IJSSR
International Journal of Social Service and Research

Vol. 4, No. 12, December 2024
e-ISSN: 2807-8691 | *p*-ISSN: 2807-839X

LEGAL VACANCY IN PROTECTION OF VICTIMS OF PERSONAL DATA MISUSE FOR FICTITIOUS BANKING CREDIT

Miftakul Azis, Zudan Arief Fakrulloh
Universitas Borobudur, Indonesia
*e-mail: azizmoeda@gmail.com cclsis@yahoo.com

Keywords

banking, fraudulent credit, legal vacuum, personal data abuse, victim protection

ABSTRACT

Personal data have become a critical issue in the era of global connectivity, where the use of mobile devices such as smartphones and tablets connected to the internet has created an increasingly complex communication network. In recent years, there has been a significant increase in cases of personal data abuse in the banking sector, especially concerning fraudulent loan applications. This study aims to identify the factors that create a legal vacuum in the protection of victims of data abuse. This research adopts a normative legal methodology aimed at examining various legal regulations in Indonesia related to personal data protection. The findings can serve as a foundation for further research aiming at developing comprehensive legal solutions and enhancing victim support mechanisms.

INTRODUCTION

As a result of digitalization, the rapid development of information and communication technology has significantly impacted the processes of collecting, processing, and exchanging personal data. Personal data, such as identity information, health history, shopping preferences, and transaction histories, have become valuable assets for companies, organizations, and governments. However, with the widening access to such data, the risks to individual privacy and security have also increased. Personal data have become a critical issue in the era of global connectivity, where the use of mobile devices such as smartphones and tablets connected to the internet has created an increasingly complex communication network. This situation demands stricter legal protections, as personal data are key elements in safeguarding individual freedoms and dignity, as regulated in Article 1 paragraph (1) of Law Number 27 of 2022 on Personal Data Protection.

The protection of personal data is not only crucial for safeguarding privacy but is also linked to political, spiritual, religious freedoms, and other fundamental rights, such as freedom of expression and the right to privacy (Aftab, 2024b, 2024a; Carolan, 2012; Rascão, 2020; Weber, 2024). Illegal access to personal data can lead to various crimes, including unauthorized wiretapping, banking fraud, and money laundering in cyberspace (Al Zaidy, 2024; Grabosky et al., 2018; Gundur et al., 2021; Kittichaisaree, 2017; Manap et al., 2015). Unauthorized wiretapping usually involves the installation of software or hardware to steal information, while banking fraud and money laundering involve illegal attempts to obtain or transfer funds through cyber banking systems (Brenner, 2010; Khadim et al., 2022; Minnaar, 2014; Pomerleau & Lowery, 2020; Sabillon et al., 2016). These crimes underscore the urgent need for better legal protections to prevent privacy violations and abuse of personal data.

The constitutional right to personal protection is regulated in Article 28G paragraph (1) of the 1945 Constitution, which covers the right to personal, family, honor, dignity, and property protection. With the advancement of information technology, this personal right must be interpreted more broadly, encompassing more sensitive privacy rights. Protection for witnesses and victims in criminal acts is stipulated in Law Number 31 of 2014 on Witness and Victim Protection, which guarantees their rights

based on the principles of protection and legal certainty. However, in the context of economic losses due to criminal acts, particularly in cases of personal data abuse in banking transactions, there is a legal vacuum. The protection of victims' economic rights is not clearly regulated, often leaving them without adequate legal protection in these cases.

In recent years, there has been a significant increase in cases of personal data abuse in the banking sector, especially concerning fraudulent loan applications. Personal data that are leaked or stolen are often used to apply for loans without the knowledge of the data owners, leading to substantial losses for the victims. Reports from the Financial Services Authority (OJK) and various consumer protection agencies indicate that these cases tend to increase alongside the development of digital technologies that facilitate illegal access to personal information.

For example, in 2023, several reports emerged regarding major banks in Indonesia related to fraudulent loan cases involving the abuse of customer personal data. Cybercriminals exploit data leaks through digital platforms or weak networks to access customer information, such as identity numbers, bank accounts, and other financial data. According to the Indonesian Fintech Association (AFTECH), over 1,000 similar cases were reported in the past year, highlighting the large scale of this threat. Data from the Consumer Protection Agency for the Financial Services Sector (LPKJ) revealed that more than 70% of personal data abuse cases in Indonesia involved illegal financial transactions, including fraudulent loans.

Victims of personal data abuse in fraudulent loan applications often face serious consequences, both financially, reputationally, and psychologically. Financially, victims may bear the burden of debts they never applied for. The loans taken out in the victims' names must be repaid, or they may be recorded as problematic customers in the banking system, affecting their credit score and ability to access future loans. In some cases, victims may also incur additional costs to prove that they are victims of fraud, such as paying for legal services or conducting independent audits of their banking transactions.

The impact on victims' reputations is also significant. Their good name can be tarnished, especially when information about defaulted loans or unpaid debts circulates among financial institutions. This can complicate victims' access to other financial services, such as opening new accounts or applying for other legitimate loans. Moreover, they often face legal problems, where they must prove that the loans were applied for fraudulently without their knowledge. This burden of proof typically takes a long time, requiring comprehensive evidence and causing tremendous psychological stress.

Psychologically, victims often experience stress, anxiety, and fear due to their situation. The uncertainty surrounding the resolution of their problems, coupled with the financial burden, exposes victims to a higher risk of mental health issues. Some victims even lose trust in the banking system and become reluctant to use digital services, which hinders their ability to transact in a technology-dependent financial era.

Although Indonesia has several regulations related to personal data protection, such as Law Number 27 of 2022 on Personal Data Protection and Law Number 19 of 2016 on Electronic Information and Transactions (ITE Law), a legal vacuum can still be clearly seen in protecting victims of personal data abuse, particularly in the banking sector. The existing laws tend to focus more on general regulations regarding data protection and penalties for violators but have not comprehensively provided adequate protection for victims of data abuse suffering financial losses due to fraudulent loans or other cybercrimes.

In the Personal Data Protection Law, data protection indeed becomes a primary concern; however, this regulation emphasizes the obligations of data controllers in maintaining the confidentiality and security of data. The law is still minimal in detailing recovery mechanisms for victims whose data have been abused. Meanwhile, the ITE Law focuses more on cybercrime in general and has yet to specifically regulate compensation or recovery mechanisms for individuals who have suffered due to data abuse in financial transactions, especially in banking. As a result, victims experiencing losses from fraudulent loans often do not have a clear pathway to seek compensation or obtain effective legal protection.

In the banking sector itself, banking regulations have not fully provided comprehensive protection for customers who are victims. Bank Indonesia and the Financial Services Authority (OJK) regulate data security and the obligations of banks to maintain customer privacy, but there is still no specific mechanism obligating banks to compensate victims for the losses incurred due to personal data abuse used to apply for fraudulent loans. The recovery process for victims is usually complicated and time-

consuming, while the accountability of banks for the losses incurred is not clearly regulated. This vacuum creates uncertainty for victims, especially regarding their rights to compensation or recovery.

The current regulations still fail to fill the gaps in protection for victims of personal data abuse in the banking sector. There is an urgent need for regulations that are more specific and clear, both in terms of the responsibilities of banking parties and recovery mechanisms for victims, to ensure justice and adequate legal protection for individuals harmed by fraudulent loans and similar crimes.

This study aims to identify the factors causing the legal vacuum in the protection of victims of personal data abuse in the banking sector. The research contributes significantly to the understanding of personal data protection within the banking sector by identifying the factors that create a legal vacuum affecting victims of data abuse. By analyzing the current regulatory landscape and pinpointing specific gaps in legal protections, the study sheds light on the vulnerabilities faced by individuals in the banking system. This contribution is crucial for informing policymakers, legal practitioners, and stakeholders about the inadequacies in existing frameworks and the need for stronger regulations to safeguard personal data. Additionally, the findings can serve as a foundation for further research aimed at developing comprehensive legal solutions and enhancing victim support mechanisms. Ultimately, this research aims to promote a more robust legal environment for personal data protection, thereby fostering greater trust in the banking sector and improving overall data security practices.

METHODS

This research adopts a normative legal methodology aimed at examining the legal rules applicable to the protection of victims of personal data abuse in cases of fraudulent banking loans. This method emphasizes the analysis of legal norms found in legislation and relevant legal concepts, incorporating both legislative and conceptual frameworks. The legislative approach is utilized to examine various legal regulations in Indonesia related to personal data protection and the safeguarding of victims of banking crimes. Regulations reviewed include Law Number 27 of 2022 on Personal Data Protection, Law Number 19 of 2016 on Electronic Information and Transactions, and banking regulations issued by the Financial Services Authority (OJK) and Bank Indonesia. The conceptual approach aids in understanding concepts related to privacy rights, consumer protection, and legal accountability in banking transactions, clarifying the legal vacuum affecting victims of fraudulent loans.

The research relies on secondary data obtained from various written sources, including laws, regulations, legal journals, books, and other pertinent documents. Data collection techniques involve two primary methods: interviews and document studies. Interviews are conducted with competent informants, such as legal practitioners, banking experts, and regulatory authorities, to gain insights into the implementation and legal vacuum in victim protection. Document studies are employed to review and analyze legally relevant materials related to the research topic. For data analysis, a deductive logic approach is used, enabling the researcher to analyze applicable legislation and legal concepts to draw conclusions about the existence of legal vacuums in victim protection. This process begins by identifying generally applicable legal rules, followed by an in-depth analysis of gaps in their application concerning cases of personal data abuse for fraudulent loans. The results of this analysis inform specific policy recommendations to address the identified legal vacuum.

RESULTS

The Legal Vacuum in Protecting Victims of Personal Data Abuse in the Banking Sector, Specifically in Cases of Fraudulent Loan Applications

Personal data can be defined as information that includes various records like health, education, and employment records that are stored in relevant systems. This personal data is part of an individual's privacy rights, which encompasses three main aspects: first, the right to enjoy personal life without disturbance; second, the right to communicate with others without surveillance; and third, the right to control access to personal information and individual data. In this case, the personal data of victims used to obtain fraudulent loans clearly demonstrates a violation of these rights. The identity cards used without the owners' knowledge for fraudulent loans represent a significant form of personal data abuse.

Fraudulent loans refer to loans given by banks to customers using invalid or false information. In this case, the data of customers, which should be protected, are exploited by others for personal gain without the knowledge or consent of the data owner. When victims' personal data are misused for the benefit of fraudsters, they not only suffer financial loss but also face broader negative impacts, including tarnished reputations and complex legal issues.

According to Law Number 31 of 2014 concerning Witness and Victim Protection, victims' rights are regulated in Article 5 paragraphs (1) and (2). Unfortunately, rights pertaining to economic interests are not explicitly mentioned in these regulations. This also reflects deficiencies in various other relevant laws, such as Law Number 23 of 2006 concerning Population Administration and Law Number 27 of 2022 concerning Personal Data Protection. In this context, victims' economic rights are crucial as they serve to protect individuals from financial losses arising from personal data abuse.

Several important rights should be afforded to victims affected by personal data abuse in cases of fraudulent loans:

1. Victims have the right to legal protection against the illegal use of personal data, including the right to report crimes and receive legal assistance to address the losses incurred.
2. They have the right to compensation or financial recovery due to the criminal acts committed against them.
3. Victims have the right to rectify credit records that may have been tainted by the misuse of their data, as a means of restoring their credit reputation.
4. Victims are also entitled to additional protections to prevent the recurrence of personal data abuse, such as enhanced data security oversight.

Law Number 31 of 2014 is an important regulation that refines Law Number 13 of 2006 regarding Witness and Victim Protection. This law was enacted as a form of guarantee for the protection of witnesses and victims who play critical roles in the criminal judicial process. Through this law, it is hoped that witnesses and victims can provide testimony freely without fear or threat that could obstruct the revelation of criminal acts. Legal protection for the public is a state obligation, which is part of human rights regulated both in national constitution and international human rights instruments ratified by the Indonesian government.

The importance of this legal protection underscores the primary reason for the enactment of Law on Witness and Victim Protection. This law explicitly defines who is entitled to protection, namely witnesses and victims of criminal acts. By providing a clear legal framework, this law aims to ensure the rights of victims in various contexts. The main focus of this law is on physical protection, security, and psychological support for witnesses and victims. However, despite the attention to these aspects, the law does not delve deeply into the protection of victims' economic rights.

A major shortcoming of Law Number 31 of 2014 is the absence of specific provisions regarding the protection of victims' economic rights, especially within the context of banking transactions. While the law addresses criminal threats against perpetrators of criminal actions, it fails to establish a clear mechanism for addressing the economic losses experienced by victims in cases involving fraudulent loans. Fraudulent loan cases often entail personal data abuse and financial fraud, yet this law does not provide clear guidelines on how to manage and protect victims in such situations.

In terms of restitution, this law provides the possibility for victims to seek compensation through judicial proceedings. However, Law on Witness and Victim Protection does not explicitly regulate the process for claiming compensation or restitution for victims of banking fraud. This can potentially cause confusion for victims wishing to recover their losses. Moreover, the law stipulates that only directly harmed victims are entitled to compensation, while victims indirectly harmed, such as those related to economic interests, do not receive adequate attention.

From the existing provisions, it is evident that there is no definitive formulation concerning economic interests in Law Number 31 of 2014. This indicates that economic rights are not included within the scope of regulation of this law. In other words, this law has yet to provide comprehensive legal protection for victims of personal data abuse in cases of fraudulent loans, which may lead to significant financial losses.

The legal vacuum in protecting victims of personal data abuse, particularly within the context of banking fraud, is an urgent issue that needs immediate attention. Despite the enactment of various laws, such as Law on Witness and Victim Protection and Law on Personal Data Protection, several gaps remain that render the legal protections for victims ineffective. One of the primary deficiencies is the lack of provisions specifically regulating the economic rights of victims who suffer losses due to personal data misuse. Many victims find themselves in situations where their identities are used without authorization to apply for fraudulent loans but have no clear legal avenues to claim compensation or restitution for their losses.

Moreover, existing regulations typically focus more on physical and psychological protection for witnesses and victims of criminal offenses without adequately addressing the vital economic aspects.

This results in victims often feeling neglected and without the necessary support to restore their rights. In many cases, they might not know how to report the violations they have experienced or what steps to take to protect themselves from further abuses. Consequently, victims face the risk of losing their credit reputations, encountering difficulties in obtaining future loans, and experiencing greater financial hardships without an adequate legal mechanism to seek recovery.

This legal vacuum also reflects the lack of operational guidelines for managing cases of personal data abuse in banking transactions. Without clear guidelines, law enforcement and banking institutions often struggle to deal with these complex cases, exacerbating the situation for victims, who are already trapped in detrimental circumstances without certainty regarding how their rights will be protected.

The existing legal vacuum pertaining to the protection of victims of personal data abuse, especially within banking transactions, can have severe implications for individuals who fall victim. One of the most apparent effects is the loss of public trust in the banking system and financial institutions. When individuals feel that their personal data can be misused without any legal repercussions for perpetrators, it creates an atmosphere of uncertainty and insecurity. Victims who lack adequate protection tend to feel alienated and vulnerable, thereby reducing their participation in banking and financial activities, which can negatively impact overall economic stability.

Additionally, the legal vacuum poses significant challenges for victims seeking recovery from their incurred losses. Without clear regulations regarding victims' economic rights, affected individuals often do not know what steps to take to protect themselves or seek compensation. They may become entangled in complex and prolonged legal processes, during which their rights are frequently not acknowledged. This lack of clarity not only adds psychological burdens for victims but also creates a scenario in which perpetrators feel safe continuing their criminal activities, knowing that the likelihood of facing prosecution or punishment is low.

This legal vacuum also creates systematic injustices. Victims of fraudulent loans and personal data abuse often come from vulnerable societal sectors, such as individuals with low economic backgrounds or limited understanding of their legal rights. Their inability to access legal assistance or support themselves in legal processes may exacerbate existing inequalities in society. This societal stigma not only complicates the victims' situations further but also leads to more extensive individual blame, often viewed as responsible for the problems they experience rather than receiving support and adequate protection.

From a legal perspective, this vacuum highlights gaps in the legal system that can be exploited by irresponsible parties. Unclear definitions and protections regarding personal data allow perpetrators to commit criminal acts without fear of consequences. This has the potential to trigger further data-related crimes, which will be increasingly challenging for authorities to address. In other words, without stringent and clear regulations, cybercrimes, including identity theft and fraud, will continue to rise, ultimately harming individuals and the banking industry as a whole. The consequences of this legal vacuum may also result in losses for the state. When victims do not receive justice, it can lead to skepticism towards the legal and banking institutions. This distrust can deter economic growth and foreign investments, as investors tend to avoid business environments viewed as unstable or risky.

Efforts to Address the Legal Vacuum and Improve Legal Protection for Victims of Personal Data Abuse in the Banking Sector

Legal protection for victims of personal data abuse, particularly in the context of fraudulent loans, is urgently needed given the prevalence of increasingly complex and dangerous fraudulent practices. Fraudulent loans, which are often perpetrated using personal data without consent, not only result in substantial financial harm to individuals but also tarnish their reputations. In situations where a person's identity is misused to apply for loans they did not authorize, victims can find themselves caught in debts that are not their responsibility. This leads to significant losses, both economically and emotionally, which can have long-term impacts on victims' quality of life.

Moreover, the existing legal vacuum in current regulations leaves many victims feeling powerless. Without clear provisions regarding their economic rights and recovery steps, they frequently do not know how to seek compensation or file complaints. This exacerbates their situation as they struggle to clear their names and rectify tainted credit records. In this regard, the urgency to fortify legal protection is not only the responsibility of the government but a necessity to uphold public trust in the banking system.

Given the rapid development of information technology, the risk of personal data abuse in banking transactions continues to rise. Therefore, there is an immediate need to update and adapt existing regulations to align with contemporary challenges. Preventive and curative efforts must be carried out simultaneously to avert abuse and deliver justice to victims. Strengthening regulations and more effective law enforcement will create a safer environment for the public, allowing them to transact without fear of losing their rights.

With the increasing cases of personal data abuse in the banking sector, the strengthening of regulatory frameworks and data protection policies becomes imperative. One of the key steps that can be taken is to revise and update the laws related to personal data protection and the rights of victims. Currently, Law Number 27 of 2022 on Personal Data Protection provides a legal foundation to protect individual data; however, it is inadequate in regulating victims' economic rights in the context of fraudulent loans. Therefore, amendments to this law are necessary to include victims' economic rights more explicitly and comprehensively. Furthermore, Law Number 31 of 2014 on Witness and Victims Protection also needs to be updated by incorporating more specific provisions related to protecting victims harmed by personal data abuse in banking transactions.

In addition to legislative revisions, the development of specific guidelines is also a vital strategy to address these issues. Clear and structured operational guidelines must be established to handle cases of personal data abuse, particularly in fraudulent loan transactions. These guidelines should include detailed procedures on how victims can file for compensation and restitution, as well as processes for restoring their tarnished credit reputations. Furthermore, these guidelines need to provide preventive measures for banks and financial institutions to enhance data security, such as increased oversight and regular audits of their data protection systems.

Such guidelines can serve as essential tools to streamline the complaint process for victims, who often face bureaucratic hurdles when trying to establish themselves as victims of crime. With clear regulations in place, victims will be better protected and not caught in protracted legal processes. These guidelines can also act as a reference for law enforcement, banking institutions, and consumer protection agencies in efficiently and equitably addressing similar cases.

Strengthening regulations and policies on the protection of personal data is an unavoidable step in addressing the evolving technological landscape and the complexities of criminal acts in the banking sector. These reforms are not only aimed at safeguarding the economic rights of victims but also at reinforcing public confidence in the financial system and ensuring that every individual who becomes a victim of personal data crimes receives adequate legal protection.

More stringent law enforcement is one of the essential measures to tackle the issue of personal data abuse in the banking sector. Enhancing the capacity of law enforcement officials through training and provision of adequate resources can assist them in understanding and managing cases related to personal data abuse more effectively. This training should encompass not only legal aspects but also technical knowledge of information technology so that law enforcement can promptly and accurately identify and investigate crimes involving personal data. By fostering a greater understanding, law enforcement is expected to take more proactive measures in preventing and responding to personal data abuse cases.

Moreover, creating a collaboration system between law enforcement agencies and financial institutions is crucial. Through this collaboration, information about potential personal data abuse can be quickly identified and acted upon. Banking institutions can also provide the necessary data and technical support to expedite the investigation process, ensuring that cases related to fraudulent loans are handled swiftly and effectively.

Applying stricter penalties against perpetrators of personal data abuse is also a critical step to establish a deterrent effect. Heavier sanctions, including substantial financial fines and imprisonment, can diminish incentives for individuals or groups considering exploiting others' personal data. With clear and stringent penalties in place, criminals will be more likely to weigh the risks they face before engaging in abusive actions. This will not only protect victims but also reinforce the integrity of the banking sector as a whole. The application of strict sanctions should be complemented by public awareness campaigns and education about individuals' rights related to personal data protection. With sufficient knowledge, the public will become more vigilant about the risks of personal data abuse and more courageous in reporting crimes if they become victims. This can cultivate a more robust culture of data protection within society and enhance public participation in safeguarding personal data.

Public education programs are crucial in raising awareness about individuals' rights regarding personal data protection. Through these programs, individuals can receive clear and comprehensive information about the importance of safeguarding their personal data and the actions they can take if they become victims of abuse. Education can be delivered through various media, such as social media campaigns, seminars, and workshops involving diverse groups, including schools, communities, and civil organizations. With better knowledge, individuals will become more cautious regarding potential risks and be better prepared to protect their personal information.

Moreover, training for banking personnel is also a critical aspect of personal data protection. Bank staff and financial institution employees are on the front lines in handling sensitive customer information. Therefore, providing in-depth training regarding the importance of data protection and victims' rights is essential. This training may include techniques for detecting and preventing data abuse, as well as procedures to follow if a security breach occurs. By enhancing the competence and awareness of banking personnel, it is hoped that there will be a decrease in incidents of data abuse and a more responsive handling of emerging cases.

Building partnerships between the government, the private sector, and civil society organizations is crucial for creating a stronger mechanism of protection for victims of personal data abuse. Through this collaboration, each party can complement one another in efforts to protect personal data. The government can provide regulations and policy support, while the private sector, particularly banks, can ensure the implementation of best practices in data protection. Civil society organizations can act as intermediaries between the public and these institutions, assisting in public education and monitoring the implementation of existing regulations.

Establishing a dedicated task force that includes various stakeholders can also be an effective solution to address personal data abuse issues. This task force can coordinate efforts to tackle data abuse at all levels, ranging from policymaking to handling cases. By involving multiple parties, this special team is expected to provide a more holistic and integrated approach to handle this problem and respond to the dynamics arising from the advancement of information and communication technology.

Providing easily accessible complaint services for victims of personal data abuse is crucial. Such services should be designed so that users can quickly and easily report cases and obtain information about the next steps to take. Well-handled complaints will enable authorities to conduct investigations and take necessary actions, allowing victims to feel they are not neglected or overlooked. Furthermore, implementing free legal assistance programs for financially challenged victims is an important step to ensure that all individuals have access to legal protection. Such legal help will not only assist victims in the legal process but also provide them with the security and support they need to cope with the effects of personal data abuse. With effective complaint mechanisms and adequate legal support, it is hoped that victims of personal data abuse can achieve justice and restore their rights.

Establishing a sustainable monitoring and evaluation system is vital in ensuring the effectiveness of existing regulations and policies regarding personal data protection in the banking sector. This system can encompass the collection of data related to incidents of personal data abuse, their impacts on victims, and the responses from banking institutions and law enforcement. Through regular monitoring, it will be easier to identify weaknesses in existing regulations and areas that need improvement. Evaluations should be conducted periodically and involve various stakeholders, including the government, financial institutions, and civil society organizations, to gain a more comprehensive perspective. The outcomes of this evaluation can inform necessary adjustments, ensuring that regulations and policies protecting personal data remain relevant and effective in addressing new challenges.

Routine reporting is also a critical element in this monitoring process. Mandating banking institutions to regularly report cases of personal data abuse, as well as the steps taken to prevent it, will create transparency and accountability within the sector. Such reports will not only provide an overview of the extent of personal data abuse issues but also assist in assessing the effectiveness of actions taken. With routine reporting, authorities will have an easier time analyzing trends and patterns related to data abuse, allowing them to formulate more proactive policies.

Implementing more advanced security technology in the banking sector is a key step in protecting customers' personal data. As information technology continues to advance, the techniques and tools used to safeguard data must also be updated and upgraded. This may include the use of stronger encryption, two-factor authentication systems, and continuous monitoring of suspicious activities. By

adopting cutting-edge security technologies, financial institutions can reduce the risk of data abuse and provide customers with assurance that their personal information is well-protected.

Incentivizing innovation in data protection is essential in facing the continuously evolving challenges of the digital age. Research and development of innovative solutions can contribute to creating more effective tools and systems for protecting personal data. For instance, the development of artificial intelligence (AI)-based technology could be used for real-time detection and prevention of potential data misuse. Furthermore, collaboration between research institutions, universities, and industry can spur greater innovation in creating responsive and adaptive data protection solutions against emerging threats. Consequently, efforts to protect personal data should not rely solely on regulations and policies but should also hinge on ongoing technological advancements and innovation.

CONCLUSION

The legal vacuum in personal data protection, especially within the banking sector, has become a pressing concern due to the increasing instances of data misuse for fraudulent loans. Current laws, such as the Law on Witness and Victim Protection and the Law on Personal Data Protection, inadequately address the economic rights of victims, focusing primarily on physical and psychological protections. Consequently, many victims lack sufficient restitution and feel unsupported by a legal framework that fails to protect their interests. To remedy this, regulatory revisions should explicitly include victims' economic rights, and operational guidelines for managing data abuse cases in banking must be established. Additionally, enhanced law enforcement, public awareness initiatives, and collaborative efforts among government, private sector, and civil society are critical. Future research should explore comprehensive frameworks to bolster data protection, assess existing laws for gaps, and evaluate the effectiveness of proposed measures in safeguarding victims' rights in the digital landscape.

REFERENCES

Aftab, S. (2024a). Right to Privacy and Freedom of Expression in the Constitution of Pakistan. In *Ius Gentium: Comparative Perspectives on Law and Justice* (Vol. 109, pp. 99–126). Springer. https://doi.org/10.1007/978-3-031-45575-9_4

Aftab, S. (2024b). The Concept of the Right to Privacy. In *Ius Gentium* (Vol. 109). https://doi.org/10.1007/978-3-031-45575-9_3

Al Zaidy, A. (2024). Digital Crimes and Digital Terrorism: The New Frontier of Threats in Cyberspace. *Journal of Information Technology, Cybersecurity, and Artificial Intelligence*, *1*(1), 18–29. https://doi.org/10.70715/jitcai.2024.v1.i1.003

Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Bloomsbury Publishing. https://books.google.co.id/books?id=UIPDEAAAQBAJ

Carolan, E. (2012). The Concept of a Right to Privacy. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1889243

Grabosky, P. N., Smith, R. G., & Wright, P. (2018). *Crime in the Digital Age*. Routledge. https://doi.org/10.4324/9780203794401

Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y.-C., & Mejía, D. D. (2021). Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. *CrimRxiv*. https://doi.org/10.21428/cb6ab371.5f335e6f

Khadim, S., Ali Hassen, O., & Ibrahim, H. (2022). A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies. *Wasit Journal of Computer and Mathematics Science*, *1*(3). https://doi.org/10.31185/wjcm.48

Kittichaisaree, K. (2017). Cyber Crimes. In *Public International Law of Cyberspace. Law, Governance and Technology Series* (pp. 263–293). Springer. https://doi.org/10.1007/978-3-319-54657-5_7

Manap, N. A., Abdul Rahim, A., & Taji, H. (2015). Cyberspace identity theft: An overview. *Mediterranean Journal of Social Sciences*, *6*(4S3). https://doi.org/10.5901/mjss.2015.v6n4s3p290

Minnaar, A. (2014). 'Crackers', Cyberattacks and Cybersecurity Vulnerabilities : the Difficulties in Combatting the 'New' Cybercriminals. *Acta Criminologica: Southern African Journal of Criminology Special Edition No. 2/2014*, *2*.

Pomerleau, P. L., & Lowery, D. L. (2020). Countering cyber threats to financial institutions: A private and public partnership approach to critical infrastructure protection. In *Countering Cyber Threats to Financial Institutions: A Private and Public Partnership Approach to Critical Infrastructure Protection*. https://doi.org/10.1007/978-3-030-54054-8

Rascão, J. P. (2020). Freedom of Expression, Privacy, and Ethical and Social Responsibility in Democracy in the Digital Age. *International Journal of Business Strategy and Automation*, *1*(3). https://doi.org/10.4018/ijbsa.2020070101

Sabillon, R., Cano, J. J., & Serra-Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, *4*(6).

Weber, A. (2024). Civil Liberties I (Freedom, Life, Liberty, Privacy). In *Writing Constitutions*. Springer. https://doi.org/10.1007/978-3-031-39622-9_4