmission, and use of personal data
8	EK	Feb. 22, 2022	Cyberbullying, online fraud, unauthorized transmission and use of personal data, online harassment
9	IN	Sept. 14, 2021	Cyberbullying, online fraud, unauthorized transmission, and use of personal data
10	CL	Oct. 14, 2021	Cyberbullying
11	AD	Nov. 19, 2020	Cyberbullying, online harassment
12	FT	Oct. 2, 2020	Cyberbullying, online harassment
13	KR	Sept. 12, 2020	Cyberbullying, unauthorized transmission, and use of personal data
14	SA	Oct. 7, 2021	Cyberbullying
15	DY	Dec. 21, 2020	Cyberbullying

Psychosocial Motives: Cyber Bullying and Online Harassment

Almost all female loan victims complained to *Mediakonsumen.com* that they experienced cyberbullying. Out of 15 women, 14 complained of threats or intimidation. Cyberbullying is intimidation using electronic technology (Kowalski et al., 2014). Desk collectors terrorize victims with high intensity, by contacting, threatening, and even coming directly to the victim's location. Cyberbullying is arguably worse than traditional bullying because it can be done anonymously and is easier to reach a wider audience.

This cyberbullying was performed with other types of cybercrime for socioeconomic motives, such as online fraud, distribution, and misuse of personal data, and psychosocial motives, such as online harassment. It was difficult to remove inappropriate or harassing messages, texts, and images after they had been posted or sent (StopBullying.gov, 2017). Cyberbullying carried out continuously would have implications for many other losses to victims, both material and non-material.

Several informants experienced those implications. NR, one of the victims, suffered

from cyberbullying in the form of threats to spread personal data, such the photos, and online harassment asking for a sex video call (VCS). She was asked to pay off loans that had never been borrowed in the Super Loan application. NR told the debt collectors that she would pay the debt only if the collector could provide proof that she had gotten the loan. Instead of providing proof, the collector offered VCS so her debt would be paid off. NR then threatened to report the collector to the police.

SA also experienced another threat in the form of online harassment. Gender-based online harassment reflects the cultural understanding of gender and women's inferior place in society. Gender-based online hate is rooted in 'old' misogynistic discourses emphasizing women's inferiority to men (Jane, 2014). The Top Balance desk collector threatened SA that her personal data and photo would be sent to her contact list because she had not paid the due bill. The Desk collector also used harassing words such as *'lonte*', which means whore, and '*entot*', which means have sex, by typing in capitals (Badan Pengembangan dan Pembinaan Bahasa, 2016). Moreover, the debt collector also threatened to advertise her number as if she was trading herself for sex, using the term of "open booking out".

Another victim, identified as FT, also had online harassment claimed to be performed by Dana Now desk collector. Her photos were distributed to her contact lists.

Cultures have the power to influence binary dichotomy related to gender: men with masculine characters and women with feminine characters (Connell & Messerschmidt, 2005). As a result, men and women experience cyberspace differently. These differences are evident in the relational processes that characterize psychosocial types of cybercrime, such as online harassment, which is mainly perpetrated by male perpetrators targeting women who are victims (Lazarus et al., 2022). It can occur due to inequality in power relations, which, if not distributed evenly online, can increase gender differences in society (Lazarus et al., 2022; Morahan-Martin, 2000). One of the victims of the debt collector experienced psychosocial cybercrime using misogynistic language sent through WhatsApp messages.

The consequences of psychosocial attacks include anxiety, self-harming, depression, low self-esteem, and suicidal ideation of varying degrees (Stevens et al., 2021; Watts et al., 2017). As reported by *CNN* and *detik.com*, a single mother committed suicide because she was trapped by online loans. There was a chat history with a debt collector that showed she had a 12-million-rupiah loan. There was also a report about a woman from Wonogiri with a total 52-million-rupiah debt from 23 different platforms (Purnomo, 2021). No regulation prevents the fatal impact of the online loan. Jakarta Legal Aid Foundation (LBH Jakarta) considers that the regulation issued by the Financial Service Authority (OJK) in 2016 is no longer relevant to today's development of fintech service, and is even counter-productive to the OJK Law, which is the hallmark of OJK's existence.

Socioeconomic Motives: Online Fraud and Unauthorized Transmission and Use of Personal Data

Online fraud is a type of socioeconomic cybercrime where the goal tends to weaken the economy of its victims (Ibrahim, 2016). This type of cybercrime refers to computers and/or acquiring financial benefits mediated by the internet through pretence, impersonation, manipulation, counterfeiting, forgery, or other fraudulent representations of facts (Lazarus, 2019). Some research find that online fraud always goes hand in hand with other socioeconomic types, particularly unauthorized transmission, and use of personal data. The pattern is similar, and the perpetrator commits online fraud by getting and using the victim's data.

An informant named IU claimed to have experienced online fraud by Cairin

platform. She confessed that she once borrowed money from Cairin – a platform that is monitored by the OJK. She got the fund in 2019 and already paid the loan and never borrowed again from Cairin. She claimed that later, her data was misused, and she was accused of having borrowed money several times with different amounts, such as IDR 500k, 992k, and 536k. According to her, there were several bank accounts for the money disbursement and the platform claimed that they were her account.

Another informant, identified as SR, was also claimed to be a victim of online fraud. In November 2020, she got a loan transferred from Fast Rupiah to her bank account which she already paid on Dec. 7, 2020. She did not delete the application from her cell phone, and on Dec. 14, 2020, she got a notification that there was a new loan created on her name amounting to IDR 1.6 million transferred to an e-wallet OVO account which was registered as her number. SR claimed that it was not her number, and she had never received the fund. She complained via telephone and email, but the responses were not professional and repetitive. By the end of the month, she started getting terrors to pay the so-called her loan which she refused to pay. She said that she tried reported the case to the police, but the detective rejected to issue letter of accepting the report, saying that it was a civil case, instead of a criminal case. There was a comment on her report claiming to have been in comparable situation.

In these two cases, personal users' data were leaked to third parties and misused. Borrowers who installed or used online loan services are at risk of having their data misused once the data is in the lender's database. Previously, there were no rules that prevent the platforms from using personal data. The platforms that own the data were free to use the data for their interests, in this case, providing/selling data to other parties. Apart from hacking, one of the causes of data leakage is the absence of people awareness to protect personal data on the internet (Kominfo, 2019). In some cases, personal data leaks violate women's right as they were used for online loans.

The involvement of Indonesian adult men in socio-economic cybercrimes might be coming from interpersonal relationship problems in offline world and cyberspace. The patriarchal culture of Indonesian society influences the centrality of cybercrime with socio-economic motives (Ibrahim, 2016). In a patriarchal system, men are shackled to their role as breadwinners, while women are stigmatized for doing domestic work.

Gender inequality is also related to employment. Several studies investigated gender inequality in the economy sector, concerning the labor market, regarding women as laborers and entrepreneurs (Klasen & Lamanna, 2009). In Indonesia, Labor Force Participation Rate issued in February 2022 reflected the gender-based inequality. Male participation rate was recorded at 83.65%, higher than female at 54.27% (Badan Pusat Statistik, 2022).

Discussion

Fundamental Rights in Data Security: Scope and Relevant Terms

Platform ownership of personal data is the main problems of online loan cases. From the desk collectors' point of view, access to the borrower's data is entry point to cybercrime. Meanwhile, from the platform side, the problem is more complex and related to security, misuse, and giving access to users' data to third parties. Personal data protection is part of human rights, namely the right to privacy. This right to privacy has been regulated by the Article 28G that stated, "Every person has the right to protection of self, family, honour, dignity, and their property, and has the right to security and protection from threats of fear to exercise or not to exercise his human rights."

In Indonesia, PDP Law limits the use of personal data. The law is meant to be used as a guideline by everyone, from public to international agencies, and private parties who have access to processing user or customer data, including online loans. One of

the law's articles stipulates electronic system operators (PSE) in managing, and processing data, and imposing fines of up to 10 billion rupiah in case of a data leak (Septiani, 2022).

In the PDP Law, fintech lending is included in the financial sector. It defines the financial services sector as banking, capital markets, insurance, financing institutions, pension funds, technology-based regulations, and financial technology. Other technology-based finance services are supervised by the central bank (Bank Indonesia), the Financial Services Authority (OJK), and the Deposit Insurance Corporation. However, Article 15D of the law explains that the rights of the subjects of the data protection are exempted in the case of supervision interest of the financial service sector, monetary, payment system, and financial system stability for the sake of state governing. This article contradicts the Australian Government's definition of privacy rights, which includes the right: 'to be free from harassment and intrusion, to associate freely with whomever the user wishes, to be able to control who can see or use information about the user', indicating the need that the rights to privacy should be upheld. The exception of the rights also contradicts to the Constitution. That article could limit the rights of the subjects of personal data protection, in this case, users of online lending platforms.

The PDP Law stipulates data acquisition and collection, processing and analysis, storage, repairs and updates, appearance, announcement, transfer, distribution, or disclosure, and deletion or destruction. Those categorised as personal data controllers and processors are stated in the Article 19, including person, public agency, and international organization. Subjects of personal data should provide consent before the processing of the data. However, desk collectors from lending platforms can access personal data and even misuse it (Undang-Undang Perlindungan Data Pribadi, 2022).

The PDP Law has also provided a submission protocol for data leakage issues. In the case of data leakage, the personal data controller must submit written notification no later than 3 x 24 (three times twenty-four) hours to subjects of personal data (Undang-Undang Perlindungan Data Pribadi, 2022). The written notification should contain the disclosed personal data, when and how the data is disclosed, and efforts to handle and recover the disclosure by the Personal Data Controller. In facts, the consumer reports show no follow up to such complaints regarding data leakage.

The regulation does not specify gender-based vulnerability as a consumer in the Deposit Insurance Corporation. The PDP Law states that those considered vulnerable are children and persons with disabilities. Women's vulnerability is assumed to be higher due to the potential for data misuse, especially in the fintech context, and the law is considered biased towards the vulnerability exercised by power relations. According to Andy Yentriyana from Komnas Perempuan (2022), Article 65 of the PDP Law has not shown different vulnerabilities and impacts between men and women, does not provide the right to remedy for victims of violations of the prohibition, and ignores gender-based special needs due to misuse of personal data. Article 65, paragraph 1 reads, 'Every person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him to benefit himself or others which can result in loss of Personal Data Subjects' (Undang-Undang Perlindungan Data Pribadi, 2022).

The Importance of Content Moderation and Recommendations for the PDP Law

As a medium that plays a role in exchanging messages and leads to potential crimes, fintech is unsafe. The danger of online loans as a platform cannot be overcome with only digital literacy ability. Financial technology platforms have more power to moderate the content within them. Platforms as consumer media have a significant role in the security of disseminating user information so that it has the potential to harm users, especially regarding personal data, which is also considered the realm of

privacy. There is a need for a moderation process and making regulation recommendations (PR2Media, 2023).

To mitigate some of the concerns highlighted here in connection with online lending and the resulting social costs, we propose the following moderation. First, there should be efforts to ensure the independence of regulatory agencies. An independent data protection supervisory agency is the key to the effectiveness of implementing the PDP Law to ensure compliance by the data controllers and processors, as well as guaranteeing the fulfilment of the rights of data subjects in the private sector and public bodies (Mursyid & Akbar, 2022). However, this non-governmental institution was formed by the president. According to the Executive Director of the Institute for Community Studies and Advocacy (ELSAM) Wahyudi Djafar, the independence of the supervisory agency had been questioned. There have been doubts that this protection supervisory institution can impose sanctions on other fellow government institutions (Mursyid & Akbar, 2022).

Second, the regulation should specifically determine the types of cybercrime, particularly making it gender-friendly by including an article regarding the right to recover personal data subjects as victims. The PDP Law needs to regulate cybercrimes related to personal data as its landscape distincts from traditional criminal acts in terms of transmission speed. The speed of the data spreads requires a quick response from data controllers and supervisory agencies to immediately conduct a risk assessment. There law should be revised to make it more gender friendly, particularly giving attention to the vulnerability of women. One of the essential parts related to women's vulnerability is providing recovery for the victims, in this case, the subject of personal data, which is supposed to be one of the rights listed in the PDP Law. Recovery for victims has been included in Act 46, but it is only mentioned as one that must be included in the report. The PDP Law needs to define the intended recovery related to the material and immaterial, such as psychological damage.

Third, the implementation of Personal Information Protection certification should be determined. As a supervisory institution, the Commission for the Protection of Personal Data should issue an output in the form of certification for data controllers who have passed the Data Privacy Impact Assessment. South Korea also enforces a similar personal Data Information Protection Law procedure. Besides being able to assess the risk of personal data on digital platforms, this procedure can also be a monitoring tool. With the implementation of certification, online loan platforms that pass certification certainly have minimal violations of personal data. The online loan will certainly have limitations in providing data subject personal information to employees as desk collectors.

Fourth, there should be self-regulation of online loan platforms regarding billing procedures and limits on personal information, and regulation on the period of data storage in the database. Many online harassment cases committed by fintech lending desk collectors should be part of the platform evaluation as these cases will affect the image of the platform itself in the eyes of consumers. It is time for online lending platforms to self-regulate in the form of billing procedures and limits on personal information accessed by DC. The platform should also train prospective DCs regarding billing procedures according to established regulations.

Conclusion

This research found various imbalances in the digital space. There are technology-related crimes, although the initial role of the technology is to mediate communication. Instead of providing security, platforms behave oppositely. The laws do not provide solutions, as it does not specifically regulate user security rights. Digital media is a technical technology concept and a medium that provides or mediates

human relations (Buckingham, 2015). In this digital ecosystem, polemics in the form of cybercrimes were born, primarily related to the security of consumer user data in online loan services. Concerning gender-related cybercrime, the TCF framework shows five types of cybercrime: online fraud, unauthorized transmission and use of personal data, identity theft, cyberbullying, and online harassment. Even though it can show the motives of crimes committed by DCs, this framework shows a clear boundary between socioeconomic and psychosocial motives, which in reality, do not see boundaries. This framework needs to be modified to see cases such as online loans.

This online loan cybercrime shows that personal data are spread without the borrower's permission. The Personal Data Protection Act (UU PDP), which was passed on September 20, 2022, responded to this problem with the aim of 'guaranteeing citizens' rights to personal data protection and raising public awareness and guaranteeing recognition and respect for the importance of protecting personal data' (Undang-Undang Perlindungan Data Pribadi, 2022). However, according to Komnas Perempuan (2022), the PDP Law 'does not provide rights to recovery for victims of prohibition violations and pay attention to gender-based special needs due to misuse of personal data.' Online loans problems have burdened the consumers psychologically and economically. The right to recovery must be included in one of the subject rights in the PDP Law, and it should be gender friendly. To realize it, there should be collaboration from all sides to support the regulation, establishment of independent supervisory agencies, specifications for cybercrimes, and determining certification and limits on personal data by relevant agencies.

References

Ameliah, R., Negara, R.A., & Rahmawati, I. (2021). Status Literasi Digital di Indonesia 2021. Retrieved from https://cdn1.katadata.co.id/media/microsites/litdik/Status_Literasi_Digital_diIndonesia%20_2021_190122.pdf

Badan Pengembangan dan Pembinaan Bahasa. (2016). *KBBI Daring*. Kemdikbud. https://kbbi.kemdikbud.go.id/

Badan Pusat Statistik. (2022). *Keadaan Ketenagakerjaan Indonesia Februari 2022* [Press Release]. https://www.bps.go.id/pressrelease/2022/05/09/1915/februari-2022--tingkat-pengangguran-terbuka--tpt--sebesar-5-83-persen.html

Buckingham, D. (2015). Defining digital literacy: What do young people need to know about digital media? *Nordic Journal of Digital Literacy*, 10, 21–35. https://doi.org/10.18261/issn1891-943x-2015-jubileumsnummer-03

Center for Digital Society. (2021). *Digital Literacy as Basic Competency for Post?Pandemic Life*. https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2021/11/78-CfDS-Case-Study-Digital-Literacy-as-Basic-Competency-for-Post-Pandemic-Life.pdf

Chandra, A., & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, *38*, 100467. https://doi.org/10.1016/j.accinf.2020.100467

Chesney-Lind, M. (2020). Feminist criminology in an era of misogyny†. *Criminology*, *58*(3), 407–422. https://doi.org/10.1111/1745-9125.12247

Common, M. F. (2020). Fear the Reaper: how content moderation rules are enforced on social media. *International Review of Law, Computers and Technology*, *34*(2), 126–152. https://doi.org/10.1080/13600869.2020.1733762

Connell, R. W., & Messerschmidt, J. W. (2005). Hegemonic masculinity rethinking the concept. *Gender and Society*, *19*(6), 829–859. https://doi.org/10.1177/0891243205278639

Deci, E. L., & Ryan, R. M. (2015). Self-Determination Theory. In *International*

Encyclopedia of the Social & Behavioral Sciences: Second Edition (Vol. 11). Elsevier. https://doi.org/10.1016/B978-0-08-097086-8.26036-4

Despotović, A., Parmaković, A., & Miljković, M. (2023). Cybercrime and cyber security in fintech. In *Digital transformation of the financial industry: approaches and applications* (pp. 255-272). Cham: Springer International Publishing

Dihni, V. A. (2021). *OJK Catat Outstanding Pinjaman Online Sebesar Rp 27,9 Triliun pada Oktober 2021*. Katadata.co.id. http://databoks.katadata.co.id/datapublish/2021/12/15/ojk-catat-outstanding-pinjaman-online-sebesar-rp-279-triliun-pada-oktober-2021

Sila, G.E. & Cevi, M.T. (2023). Literasi Digital Untuk Melindungi Masyarakat Dari Kejahatan Siber. *Komversal*, *5*(1), 112–123. https://doi.org/10.38204/komversal.v5i1.1225

Estrada, M. S. (2023). Feminist Strategies Against Digital Violence: Embodying and Politicizing the Internet. *Studies in Social Justice*, *17*(2), 241–258. https://doi.org/10.26522/ssj.v17i2.3417

Europol. (2011). *Cybercrime presents a major challenge for law enforcement*. https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-presents-major-challenge-for-law-enforcement

Gagné, M., Gagné, M., & Deci, E. L. (2014). The History of Self-Determination Theory in Psychology and Management. In M. Gagné (Ed.), *The Oxford Handbook of Work Engagement, Motivation, and Self-Determination Theory*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199794911.013.006

Henry, N., Flynn, A., & Powell, A. (2020). Technology-Facilitated Domestic and Sexual Violence: A Review. *Violence Against Women*, *26*(15–16), 1828–1854. https://doi.org/10.1177/1077801219875821

Hiyanti, H., Nugroho, L., Sukmadilaga, C., & Fitrijanti, T. (2020). Peluang dan Tantangan Fintech (Financial Technology) Syariah di Indonesia. *Jurnal Ilmiah Ekonomi Islam*, *5*(3), 326–333. https://doi.org/10.29040/jiei.v5i3.578

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Undang-Undang Perlindungan Data Pribadi, Ditama Binbangkum - BPK RI 1 (2022). https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022

Jane, E. A. (2014). "Your a ugly, whorish, slut": Understanding E-bile. *Feminist Media Studies, 14*(4), 531–546. https://doi.org/10.1080/14680777.2012.741073

Katadata Insight Center & Kominfo (2021). *Status Literasi Digital di Indonesia: Hasil Survei di 34 Provinsi*. https://katadata.co.id/StatusLiterasiDigital

Kivivuori, J., Aaltonen, M., & Näsi, M. (2021). *Kriminologia: Rikollisuus ja kontrolli muuttuvassa yhteiskunnassa* (3. painos). Gaudeamus.

Klasen, S., & Lamanna, F. (2009). The impact of gender inequality in education and employment on economic growth: New evidence for a panel of countries. *Feminist Economics*, *15*(3), 91–132. https://doi.org/10.1080/13545700902893106

Kominfo. (2019). *5 Alasan Mengapa Data Pribadi Perlu Dilindungi*. https://www.kominfo.go.id/content/detail/19991/5-alasan-mengapa-data-pribadi-perlu-dilindungi/0/sorotan_media

Sari, D.A.K, Hutabarat, R.M., Tardi, S.A. (Eds.) (2021). *Perempuan dalam himpitan pandemi: lonjakan kekerasan seksual, kekerasan siber, perkawinan anak,dan keterbatasan penanganan di tengah covid-19*. Catatan Kekerasan terhadap Perempuan Tahun 2020. https://komnasperempuan.go.id/catatan-tahunan-detail/catahu-2021-perempuan-dalam-himpitan-pandemi-lonjakan-kekerasan-seksual-kekerasan-siber-perkawinan-anak-dan-keterbatasan-penanganan-di-tengah-covid-19

Komnas Perempuan. (2022, September 28). *Siaran Pers Terkait Tindak Lanjut UU Perlindungan Data Pribadi Untuk Memastikan Jaminan Rasa Aman Bagi Perempuan* [Press Release]. https://komnasperempuan.go.id/siaran-pers-detail/siaran-pers-terkait-tindak-lanjut-uu-perlindungan-data-pribadi-untuk-memastikan-jaminan-rasa-aman-bagi-perempuan

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, *140*(4), 1073–1137. https://doi.org/10.1037/a0035618

Kumar, P., Gruzd, A., & Mai, P. (2021). Mapping out Violence Against Women of Influence on Twitter Using the Cyber–Lifestyle Routine Activity Theory. *American Behavioral Scientist*, *65*(5), 689–711. https://doi.org/10.1177/0002764221989777

Kurnianingsih, M., Azhari, A. F., Dimyati, K., Absori, A., Wardiono, K., Kuswardhani, K., & Nurrachman, A. D. (2022). Criminal Victimization: Women and Fintech Financing from the Theory of Lifestyle Exposure. *International Journal of Multicultural and Multireligious Understanding*, *9*(2), 157. https://doi.org/10.18415/ijmmu.v9i2.3357

Lazarus, S. (2019). Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework. *International Social Science Journal*, *69*(231), 15–33. https://doi.org/10.1111/issj.12201

Lazarus, S., Button, M., & Kapend, R. (2022). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Lee, C. C., Li, X., Yu, C. H., & Zhao, J. (2021). Does fintech innovation improve bank efficiency? Evidence from China's banking industry. *International Review of Economics and Finance*, *74*, 468–483. https://doi.org/10.1016/j.iref.2021.03.009

Lynch, M. J. (2018). Acknowledging Female Victims of Green Crimes: Environmental Exposure of Women to Industrial Pollutants. *Feminist Criminology*, *13*(4), 404–427. https://doi.org/10.1177/1557085116673172

Morahan-Martin, J. (2000). Women and the Internet: Promise and perils. *Cyberpsychology and Behavior*, *3*(5), 683–691. https://doi.org/10.1089/10949310050191683

Mursyid, F., & Akbar, N. A. (2022, September 20). *Terbitnya UU PDP Bukan Solusi Akhir Masalah Perlindungan dan Kebocoran Data*. Republika. https://news.republika.co.id/berita/riiarn328/terbitnya-uu-pdp-bukan-solusi-akhir-masalah-perlindungan-dan-kebocoran-data

Mutiara, C. (2022). *Literasi Digital Perempuan Indonesia Belum Setara dengan Laki-laki*. https://databoks.katadata.co.id/datapublish/2022/07/14/literasi-digital-perempuan-indonesia-belum-setara-dengan-laki-laki

Novia, I. (2022, September). *OJK: Kredit Macet Pinjol Capai Rp 1,21 Triliun, Kebanyakan Perempuan Usia Produktif*. Republika. https://ekonomi.republika.co.id/berita/ri4lmc349/ojk-kredit-macet-pinjol-capai-rp-121-triliun-kebanyakan-perempuan-usia-produktif

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *18*(4), 329–340. https://doi.org/10.1016/j.bir.2017.12.003

PR2Media. (2023). *Research Paper: Regulations for Moderating Illegal content on social media in Indonesia*. https://pr2media.or.id/publikasi/research-paper-regulations-for-moderating-illegal-content-on-social-media-in-indonesia/

Purnomo, A. (2021). *Tragis Wanita Terjerat Utang 23 Pinjol Ilegal hingga Bunuh Diri*. https://news.detik.com/berita-jawa-tengah/d-5776778/tragis-wanita-terjerat-utang-23-pinjol-ilegal-hingga-bunuh-diri

Rahayu. (2021). *Perempuan dan Literasi Digital*. Gadjah Mada University Press.

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime Science*, *7*(1). https://doi.org/10.1186/s40163-018-0079-3

Rolobessy, V. Y., Malik, F., & Suwarti, S. (2023). Legal Liability of Illegal Online Loans in the Perspective of Criminal Law. *Journal of Social Science*, *4*(2), 439–454. https://doi.org/10.46799/jss.v4i2.542

Romansky, R. (2019). A Survey of Informatization and Privacy in the Digital Age and Basic Principles of The New Regulation. *International Journal on Information Technologies & Security*, *11*(1), 95–106. https://openurl.ebsco.com/EPDB%3Agcd%3A14%3A14696174/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A135033191&crl=f

Ryan, K. M. (2018). Vertical video: rupturing the aesthetic paradigm. *Visual Communication*, *17*(2), 245–261. https://doi.org/10.1177/1470357217736660

Schreier, M. (2012). *Qualitative Content Analysis in Practice*. Jacobs University Bremen, Germany.

Septiani, L. (2022). *Marak Kebocoran Data di Indonesia, Ahli IT Akui BSSN Kekurangan Dana*. https://katadata.co.id/desysetyowati/digital/631ae3496034b/marak-kebocoran-data-di-indonesia-ahli-it-akui-bssn-kekurangan-dana

Shabrina, D. (2022, September 30). *RUU Perlindungan Data Pribadi belum Lindungi Perempuan dari Kekerasan Siber*. Media Indonesia. https://mediaindonesia.com/humaniora/526775/ruu-perlindungan-data-pribadi-belum-lindungi-perempuan-dari-kekerasan-siber

Sharp, S. F. (2015). Feminist Criminology and Gender Studies. In J.D. Wright (Ed.) *International Encyclopedia of the Social & Behavioral Sciences* (2nd Ed, pp. 912–917). https://doi.org/10.1016/B978-0-08-097086-8.45059-2

Sheldon, K. M., & Titova, L. (2023). Social media use and well-being: testing an integrated self-determination theory model. *Media Psychology*, *26*(6), 637–659. https://doi.org/10.1080/15213269.2023.2185259

Siagian, N., Siregar, H., & Nababan, R. (2023). Online Lending Business and Its Criminal Aspect of Collectibility. *Journal on Education*, *5*(3), 7400–7405. https://doi.org/10.31004/joe.v5i3.1529

Sim, W. L., Chua, H. N., & Tahir, M. (2019). Blockchain for Identity Management: The Implications to Personal Data Protection. *2019 IEEE Conference on Application, Information and Network Security,* 30–35. https://doi.org/10.1109/AINS47559.2019.8968708

Sinombor, S. H. (2023). *Perempuan Paling Banyak Terjerat "Pinjol"*. Kompas.Com. https://www.kompas.id/baca/humaniora/2023/02/03/rendah-literasi-keuangan-digital-perempuan-terus-jadi-korban

Soomro, T. R., & Hussain, M. (2019). Social media-related cybercrimes and techniques for their prevention. *Applied Computer Systems, 24*(1), 9-17. https://doi.org/10.2478/acss-2019-0002

Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367–376. https://doi.org/10.1089/cyber.2020.0253

StopBullying.gov. (2017). *The Consequences of Bullying Academic Effects* [Fact Sheet]. The Maternal and Child Health Bureau, Health Resources and Services Administration, U.S. Department of Health and Human Services. https://www.stopbullying.gov/sites/default/files/2017-10/consequences-of-bullying-fact-sheet.pdf

Tamò-Larrieux, A. (2018). *Designing for privacy and its legal framework: Data*

protection by design and default for the internet of things (1st Ed). Springer.
Tan, C. (2018). *Regulating Content on Social Media*: *Copyrights, Terms of Service and Technological Features*. UCL Press. https://doi.org/10.2307/j.ctt2250v4k
Thakor, A. (2020). Corrigendum to: Fintech and Banking: What Do We Know? *Journal of Financial Intermediation*, *43,* 100858. https://doi.org/10.1016/j.jfi.2020.100858
Viano, E. C. (Ed.). (2017). *Cybercrime, Organized Crime, and Societal Responses: International Approaches (*1st Ed). Springer. https://doi.org/10.1007/978-3-319-44501-4
Watts, L. K., Wagner, J., Velasquez, B., & Behrens, P. I. (2017). Cyberbullying in higher education: A literature review. *Computers in Human Behavior*, *69*, 268–274. https://doi.org/10.1016/j.chb.2016.12.038