Protection of Personal Data in Criminal Law Enforcement Processes

Sintong Gariel Lumban Tobing [*1] T. Riza Zarzani [*2] Henry Aspan [*3]

[123]Panca Budi Development University
E-mail: sintonggabariel926@gmail.com trizazarzani@dosen.pancabudi.ac.id
henryaspan@dosen.pancabudi.ac.id

Article Info
Article History
Received: 2025-08-25
Revised: 2025-08-29
Published: 2025-09-05

Keywords:
Law enforcement, Protection, Personal Data

Abstract
This study aims to determineHow is Personal Data Protection in the Criminal Law Enforcement Process? The research methodology used in this study is normative juridical research using a statute approach, a conceptual approach, and a case approach.
The results of the discussion stated that the regulations regarding Personal Data in Indonesia are regulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) which was ratified on Tuesday, September 20, 2022. If there is a failure in Personal Data Protection, Administrative Sanctions will be imposed under Article 57 and Criminal Provisions under Article 67 and Article 69. In the case of criminal acts, Article 70 will be imposed.

I. INTRODUCTION

The issue of personal data protection has become increasingly prominent in recent decades, particularly in the digital era, where the flow of information is limitless. Modern life is now inextricably linked to the use of personal data, from financial transactions and healthcare services to education and even daily interactions via social media. Personal data is no longer simply technical information associated with an individual, but has become a fundamental part of a person's legal and social identity. Personal data allows a person to be identified, granted access rights, and even subject to legal liability. It's no wonder that personal data protection is viewed as a human right that the state must uphold.

The Indonesian Constitution has affirmed this. Article 28G paragraph (1) of the 1945 Constitution states that everyone has the right to protection of themselves, their families, their honor, their dignity, and their property under their control, and has the right to a sense of security and protection from the threat of fear. This constitutional norm provides a strong basis for the constitutional right of citizens to protect personal data. This protection is increasingly relevant when linked to developments in information technology that allow for massive data misuse. When personal data is leaked or falsified, not only technical information is lost, but also a person's basic right to live safely, with dignity, and with protection.

From an international perspective, the principle of personal data protection is also an essential part of human rights instruments. Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) both affirm the right to privacy and protection from arbitrary interference with private life. This means that personal data protection is not merely a local or domestic issue but also part of a global commitment that Indonesia, as a state party, must fulfill. Khaila (2024) emphasized that in the digital era, the right to privacy cannot be separated from the right to personal data protection, as the two are closely interconnected and are prerequisites for ensuring individual freedom.

The emergence of the Personal Data Protection Bill (PDP Bill) in 2012, which was later ratified as Law Number 27 of 2022, demonstrates the state's awareness of the urgency of this issue. For years, prior to the enactment of the PDP Law, Indonesia relied solely on partial regulations from the Electronic Information and Transactions (ITE) Law and sectoral regulations in banking, health, and population administration. This legal fragmentation created uncertainty and vulnerability, as there was no comprehensive regulation governing who is responsible for data breaches, how victims should be rehabilitated,

and what sanctions can be imposed on perpetrators. Barda Nawawi Arief (2000) emphasized that criminal law must adapt to societal developments, including addressing the challenges of modern crimes such as the misuse of personal data.

In practice, personal data leaks have caused public unrest. In recent years, Indonesia has been rocked by numerous large-scale data leaks, including data from telecommunications operators, bank customers, and even hospital patients. These cases highlight the weaknesses of data security systems and the unpreparedness of regulations to provide effective protection. As a result, the public is often the most disadvantaged, while those who should be held responsible are often difficult to hold accountable. This phenomenon demonstrates the importance of specific regulations that provide legal certainty and guarantee the protection of victims' rights (Nurul Qamar, 2017).

The issue of personal data protection is also closely related to the criminal law enforcement process. On the one hand, law enforcement officials need access to personal data to investigate crimes, such as money laundering or terrorism. However, on the other hand, uncontrolled access has the potential to violate citizens' privacy rights. Therefore, clear regulations are needed regarding the extent to which officials can access personal data, the procedures they must follow, and the oversight mechanisms in place. Without clear regulations, law enforcement officials could be tempted to abuse their authority, while the public lacks assurance that their data is used only for legitimate purposes.

The urgency of personal data protection is further strengthened when linked to the theory of legal protection. According to Ismatullah (2014), legal protection is a guarantee provided by the state to prevent individual rights from being violated, both through preventive and repressive measures. Preventive protection is realized through regulations prohibiting data misuse, while repressive protection is realized through criminal sanctions, compensation, and restitution for victims when violations have already occurred. Within this framework, the Personal Data Protection Law is seen as a strategic step to strengthen both dimensions, with the hope that victims of personal data leaks or falsification will no longer be left to struggle alone.

The victimology approach also provides an important perspective. Sahetapy (1987) stated that victims are often the most disadvantaged yet receive the least attention in the criminal justice system. In cases of leaked or falsified personal data, victims suffer economic, social, and psychological losses. They can lose access to their accounts, be accused of illegal transactions, and even experience social pressure due to their identity being misused. Therefore, victim protection must be a primary focus of all legal policies. In other words, the law must not only prosecute perpetrators but also ensure reparation for victims.

The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is inextricably linked to global developments that position personal data as a strategic asset. Personal data now has high economic value because it can be used for commercial, political, and criminal purposes. Large companies frequently collect data for market analysis, while irresponsible parties misuse it for fraud or identity manipulation. In this context, the PDP Law affirms that personal data is a fundamental human right that must be protected. Article 4 of the PDP Law states that everyone has the right to protection of their personal data, including the right to confidentiality, access, correction, and deletion of data. With this provision, the state places personal data on a par with other fundamental rights such as the right to security or privacy.

The need for specific regulations is even more pressing given the reality that data breaches often lack clear accountability mechanisms. Prior to the PDP Law, when large-scale data breaches, such as those involving telecommunications customers, occurred, victims struggled to seek compensation. Law enforcement officials were also limited to using general articles of the Criminal Code or the Electronic Information and Transactions Law (UU ITE). As a result, many cases ended without legal certainty. Nurul Qamar (2017) emphasized that modern criminal law must not only regulate sanctions but also ensure the protection of victims. With the enactment of the PDP Law, it is hoped that a paradigm shift will occur, ensuring that victims of data breaches have a clear right to demand accountability.

The link between personal data protection and criminal law enforcement also presents a dilemma. Law enforcement officials often require access to personal data during investigations. For example, to investigate a corruption case, officials may need to trace an individual's personal account transactions. However, this access must

be conducted legally, measured, and monitored to avoid violating privacy rights. Ismatullah (2014) states that true legal protection is only achieved when there is a balance between the public interest in upholding the law and the individual's interest in protecting their personal rights. Without this balance, the legal system can become an instrument of repression.

Furthermore, from a human rights perspective, personal data is viewed as an integral part of human dignity. Khaila (2024) asserts that digital privacy is the new face of human rights protection in the modern era. Countries that fail to protect their citizens' personal data are deemed to have failed to fulfill their constitutional and international obligations. This was also emphasized in the General Assembly Resolution on the Right to Privacy in the Digital Age (2013), which called on UN member states to ensure that privacy rights are respected in the use of digital technology. Thus, the PDP Law is not only relevant domestically but also fulfills Indonesia's obligations internationally.

However, the existence of the PDP Law does not automatically solve the problem. The biggest challenge lies in its implementation. Many institutions in Indonesia, both government and private, do not yet have adequate data security systems. Data breaches continue to occur even though the PDP Law is in effect. This demonstrates that regulations without consistent oversight and enforcement will become meaningless legal texts. Soedjono (2008) emphasized that law must be viewed as a living tool in society, not simply a written rule. Therefore, the effectiveness of the PDP Law will depend heavily on the extent to which officials, institutions, and the public collectively comply with and implement it.

In addition to institutional factors, public digital literacy is also a crucial aspect in the success of personal data protection. Many data breaches stem from individual negligence, such as readily providing copies of ID cards, passwords, or other personal information. The Personal Data Protection Law (PDP) provides individuals with the right to refuse unauthorized use of their personal data. Low legal awareness often leads to this right going unused. Therefore, in addition to law enforcement, public education must be an integral part of any personal data protection strategy. By increasing public awareness, the risk of data breaches and identity theft can be significantly reduced (Sahetapy, 1987).

Given all of this, it is clear that personal data protection is no longer an option but a necessity in the Indonesian legal system. This introduction demonstrates that personal data protection is a constitutional issue, a fundamental human right, and a challenge under modern criminal law. The state has an obligation to ensure that its citizens' personal data is not misused, either by individuals or institutions. The ITE Law and the Personal Data Protection Law provide a more robust legal framework, although their implementation still faces many obstacles. Therefore, this research is based on the belief that personal data protection must be a top priority in national legal development, particularly in the context of fair and victim-oriented criminal law enforcement.

II. RESEARCH METHODS

This study uses a normative juridical approach with an emphasis on the analysis of relevant primary, secondary, and tertiary legal materials, particularly those related to personal data protection in the context of criminal law enforcement. The normative approach was chosen because the issues studied focus on positive legal norms, both those contained in the constitution, the Criminal Code, the ITE Law, and the PDP Law, as well as legal doctrine and expert views. Data were collected through a library study by reviewing literature, journals, and international legal instruments related to the right to privacy and personal data protection. The analysis was conducted qualitatively descriptively to describe, interpret, and critique the effectiveness of regulations in providing legal protection for victims, while simultaneously identifying existing weaknesses as a basis for recommendations for legal reform (Barda Nawawi, 2000; Nurul Qamar, 2017).

III. RESULTS AND DISCUSSION

A. Literature review

A literature review in legal research serves to provide a strong conceptual foundation for framing the analysis. Regarding the issue of personal data protection in criminal law enforcement, several important theoretical frameworks exist, including an overview of criminal law enforcement and theories of personal data protection that are currently developing in line with the right to privacy in the digital age.

First, criminal law enforcement is essentially understood as a series of state efforts to control and combat crime through criminal law instruments. Barda Nawawi Arief (2000) outlines that criminal law enforcement occurs in three stages: the formulation stage (legislative policy), the application stage (judicial and executive policy), and the execution stage (administrative policy). The formulation stage is the lawmaker's effort to formulate clear and enforceable rules, the application stage is the implementation of the rules by law enforcement officials, while the execution stage is the implementation of court decisions. These three stages demonstrate that criminal law enforcement does not stop at the text of the law but must be realized in consistent practice. In the context of personal data protection, these three stages are important because regulations often exist, but their implementation and execution are weak.

Second, personal data protection is understood as part of legal protection for human rights. Personal data is considered a fundamental right because it concerns human integrity and dignity. According to Ismatullah (2014), legal protection has preventive and repressive dimensions. Preventive means preventing violations through a proper system, while repressive means providing redress once a violation has occurred. In the case of personal data, preventive protection is realized through regulations requiring data controllers to maintain information security, while repressive protection is realized through sanctions for perpetrators of data leaks and compensation mechanisms for victims.

Personal data protection is also closely linked to the right to privacy under international law. UDHR Article 12 and ICCPR Article 17 affirm that no one shall be subjected to arbitrary interference with his or her privacy, family life, or correspondence. This principle was further developed in the General Assembly Resolution on the Right to Privacy in the Digital Age (2013), which emphasized that privacy must be respected in the use of modern technology. This means that personal data protection is the new face of privacy protection. This is reinforced by Khaila (2024), who stated that in the digital age, personal data protection is not merely an administrative necessity but is at the heart of human rights protection itself.

The victimology literature also provides an important perspective on protecting victims of personal data breaches. Sahetapy (1987) emphasized that victims of crime are often the most disadvantaged yet receive the least attention. In the context of data breaches, victims can suffer economic, social, and even psychological losses. They may lose money due to data-based fraud, suffer reputational damage, or live with anxiety due to the misuse of their identity. Therefore, the victimology literature review emphasizes that victims must be placed as the primary subjects of legal protection, not simply objects neglected after the perpetrator is punished.

Furthermore, modern criminal law doctrine also outlines the importance of balancing individual interests with the public interest. According to Nurul Qamar (2017), criminal law should not only prioritize punishment but also ensure legal certainty and victim protection. In cases of personal data breaches, the state does have an interest in maintaining national security, but the individual's interest in data protection should not be sacrificed. This balance requires clear regulations regarding the limits of law enforcement officials' authority to access personal data during investigations.

Soedjono (2008) adds a sociological perspective that law should not be viewed merely as text, but must also function within society. In the context of personal data protection, this means regulations must be effectively implemented by institutions and understood by the public. If regulations exist only on paper, while authorities are reluctant to take action against violations and the public is unaware of their rights, personal data protection will be difficult to achieve. In other words, the effectiveness of law depends not only on written norms but also on legal awareness and the legal culture that exists within society.

The literature review also reveals a close relationship between personal data protection and criminal law enforcement in the digital age. Authorities require personal data to investigate crimes, but such access must be conducted in accordance with legal procedures to avoid violating individual rights. This creates a dilemma referred to in the literature as the privacy versus security dilemma. On the one hand, the state needs to maintain public security by accessing data; on the other, citizens have the right to protect their personal data. This dilemma can only be addressed through clear regulations, transparency in investigative procedures, and effective oversight mechanisms.

Thus, this literature review demonstrates that personal data protection in the context of criminal law enforcement must be understood multidimensionally. Criminal law enforcement theory (Barda Nawawi Arief, 2000) provides a framework for policy stages, legal protection theory (Ismatullah, 2014) emphasizes the balance between prevention and repression, victimology theory (Sahetapy, 1987) emphasizes victim protection, and a human rights perspective (Khaila, 2024) positions personal data as a fundamental right. Meanwhile, Nurul Qamar (2017) and Soedjono (2008) emphasize the need for legal certainty and the functioning of law in society. All of this literature forms a solid theoretical foundation for the analysis of personal data protection in criminal law enforcement in Indonesia.

B. Regulations on Personal Data Protection in Criminal Law Enforcement in Indonesia

Personal data protection in criminal law enforcement is an issue that relates not only to technical administrative aspects but also to legal philosophy and respect for human rights. In Indonesia, this issue is becoming increasingly relevant with the rise in data breaches in various sectors, from public services and healthcare to finance and digital applications. Personal data, which should be protected, often becomes the object of exploitation, both for commercial and criminal purposes. In such situations, the state is required to provide clear legal protection.

Normatively, the constitutional basis for personal data protection can be found in the 1945 Constitution. Article 28G paragraph (1) affirms the right of every person to protection of themselves, their families, their honor, their dignity, and their sense of security. Article 28D paragraph (1) also states that every person has the right to recognition, guarantees, protection, and fair legal certainty. These two articles form the constitutional basis that personal data protection is an integral part of human rights. In other words, when a person's personal data is misused, it is not only administrative rights that are violated, but also the constitutional rights of citizens (Khaila, 2024).

At the international level, similar provisions can be found in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Both guarantee the protection of individual privacy from arbitrary interference. Indonesia, as a state party to the ICCPR, is obliged to adjust its national laws to align with these international standards. In this context, personal data protection is not only a domestic issue but also an international responsibility that must be fulfilled by the state.

Prior to the enactment of the Personal Data Protection Law (PDP Law), data protection in Indonesia was still regulated partially. Several sectoral laws did address specific aspects, such as the Electronic Information and Transactions (ITE) Law, the Population Administration Law, the Banking Law, and the Health Law. However, this partial nature created a legal vacuum when cross-sectoral data breaches occurred. For example, in the case of a telecommunications customer data breach, it was difficult to determine who was responsible and what redress mechanisms the victim could pursue. Barda Nawawi (2000) emphasized that weaknesses in legal formulation would result in weak law enforcement during the application and execution stages.

The ITE Law, first enacted in 2008, does provide a legal basis for prosecuting a number of data breaches, for example in Article 30 concerning illegal access or Article 35 concerning electronic data manipulation. However, the ITE Law places more emphasis on criminalizing perpetrators than protecting victims. Ismatullah (2014) noted that the ITE Law tends to be repressive without a clear compensation mechanism for victims. Thus, although the ITE Law can be used to prosecute perpetrators of data falsification or data leaks, victims still do not receive adequate redress.

This situation prompted discussions on the Personal Data Protection Bill (PDP Bill) in 2012. After a lengthy process, the regulation was finally ratified in 2022 as Law Number 27 of 2022 concerning Personal Data Protection. This law marked a historic milestone, as it was the first time Indonesia had comprehensive regulations regarding personal data protection. Article 4 of the PDP Law affirms the rights of data subjects, including the right to confidentiality and the right to access data, correct, update, delete, and even stop the processing of personal data. This provision strengthens the position of data breach victims, providing them with a legal basis to assert their rights.

The PDP Law also regulates the obligations of data controllers. Article 16 states that data controllers are obliged to maintain the security of personal data from unlawful processing interference. Article 18 emphasizes the data

controller's obligation to process data in a limited, relevant, and legitimate manner. In the event of a violation, Articles 57 and 67 provide a basis for victims to demand accountability, while Articles 69 and 70 regulate criminal and administrative sanctions for perpetrators of data misuse. Thus, the PDP Law clarifies the legal standing for both victims and perpetrators.

However, the implementation of the PDP Law in the context of criminal law enforcement still faces several obstacles. First, technical issues related to digital forensics. Investigating data breaches requires specialized skills to trace data flows, identify perpetrators, and ensure the integrity of digital evidence. Without these skills, law enforcement officials will struggle to prove criminal acts. Second, there are issues with inter-agency coordination. Data breaches can involve both government and private institutions, but accountability mechanisms are often unclear. Nurul Qamar (2017) emphasized the need for detailed derivative regulations to prevent shifting responsibility between institutions.

Third, the issue of public literacy. Many data breach victims are unaware of their rights under the PDP Law, and therefore do not pursue legal action. This demonstrates that legal protection will only be effective if accompanied by increased public awareness. Sahetapy (1987) cautions that without a victimological perspective, victims will continue to be disadvantaged without redress. In the context of data breaches, legal protection must include compensation mechanisms and psychological rehabilitation for victims, who often experience trauma due to identity theft.

Furthermore, the relationship between personal data protection and criminal law enforcement also presents a dilemma. Authorities need data to investigate crimes, but access must be restricted to prevent violations of citizens' privacy. Without clear regulations, authorities' authority can be abused. Ismatullah (2014) emphasized the need for a balance between public interest and individual interests. The PDP Law attempts to address this dilemma by regulating the limits of data processing by authorities, but its implementation still requires strict oversight.

Given these developments, it can be concluded that the regulation of personal data protection in Indonesian criminal law has undergone significant evolution. Initially only partially regulated through the Criminal Code and the Electronic Information and Transactions Law, a comprehensive Personal Data Protection Law (PDP) now exists. However, sound regulation must be accompanied by consistent implementation. Without it, victims of data breaches will remain vulnerable. Therefore, strengthening the capacity of authorities, inter-institutional coordination, and increasing public awareness are key to achieving real legal protection.

C. The Urgency of Ratifying the PDP Law

The urgency of ratifying the Personal Data Protection Law (PDP Law) cannot be separated from the context of information technology developments and the need for human rights protection in the digital age. For years, prior to the PDP Law's enactment in 2022, Indonesia relied solely on partial provisions from the Electronic Information and Transactions (ITE) Law and a number of sectoral regulations. This fragmented regulation has created numerous problems, particularly when large-scale data breaches occur. These cases demonstrate the vulnerability of Indonesians to personal data misuse, while existing legal instruments have been unable to provide optimal protection.

One of the main reasons for the urgency of ratifying the Personal Data Protection Law is the increasingly strategic position of personal data in modern life. Personal data is no longer merely viewed as an administrative record but has become an economic, political, and social asset. Large companies use personal data for business purposes, while certain parties misuse it for fraud, manipulation, and even identity forgery. Khaila (2024) emphasized that personal data is the new face of human rights in the digital era. Without strong protection, a person's right to privacy can easily be violated, even without the data owner being aware of it.

The urgency of the PDP Law also arises from the increasing frequency and scale of data leaks in Indonesia. In recent years, the public has been repeatedly shaken by news of data leaks involving millions of users. These cases have involved data from mobile operators, banking customers, and even patient data in the healthcare sector. This situation has caused public unrest and undermined public trust in the institutions that are supposed to safeguard their data. Without specific regulations, it is difficult to determine who is responsible when leaks occur, and victims often lack redress. Barda Nawawi (2000) stated that weak legal formulation will directly impact public protection. Therefore, the ratification of the

PDP Law is urgently needed to address this legal gap.

Furthermore, the PDP Law is crucial in providing legal certainty regarding the rights and obligations of data subjects and data controllers. Article 4 of the PDP Law affirms that everyone has the right to protection of their personal data, including the right to know the purpose of data collection, the right to access data, and the right to correct and delete data. This provision positions data subjects as the legitimate owners of their personal information, while data controllers have only limited rights to process the data in accordance with their consent. Ismatullah (2014) states that legal protection must place individuals at the center, not merely objects of the legal system. With the PDP Law, the public has a clear legal basis to protect themselves from data misuse.

The urgency of the PDP Law is also related to harmonizing Indonesian law with international standards. Several countries already have personal data protection regulations, such as the European Union's General Data Protection Regulation (GDPR), which serves as a global reference. Without such regulations, Indonesia risks being left behind and perceived as not serious about protecting its citizens' rights. This could hinder international cooperation, particularly in the areas of digital trade and cybersecurity. With the PDP Law, Indonesia demonstrates its commitment to fulfilling its international obligations, including as a party to the ICCPR, which guarantees the right to privacy. Nurul Qamar (2017) emphasized that legal certainty aligned with global standards will increase international trust in Indonesia.

From a victimology perspective, the urgency of the PDP Law is also evident in the need to provide redress for victims of data breaches. Prior to the PDP Law, victims could only rely on civil or criminal law mechanisms, which were often lengthy and complicated. With the PDP Law, victims have a legal basis to demand direct accountability from data controllers. Article 57 of the PDP Law even grants victims the right to compensation. Sahetapy (1987) emphasized that the criminal justice system must be victim-oriented. The presence of the PDP Law demonstrates the state's efforts to position data breach victims as the primary subjects of legal protection.

Another urgent need is to encourage better data governance. Articles 16 and 18 of the PDP Law require data controllers to maintain the security of personal data and process data only for legitimate purposes. Without this obligation, institutions often neglect data security, resulting in continued data leaks. Soedjono (2008) emphasized that law is not merely a text, but also an instrument for regulating social behavior. With the PDP Law, it is hoped that there will be a shift in legal culture, where data controllers will be more careful and responsible in managing public data.

Nevertheless, the challenges of implementing the PDP Law remain significant. First, there is the limited capacity of law enforcement officials, both in the technical aspects of digital forensics and in understanding the substance of the new law. Second, there is weak public awareness of the importance of protecting personal data. Many individuals still readily share photocopies of their ID cards or personal data without realizing the risks. Third, there is the need for detailed implementing regulations to ensure the PDP Law can be truly operationalized. Without these steps, the PDP Law risks becoming a regulation that only exists on paper.

However, despite implementation challenges, the passage of the Personal Data Protection Law remains a crucial step forward. This law not only provides legal certainty for data breach victims but also affirms Indonesia's position as a nation that respects human rights in the digital age. With the Personal Data Protection Law, the government demonstrates its commitment to protecting citizens from the threat of data misuse, strengthening digital security, and increasing public trust in the law and state institutions.

Thus, the urgency of ratifying the Data Protection and Protection Act (PDP) can be summarized in several aspects. First, to close the legal gap that has left data breach victims unprotected. Second, to provide legal certainty for data subjects and data controllers. Third, to align national law with international standards. Fourth, to place victims at the center of legal protection. Fifth, to encourage a more responsible legal culture in data governance. All these aspects demonstrate that the PDP Act is not simply a new legal instrument, but also a foundation for human rights protection in the digital age.

Upon closer examination, the urgency of ratifying the Personal Data Protection Law (PDP) relates not only to individual protection but also to public trust in the rule of law. In the theory of a rule of law, one of the main indicators is the guarantee of certainty and protection of citizens'

rights (Ismatullah, 2014). When personal data leaks occur repeatedly without a recovery mechanism, the state's authority is questioned. The public will doubt the government's commitment to fulfilling its constitutional obligations. Therefore, the PDP Law must be seen not merely as a technical regulation, but as a symbol of the state's presence in fulfilling its constitutional mandate to protect the dignity of its citizens.

On the other hand, the ratification of the PDP Law is also crucial within the framework of national digital economic development. Indonesia's rapidly growing digital economy would be impossible without consumer trust. Consumers will be reluctant to engage in electronic transactions if they feel their personal data is insecure. Barda Nawawi (2000) reminds us that criminal law, in addition to its repressive function, also has a preventive function, namely preventing violations and providing a sense of security to the public. In the context of the digital economy, the PDP Law serves a preventive function by encouraging companies to be more responsible in managing data, so that the public feels safe conducting online transactions.

Furthermore, the Personal Data Protection Law must also be understood as an instrument to strengthen Indonesia's digital sovereignty. Citizens' personal data is a strategic resource that cannot be arbitrarily controlled by foreign parties. Without strict regulations, Indonesian citizens' data is at risk of being controlled by global corporations operating across borders. This is not only a privacy issue but also concerns national sovereignty. From an international legal perspective, data protection is now part of digital sovereignty, determining a country's position in global geopolitics. With the Personal Data Protection Law, Indonesia demonstrates that it has full authority over its citizens' data and is not subject to the domination of transnational corporations.

From a victimology perspective, the PDP Law is also important because it restores the balance between perpetrators and victims. Until now, victims of data breaches have often been denied the opportunity to seek compensation. For example, in the case of the data breach involving millions of digital platform customers, victims were only given an apology without any concrete compensation. Sahetapy (1987) emphasized that victims should not be viewed as passive recipients of the consequences, but rather as active participants whose rights must be restored. Article 57 of the PDP Law, which grants victims the right to restitution, is an implementation of this principle of victimology.

Furthermore, the PDP Law is also relevant for strengthening the legitimacy of law enforcement officials. Without specific regulations, officials often use the loose provisions of the ITE Law to prosecute data breaches. This has drawn criticism due to the potential for abuse. With the PDP Law, officials have a clearer legal basis, enabling them to be held legally accountable for their actions. This is crucial for maintaining public trust and preventing potential abuse of authority. Soedjono (2008) emphasized that the law will only be effective if it is enforced fairly and transparently, not arbitrarily.

Another urgency can be seen from the aspect of distributive justice. Personal data is now viewed as a "digital asset" with economic value. Many companies exploit personal data for substantial profits, but there is no mechanism for sharing these profits with data owners. The Personal Data Protection Law (PDP) aims to correct this injustice by giving individuals control over their own data. By requiring consent for data processing, individuals are given a stronger bargaining position. Nurul Qamar (2017) believes that sound legal protection governs not only the relationship between the state and individuals but also the relationship between individuals and corporations.

Equally important, the PDP Law also addresses the phenomenon of surveillance capitalism, the practice of massive commercialization of personal data by technology companies. This practice is dangerous because it erodes individual privacy and freedom. Without the PDP Law, Indonesia risks becoming a large market exploited by global corporations without meaningful protection for its citizens. With the PDP Law, the state asserts its regulatory position to balance power between individuals and corporations. This aligns with Khaila's (2024) view that the right to privacy must be positioned as the last bastion in preserving human dignity in the digital age.

With this deeper analysis, it can be emphasized that the urgency of ratifying the PDP Law is not only a technical matter of data protection, but also concerns: (1) the legitimacy of the rule of law, (2) the sustainability of the digital economy, (3) Indonesia's digital sovereignty, (4) the protection of victims as the main subjects of the law, (5) the legitimacy of law enforcement officers, (6) distributive justice in the data

economy, and (7) protection against the dangers of surveillance capitalism. All of these aspects show that the PDP Law is a strategic regulation that not only protects individuals but also strengthens Indonesia's position in the global context.

IV. CONCLUSIONS AND RECOMMENDATIONS

In Law Number 27 of 2022 concerning Personal Data Protection, if there is a failure in Personal Data Protection, Administrative Sanctions will be imposed under Article 57 and Criminal Provisions under Article 67 and Article 69. In the case of criminal acts, Article 70 will be imposed. However, the unclear regulations regarding criminal liability in the event of a failure in Personal Data Protection in Cyber Crimes create legal uncertainty for Legal Subjects.

REFERENCE LISTAN

Barda, NA (2005). Several Aspects of Law Enforcement Policy and Criminal Law Development, Bandung: Citra Adtya Bakti.

Directives (EU) 2016/680 of The European Parliament and of The Council of 27.

Graham Greenleaf. (2011) Global Data Protection Laws, Privacy Laws & Business Special Report.

H Aspan, A Setiawan, ES Wahyuni, A Prabowo, AN Zahara,The Legal Review of the Mechanism for Determining Injury in the Imposition of Antidumping Duties on Uncoated Writing and Printing Paper in Indonesia, Journal of Namibian Studies 34

H Aspan, A Setiawan, ES Wahyuni, A Prabowo, AN Zahara,The Legal Review of the Mechanism for Determining Injury in the Imposition of Antidumping Duties on Uncoated Writing and Printing Paper in Indonesia, Journal of Namibian Studies 34

M Saragih, H Aspan, APU SiahaanViolations of Cybercrime and the Strength of Jurisdiction in Indonesia, The International Journal of Humanities & Social Studies 12 (5), 209-214

H Aspan, A Setiawan, ES Wahyuni, A Prabowo, AN Zahara,Cyber Notary Issues Authority Certificate to Provide Legal Protection in Online SellingJournal of Law and Sustainable Development 11 (10), e1801-e1801

National Human Rights Commission of the Republic of Indonesia, Standard Norms and Regulations Number 5 concerning the Right to Freedom of Opinion and Expression

Mardjono, R. (1994). The Indonesian Criminal Justice System: Viewing Crime and Law Enforcement within the Boundaries of Tolerance, Center for Justice and Legal Service, Jakarta.

M Hutagalung, TR Zarzani,An Implementation of Restorative Justice in Settlement Framework Criminal Acts Fraud and Employment to Provide Useful And Fair Legal Guarantee (Study In Police Regional North...Legal Brief 11 (4), 2148-2154, Academic Paper on the Personal Data Protection Bill

TR Zarzani, B Fitrianto, S Annisa,The Idea of Renewing Terrorism Criminal Law in Indonesia as an Effort to Overcome Terrorism Based on the Justice ValuesInternational Journal of Law Reconstruction 8 (1), 38-55

TR Zarzani, I Ismaidar, W Fahriza,Dimensions of Corporate Crime, International Journal of Law, Crime and Justice 1 (2), 108-113

R Rianto, TR Zarzani, YM Saragih, Legal Responsibilities of Online Media Corporations and Social Media UsersRegarding the Public Sharing of News Containing ITE Crimes, JIIP-Scientific Journal of Educational Sciences 7 (1), 393-398

Samuel, W & Louis, D. B. (1890). "The Right To Privacy", Harvard Law Review.

United Nations General Assembly, Resolution 68/167: "The Right to Privacy in the Digital Age"

Y Yasmirah, F Halawa, S Tandiono, TR ZarzaniCriminal acts of corruption procurement of goods and services of local governments through electronic procurement services (LPSE),Budapest International Research and Critics Institute (BIRCI-Journal

Yulies, T M. (2004). Introduction to Indonesian Law, Jakarta: Sinar Grafika.