Estudiante Law Journal

Volume 6 Number 1, February 2024: Pp. 1-13
Faculty of Law, Universitas Negeri Gorontalo, City of Gorontalo, Indonesia
https://ejurnal.ung.ac.id/index.php/eslaw/index

Legal Process for Banking Negligence in Violations of Customers's Privacy Rights and Personal Data

Rifky Pulubolo[1], Mutia Cherawaty Thalib[2], Ahmad[3]

[1] *Faculty of Law, State University of Gorontalo, Indonesia. E-mail: r.pulubolo24@gmail.com*
[2] *Faculty of Law, State University of Gorontalo, Indonesia. E-mail: mutiacherawati@ung.ac.id*
[3] *Faculty of Law, State University of Gorontalo, Indonesia. E-mail: ahmad_wijaya@ung.ac.id*

Abstract: This research aims to find out and analyze the legal process for banking negligence in violating privacy rights and personal data. This research is classified as normative research with a statutory approach and a case approach. The research results show that personal data subjects have the right to sue and receive compensation for violations of the processing of personal data about themselves in accordance with statutory provisions. This is stated in Article 64 Paragraph (1) of Law no. 27 of 2022 concerning Personal Data Protection, "Personal Data dispute resolution is carried out through arbitration, court, or other alternative dispute resolution institutions by statutory provisions. Non-litigation resolution is through arbitration or alternative dispute resolution institutions. Meanwhile, for settlement through litigation, criminal liability can be carried out or through civil lawsuits.
Keywords: **Data Protection; Customers; Banking**

How to cite (Chicago Style):

Pulubolo. R, Thalib. M.C, Ahmad. " Legal Process for Banking Negligence in Violations of Customers' Privacy Rights and Personal Data" *Estudiante Law Journal, 6* (1), (February 2024): 1–13

1. Introduction

Banks, as institutions that protect customer funds, are also obliged to maintain the confidentiality of customer funds from parties who could harm customers. And conversely, people who entrust their funds to be managed by banks must also be protected against arbitrary actions carried out by banks that could harm their customers.[1]

The relationship between banks and customers is not like an ordinary contractual relationship. However, in this relationship, there is also an obligation for the bank not to disclose the secrets of its customers to other parties unless otherwise determined by applicable legislation. This relationship has become more complex due to technological advances and banking digitalization.

Technology has brought advantages by making human life easier, as well as disadvantages by making it easier for criminals to commit crimes. Technology has had a significant influence on the understanding of crime, especially in criminology, which focuses on human factors, both physical and psychological.[2]

The development of science and technology has recently grown rapidly and has also had an impact on people's life patterns in almost all fields, including the economic, social, and cultural fields, as well as the confidentiality of personal data. Confidentiality is protected in statutory regulations in the form of granting the right to privacy, namely the rights that individuals have to fulfill their personal interests regarding access to information and electronic personal data, namely personal data that uses electronic means, so that other parties need to respect them by not violating the rights to privacy and data.[3]

Perlindungan tersebut semakin penting sejalan dengan perkembangan teknologi informasi dan komunikasi yang masif karena didukung media digital, sehingga mudah untuk diakses dan menimbulkan kekhawatiran bagi nasabah bank. Sejalan dengan hal itu, terdapat beberapa alasan pentingnya menjaga data pribadi elektronik, untuk mencegah penyalahgunaan data pribadi secara elektronik oleh pihak yang tidak bertanggung jawab dan menjaga hak kendali atas data pribadi dalam arti memiliki kontrol atas data tersebut.

Personal data is a high-value asset or commodity in the era of big data and the digital economy, so it is necessary to minimize privacy violations and misuse of personal data and increase public awareness to protect their own personal data. Personal data protection not only protects a person's data but also the basic rights and freedoms of

---

[1] Qatrunnada Ernanti, Bambang Eko Turisno, and Aminah, "Perlindungan Hukum Bagi Konsumen Perbankan Dalam Penggunaan Data Pribadi Nasabah (studi Pada Pt Bri Kantor Wilayah Semarang)," *Diponegoro Law Journal* 5, no. 3 (July 12, 2016): 1–14, https://doi.org/10.14710/dlj.2016.12557.

[2] Agus Raharjo, *Cybercrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi* (Bandung: PT Citra Aditya Bakti, 2002).

[3] Sudjana - Sudjana, "Pembocoran Rahasia Bank Sebagai Pelanggaran Hak Privasi Dan Data Pribadi Elektronik Nasabah Bank," *Refleksi Hukum: Jurnal Ilmu Hukum* 6, no. 2 (June 10, 2022): 247–66, https://doi.org/10.24246/jrh.2022.v6.i2.p247-266.

individuals; therefore, it is necessary to ensure that a person's rights and freedoms are not violated, including the confidentiality of bank financial data.[4]

Regarding public interests in the context of state administration, such as the administration of population administration, social security, taxation, customs, and business licensing services integrated electronically, guarantee is a translation from Dutch, namely *Zekerheid* or *Cautie*.[5] It cannot be denied that the banking world is increasingly digitizing so that more and more crimes and criminal acts can occur. The need and use of this information technology with the internet can be found in various fields such as e-commerce, e-banking, e-education, and many more, which have become commonplace.[6]

Leaks or misuse of privacy rights and electronic personal data relating to bank customers give rise to legal consequences because someone feels that their reputation and financial data have been harmed. An example of an account burglary case happened to senior journalist Ilham Bintang. At the trial that took place on July 8, 2020, at the West Jakarta District Court, Ilham explained the chronology of the case that happened to him. On January 4, 2020, an SOS network appeared on the victim's cellphone. Furthermore, on January 6, 2020, when he wanted to make a transaction via the Commonwealth Bank mobile banking (m-banking) application, another problem arose: the victim could not access the Commonwealth Bank m-banking application. And when he decided to check his account directly at the bank, 25,000 Australian dollars, or the equivalent of his 250,000,000 had disappeared.[7]

Another similar case, namely the breach of personal data of bank customers, was the reporting of a private company in Tangerang, PT Bangun Teknik Utama (BTU), regarding the leak of the company's confidential banking data in the form of print-outs of bank statements to Polda Metro Jaya. In the report, the data leak was allegedly carried out by one of the employees of Bank Mandiri Summarecon Gading Serpong KCP, Tangerang, Banten. In the reporting process, PT BTU, through its attorney, brought a number of pieces of evidence in the form of conversations via the WhatsApp

[4] Faiz Rahman, "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia," *Jurnal Legislasi Indonesia* 18, no. 1 (March 31, 2021): 81, https://doi.org/10.54629/jli.v18i1.736.

[5] Nagita Pujiastuti Djafar, Nirwan Junus, and Mohamad Taufiq Zulfikar Sarson, "Perlindungan Hukum Bagi Kreditur Apabila Akta Jaminan Fidusia Tidak Didaftarkan Oleh Notaris," *Jurnal Hukum Dan Sosial Politik* 2, no. 1 (2024): 272–84, https://doi.org/10.59581/jhsp-widyakarya.v2i1.2196.

[6] Muhammad Lathoiful Fikri, "Analisis Hukum Pidana Islam TerhadapPembobolan Rekening Melalui ATM Dalam Direktori Putusan Mahkamah Agung Republik Indonesia (Studi Putusan Nomor: 688/Pid.B/2012/PN.Dps)" (Bachelor Thesis, Surabaya, Universitas Islam Negeri Sunan Ampel, 2017).

[7] Jimmy Ramadhan Azhari and Irfan Maullana, "Kronologi Ilham Bintang Kehilangan Ratusan Juta Rupiah akibat Pembobolan Rekening," KOMPAS.com, July 8, 2020, https://megapolitan.kompas.com/read/2020/07/08/18275931/kronologi-ilham-bintang-kehilangan-ratusan-juta-rupiah-akibat-pembobolan.

application, softcopy prints of newspaper accounts, and four witnesses to provide information to the police.[8]

Based on this, negligence on the part of the bank is very detrimental to customers as consumers of banking services. The problem is the lengthy resolution of cases in court, which is very detrimental to consumers, even though they get compensation.

2. Method

This research is normative legal research. Because this research was carried out or aimed only at written regulations or other legal materials and was mostly carried out on secondary data in the library. In this research, there is a statutory approach and a case approach. This legislative approach is used to examine legislative regulations whose norms still contain deficiencies or even foster irregular practices, either at the technical level or in their implementation in the field.[9] The case approach is a type of approach in normative legal research where prospective researchers try to build legal arguments from the perspective of concrete cases that occur in the field.[10]

3. Legal Process for Banking Negligence

The bank's responsibility for losses experienced by customers can be carried out by resolving disputes. Banks as Financial Services Business Actors (PUJK) are obliged to handle complaints from customers as consumers and resolve disputes regarding their products or services. This is as regulated in Article 6 POJK Number 6/POJK.07/2022 concerning Consumer and Public Protection in the Financial Services Sector. PUJK is obliged to provide accountability for losses experienced by customers after receiving complaints from related victims. In general, each PUJK has an obligation to protect the privacy of each consumer and is responsible for any consumer losses resulting from criminal acts committed by parties representing the interests of the relevant PUJK or errors in the conduct of business by the relevant PUJK.

The presence of Law No. 27 of 2022 has formulated sanctions for personal data violations. In Article 57 Paragraph (2) of the PDP Law, it is stated that personal data controllers can be subject to administrative sanctions in the form of:[11]

1. written warning;
2. temporary suspension of personal data processing activities;
3. deletion or destruction of personal data; and/or
4. administrative fines of a maximum of 2% of annual income or annual receipts for variable violations.

---

[8] Deni Muhtarudin, "Data Rahasia di Mandiri Bocor, Perusahaan Swasta di Tangerang Lapor Polisi," *MONITOR* (blog), April 13, 2021, https://monitor.co.id/2021/04/13/data-rahasia-di-mandiri-bocor-perusahaan-swasta-di-tangerang-lapor-polisi/.

[9] Irwansyah, *Penelitian Hukum* (Yogyakarta: Mira Buana Media, 2020).

[10] Irwansyah.

[11] Indonesia, "Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," Pub. L. No. 27 (2022).

Legal protection has the meaning of protection using legal means or protection provided by law directed at certain interests, namely by turning the interests that need to be protected into a legal right.[12] In addition to imposing administrative sanctions by the designated institution, personal data subjects also have the right to sue and receive compensation for violations of processing personal data about themselves in accordance with statutory provisions as a form of legal protection. This is stated in Article 64 Paragraph (1): "Personal data dispute resolution is carried out through arbitration, court, or other alternative dispute resolution institutions in accordance with the provisions of statutory regulations." Referring to these provisions, the legal process that can be taken is litigation or non-litigation. Non-litigation resolution is through arbitration or alternative dispute resolution institutions.

3.1 Non-Litigation Legal Efforts

1. Arbitration

   Arbitration, according to Article 1, point 1, of Law 30/1999, is a method of resolving civil disputes outside the general court that is based on an arbitration agreement made in writing by the parties to the dispute. An arbitration dispute begins with an agreement to resolve the dispute through arbitration, which is contained in a document signed by the parties. Then, the parties determine together with the arbitrator who will be the executor or decision-maker for the dispute that occurs.

   An arbitrator is one or more persons chosen by the parties to a dispute or a party appointed by the District Court or arbitration institution to provide a decision on a dispute. The arbitrator's role is to provide a decision on the dispute between the parties. The results of the arbitration award are a win-lose judgment, final, have permanent legal force, and are binding on the parties.

2. Other Alternative Dispute Resolution Institutions

   According to Law 30/1999, apart from arbitration, there are alternative dispute resolution institutions other than arbitration, namely by means of consultation, negotiation, mediation, conciliation, or expert assessment. In the context of the PDP Law, there is a mandate to establish an institution determined by the president and responsible to the president to protect personal data.

   The institution administering personal data protection has the authority to:[13]

   1) impose administrative sanctions for violations of personal data protection by personal data controllers and/or processors;
   2) receive complaints and/or reports regarding alleged violations of personal data protection;

[12] Condro Susanto Riyadi and Mutia Ch Thalib, "Jaminan Perlindungan Hukum Terhadap Kesehatan Dan Keselamatan Kerja Kepada Tenaga Kerja Konstruksi," *JURNAL LEGALITAS* 13, no. 02 (February 7, 2021): 79–93, https://doi.org/10.33756/jelta.v13i02.7607.

[13] Indonesia.

3) carry out inspections and investigations of complaints, reports, and/or monitoring results regarding allegations of personal data violations;
4) summon and present every person and/or public body related to alleged violations of personal data protection;
5) request information, data, and documents from every person and/or public body regarding alleged violations of personal data protection;
6) summon and present the necessary experts for examination and investigation regarding suspected violations of personal data protection;
7) inspect and trace electronic systems, facilities, spaces, and/or places used by personal data controllers and/or processors, including gaining access to data and/or appointing third parties; and
8) request legal assistance from the prosecutor's office in resolving personal data protection disputes.

Through the institution that organizes personal data protection, it can also be used as an alternative institution for resolving personal data disputes between subjects and personal data controllers in a non-litigation manner.

3.2 Litigation Legal Efforts

Apart from non-litigation resolution, in Article 64 Paragraph (2) of the PDP Law it is stated that "The procedural law applicable in dispute resolution and/or the judicial process for the Protection of Personal Data as intended in paragraph (1) is implemented based on the applicable procedural law in accordance with the provisions of the regulations".[14] Therefore, for losses resulting from bank negligence, customers can file lawsuits based on civil or criminal matters, for which there are several remedies:

1. Criminal Legal Remedies

   Protection of personal data means that every individual who is the owner of personal data has the right to decide, share, or exchange information or personal data. For this reason, data use must have permission from the data owner so that if there is a problem, the law can regulate the problem. For this reason, those who violate Article 30 paragraph (3) of the ITE Law, which reads:

   "Any person intentionally and without authority or unlawfully accesses a computer and/or electronic system in any way by violating, breaching, surpassing, or breaching the security system."

   For this act, he could be imprisoned for a maximum of 8 years and subject to administrative sanctions of up to 800 million. Other criminal sanctions in Article 48 of the ITE Law are: Every person who fulfills the elements as intended in Article 32. Every person who meets the elements as intended in Article 32, paragraph (2), shall be punished with a maximum

[14] Indonesia.

imprisonment of 9 (nine) years and/or a maximum fine. IDR 3,000,000,000.00 (three billion rupiah).

As for the evidentiary provisions in the PDP Law, Article 64 Paragraph (3), it is stated that valid evidence in this Law includes:[15]

a. evidence as intended in procedural law; And
b. other evidence in the form of electronic information and/or electronic documents in accordance with statutory provisions.

2. Civil Legal Action

Personal data protection is related to the concept of privacy. This concept is the idea of protecting or maintaining the integrity and dignity of personal rights. According to Article 1365 of the Civil Code, "every act that violates the law and causes loss to another person requires the person who caused the loss through his fault to compensate for the loss." Banking has harmed customers due to negligence in protecting customer data, for this reason, civil elements have been discovered, namely unlawful acts and forms of loss.

The basic elements of the lawsuit are:

A. There is an unlawful act;
B. There is an error;
C. There is a causal relationship between unlawful acts, errors, and existing losses.

Article 26 of the Information and Electronic Transactions Law states that anyone can demand personal information without their consent. Violations of the PDP can at least be prosecuted as an unlawful act according to law (1365 Civil Code) or due to incompetence or negligence (1366 Civil Code). Article 3 of the Information and Electronic Transactions Law states that the Precautionary Principle applies, also giving responsibility to every electronic system operator, both companies and governments, to carry out the responsibility for administering electronic systems, namely that they must be reliable, safe, and responsible.

4. Factors Causing Personal Data Leaks

The large number of cases of personal data leaks in Indonesia has created concern among the public. This leak of personal data occurs due to several factors, while the main causes are Standard Operating Procedures (SOP), Human Resources (HR) and Technology. If you look at the number of journals used as references by the author in this research, SOP for personal data protection in Indonesia is currently the most

[15] Indonesia.

researched topic because Indonesia needs time to pass a personal data protection law, starting with the emergence of problems related to data leaks. personal data for the first time in 2020.[16] In response to this problem, the Ministry of Communication and Information issued a draft Law on Personal Data Protection in the same year, although in the end, the draft was only passed in 2022. This means that within two years, there was no law regulating protection people's personal data. This regulatory vacuum has an impact on the vulnerability of personal data to leaks because there is no SOP that regulates maintenance, safeguarding, and other procedures for personal data itself. Apart from that, SOPs are also a major factor in minimizing the occurrence of personal data leaks is because if there are no procedures governing the management of personal data, it could result in personal data controllers not maintaining the security of the personal data they obtain.[17]

Then there is the Human Resources (HR) factor. In terms of personal data, those who are processors and controllers of personal data are grouped into three categories: government/public bodies, organizations/companies, and every person. Governments and public bodies that require personal data must empower people who are able to master the protection of personal data, in the same way that organizations and institutions must also employ employees who have the skills related to personal data protection. Then, everyone must have knowledge about the importance of protecting personal data so that people understand how to protect their own personal data. Finally, the technological factor of personal data security is basically also influenced by the level of hardware and software security; the base used must meet standards for protecting data so that personal data security is maintained. For the benefit of customers, banks are obliged to provide information regarding possible risks of loss arising in connection with customer transactions carried out through the bank. "The availability of complete and accurate legal information is an absolute requirement that must be fulfilled in the legislative process.[18]

Hardware is "all the equipment in a data processing activity." Hardware is used to carry out the functions of data preparation, data entry, calculations, supervision of calculations, storage, and output of results. Hardware is a component that can be touched. Computer hardware cannot do anything without software. Sophisticated hardware technology will function if certain instructions have been given to it. These instructions are called software. Software instructions are written by humans to enable the functioning of computer hardware.Of all the factors causing personal data leaks, SOP is the one most widely discussed in various studies. This shows that the absence

[16] Luqman Sulistiyawan and Bayu Galih, "Kilas Balik, Lima Kasus Kebocoran Data Pribadi di Indonesia," KOMPAS.com, September 6, 2022, https://www.kompas.com/cekfakta/read/2022/09/06/171100182/kilas-balik-lima-kasus-kebocoran-data-pribadi-di-indonesia-.

[17] PDSI KOMINFO, "Memastikan Data Pribadi Aman," Website Resmi Kementerian Komunikasi dan Informatika RI, accessed September 13, 2023, http:///content/detail/37332/memastikan-data-pribadi-aman/0/artikel.

[18] Novendri M. Nggilu and Ahmad Ahmad, "Optimalisasi Jaringan Dokumentasi Dan Informasi Hukum (JDIH) Dalam Pembentukan Produk Hukum Desa Tabongo Timur," *DAS SEIN: Jurnal Pengabdian Hukum Dan Humaniora* 3, no. 1 (January 31, 2023): 49–66, https://doi.org/10.33756/jds.v0i0.15535.

of a Personal Data Protection Law means that Indonesia does not have a legal basis or policy that regulates the protection of personal data in its entirety and creates opportunities for various cases of personal data leakage. Ratification of the law is considered urgent because personal data control procedures must be regulated so that personal data leaks do not occur. Weak legal regulations mean that people who control personal data do not safeguard it properly. This is because there are no procedures on how to safeguard other people's personal data. A personal data controller is defined as any person, public body, or international organization acting individually or jointly in determining the purposes and exercising control over the processing of personal data. Different from personal data processors, personal data processors are every person, public body, and international organization that acts individually or jointly in processing personal data on behalf of the personal data controller.

4.1 Standard Operational Procedure Factors in the Personal Data Protection Law

The ratification of the Personal Data Protection Law makes the policy provisions regarding Standard Operating Procedures related to personal data clear because this law is the basis for the principles of personal data control, but researchers analyzed this law to see whether it is in accordance with the benefits of SOPs that are in accordance with the applicable law.[19]

If we look at the theory used, it is at least stated that there are 15 points or indicators, as follows:

1. As a standardization of the methods used by officials to complete the work they are tasked with. If you look at Article 20 to Article 54 of Personal Data Protection Law No. 27 of 2022, where the discussion regarding the obligations of personal data controllers is explained in detail about the obligations of personal data controllers in controlling personal data, this means that this law resolves the indicator problem.[20]
2. Reduce the level of errors and negligence that may be made by an officer or executor in carrying out their duties. This is written in Chapter VIII, where there is a discussion regarding administrative sanctions, which can be interpreted as meaning that if negligence is carried out by a personal data controller, they can be given sanctions up to being punished.
3. Increase the efficiency and effectiveness of implementing the duties and responsibilities of individual officers and the organization as a whole.
4. Helping officials become more independent and less dependent on management intervention, thereby reducing leadership involvement in the implementation of daily processes.
5. Increase accountability in carrying out tasks.

[19] Republik Indonesia, "Peraturan Menteri Pendayagunaan Aparatur Negara Dan Reformasi Republik Indonesia No. 35 Tahun 2012 Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan," Pub. L. No. 35 (2012).

[20] Indonesia, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

6. Create standard performance measures that will provide officials with concrete ways to improve performance and help evaluate the efforts that have been made.
7. Ensure that the implementation of government administration duties can take place in various situations.
8. Ensure consistency of service to the community, both in terms of quality, time, and procedures. The Personal Data Protection Law, Chapter VI, answers the responsibility of every person and international organization in carrying out the procedures that have been regulated as best as possible. The points above can be said to have been regulated by this law.
9. Provide information regarding competency qualifications that must be mastered by officials in carrying out their duties.
10. Provide information for efforts to increase apparatus competency.
11. Provide information regarding the workload carried by an officer in carrying out his duties.
12. As an instrument that can protect officials from possible lawsuits due to accusations of irregularities.
13. Avoid overlapping implementation of tasks.
14. Assist in tracing procedural errors in providing services.
15. Help provide the information needed in preparing service standards so that it can also provide information for service performance.

In the same chapter, it is also explained what procedures are followed by personal data controllers so that information about the procedures for personal data controllers in processing personal data is clear. Even if adequate SOPs are created, talking about personal data security must also be accompanied by technological security and existing human resource capabilities.

4.2 Human Resources Factors in Personal Data Protection Law

Human Resources have an important role in controlling personal data, this is because the quality of the people who carry out the task of securing personal data must have adequate knowledge of both the technology used and the procedures for controlling personal data. Talking about the quality of human resources itself, according to the theory used, it is explained that there are 3 things that can be used as an assessment of the quality of human resources, namely:

1. Accuracy, accuracy is a measure of how close the observed results are to the true value.
2. Performance, evaluating employee performance is an important part of managing all organizational performance.

3. Effectiveness, is a measure of an organization's ability to achieve its goals, it is the basis for successfully doing the right things correctly.[21]

If you look at the 3 things above, the Personal Data Protection Law does not explain how a controller or processor of personal data must have these 3 aspects, but rather about the responsibilities of the controller and processing of personal data regarding the acquisition and collection; processing and analysis; storage; fixes and updates; appearance, announcement, transfer, distribution, or disclosure; and/or deletion or destruction.[22] This is because personal data belongs to everyone and remains with them from birth.

4.3 Technological Factors in Personal Data Protection Law

The opinion about technology according to scientists is that, according to Yp Simon, technology is a rational discipline designed to ensure scientific mastery and application. According to Paul Saetiles, technology, apart from leading to machinery, includes processes, systems, management, and human and non-human control mechanisms.[23]

In the Personal Data Protection Law, there is no discussion about technology at all. This is very unfortunate because this factor is also the key to security against personal data leaks that occur in Indonesia. Hackers who understand technology will very easily penetrate existing technological security protection if it is not there. state-of-the-art technological security system. Of all the existing stages of personal data processing: acquisition, processing, storage, transfer, and deletion of data, which can be ensured using technology, the stage that is most likely to cause personal data leakage is the.

This is because personal data can be processed by yourself or a third party, and the storage carried out by the personal data controller could be hacked by irresponsible people, therefore the need for high technological security.

5. Conclusion

Personal data subjects have the right to sue and receive compensation for violations of the processing of personal data about themselves in accordance with statutory provisions. This is stated in Article 64 Paragraph 1 of Law No. 27 of 2022 concerning Personal Data Protection: "Personal data dispute resolution is carried out through arbitration, court, or other alternative dispute resolution institutions in accordance with statutory provisions." Referring to these provisions, the legal process that can be taken is litigation or non-litigation. Non-litigation resolution is through arbitration or

[21] Kirana Putri Estiningtyas, "Pengaruh Kapabilitas Teknologi Informasi Dan Kualitas Sumber Daya Manusia Terhadap Keamanan Sistem Informasi Akuntansi (studi Pada Bank Bjb Pusat Kota Bandung)" (Thesis, STIE Ekuitas, 2022), http://repository.ekuitas.ac.id/handle/123456789/1559.
[22] Indonesia, Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.
[23] Rogantina Meri Andri, "Peran Dan Fungsi Teknologi Dalam Peningkatan Kualitas Pembelajaran" (Bachelor Thesis, 2017).

alternative dispute resolution institutions. Meanwhile, for settlement through litigation, criminal liability can be carried out through civil lawsuits. The presence of Law No. 27 of 2022 has formulated sanctions for personal data violations. In Article 57 Paragraph (2) of the PDP Law, it is stated that personal data controllers may be subject to administrative sanctions in the form of written warnings, temporary suspension of personal data processing activities, deletion or destruction of personal data, and/or administrative fines.

References

Books:

Irwansyah. *Penelitian Hukum*. Yogyakarta: Mira Buana Media, 2020.

Raharjo, Agus. *Cybercrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*. Bandung: PT Citra Aditya Bakti, 2002.

Suratman, and Philips Dillah. *Metode Penelitian Hukum*. Bandung: Penerbit Alfabeta, 2015.

Journals:

Djafar, Nagita Pujiastuti, Nirwan Junus, and Mohamad Taufiq Zulfikar Sarson. "Perlindungan Hukum Bagi Kreditur Apabila Akta Jaminan Fidusia Tidak Didaftarkan Oleh Notaris." *Jurnal Hukum Dan Sosial Politik* 2, no. 1 (2024): 272–84. https://doi.org/10.59581/jhsp-widyakarya.v2i1.2196.

Ernanti, Qatrunnada, Bambang Eko Turisno, and Aminah. "Perlindungan Hukum Bagi Konsumen Perbankan Dalam Penggunaan Data Pribadi Nasabah (studi Pada Pt Bri Kantor Wilayah Semarang)." *Diponegoro Law Journal* 5, no. 3 (July 12, 2016): 1–14. https://doi.org/10.14710/dlj.2016.12557.

Nggilu, Novendri M., and Ahmad Ahmad. "Optimalisasi Jaringan Dokumentasi Dan Informasi Hukum (JDIH) Dalam Pembentukan Produk Hukum Desa Tabongo Timur." *DAS SEIN: Jurnal Pengabdian Hukum Dan Humaniora* 3, no. 1 (January 31, 2023): 49–66. https://doi.org/10.33756/jds.v0i0.15535.

Rahman, Faiz. "Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia." *Jurnal Legislasi Indonesia* 18, no. 1 (March 31, 2021): 81. https://doi.org/10.54629/jli.v18i1.736.

Riyadi, Condro Susanto, and Mutia Ch Thalib. "Jaminan Perlindungan Hukum Terhadap Kesehatan Dan Keselamatan Kerja Kepada Tenaga Kerja Konstruksi." *JURNAL LEGALITAS* 13, no. 02 (February 7, 2021): 79–93. https://doi.org/10.33756/jelta.v13i02.7607.

Sudjana, Sudjana -. "Pembocoran Rahasia Bank Sebagai Pelanggaran Hak Privasi Dan Data Pribadi Elektronik Nasabah Bank." *Refleksi Hukum: Jurnal Ilmu Hukum* 6, no. 2 (June 10, 2022): 247–66. https://doi.org/10.24246/jrh.2022.v6.i2.p247-266.

Thesis:

Andri, Rogantina Meri. "Peran Dan Fungsi Teknologi Dalam Peningkatan Kualitas Pembelajaran," 2017.

Estiningtyas, Kirana Putri. "Pengaruh Kapabilitas Teknologi Informasi Dan Kualitas Sumber Daya Manusia Terhadap Keamanan Sistem Informasi Akuntansi (studi Pada Bank Bjb Pusat Kota Bandung)." Thesis, STIE Ekuitas, 2022. http://repository.ekuitas.ac.id/handle/123456789/1559.

Fikri, Muhammad Lathoiful. "Analisis Hukum Pidana Islam TerhadapPembobolan Rekening Melalui ATM Dalam Direktori Putusan Mahkamah Agung Republik Indonesia (Studi Putusan Nomor: 688/Pid.B/2012/PN.Dps)." Bachelor Thesis, Universitas Islam Negeri Sunan Ampel, 2017.

Internet:

Azhari, Jimmy Ramadhan, and Irfan Maullana. "Kronologi Ilham Bintang Kehilangan Ratusan Juta Rupiah akibat Pembobolan Rekening." KOMPAS.com, July 8, 2020. https://megapolitan.kompas.com/read/2020/07/08/18275931/kronologi-ilham-bintang-kehilangan-ratusan-juta-rupiah-akibat-pembobolan.

KOMINFO, PDSI. "Memastikan Data Pribadi Aman." Website Resmi Kementerian Komunikasi dan Informatika RI. Accessed September 13, 2023. http:///content/detail/37332/memastikan-data-pribadi-aman/0/artikel.

Muhtarudin, Deni. "Data Rahasia di Mandiri Bocor, Perusahaan Swasta di Tangerang Lapor Polisi." *MONITOR* (blog), April 13, 2021. https://monitor.co.id/2021/04/13/data-rahasia-di-mandiri-bocor-perusahaan-swasta-di-tangerang-lapor-polisi/.

Sulistiyawan, Luqman, and Bayu Galih. "Kilas Balik, Lima Kasus Kebocoran Data Pribadi di Indonesia." KOMPAS.com, September 6, 2022. https://www.kompas.com/cekfakta/read/2022/09/06/171100182/kilas-balik-lima-kasus-kebocoran-data-pribadi-di-indonesia-.

Laws:

Indonesia. Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi, Pub. L. No. 27 (2022).

Republik Indonesia. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Republik Indonesia No. 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan, Pub. L. No. 35 (2012).