Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens

Dampak Transisi Model Hukum Siber: Legislasi Kejahatan Siber Undang-Undang Perlindungan Data Pribadi (PDP).

Impacts of the Cyber Law Model Transition The Preceding Cybercrime Legislation was the PDP Law

Tri Ginanjar Laksana ✉
Program Studi S1 - Informatika, Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya

✉ Tri Ginanjar Laksana
tri.ginanjar.laksana@dsn.ubharajaya.ac.id

Abstrak

Saat ini, masyarakat global mengalami peningkatan keterhubungan melalui sarana digital. Internet telah menjadi komponen integral dari kehidupan sehari-hari. Namun demikian, kemajuan teknologi menghadirkan hambatan baru yang harus dihadapi masyarakat dan pemerintah. Kejahatan siber mencakup banyak tindakan jahat yang dilakukan melalui internet. Tujuannya adalah untuk melindungi individu dan organisasi dari ancaman siber dan menjaga keamanan serta keandalan data di ranah digital. Tujuan penelitian ini adalah untuk memastikan evolusi kerangka hukum siber: keberadaan dan konsekuensi legislasi kejahatan siber sebelum implementasi undang-undang Perlindungan Data Pribadi. Metodologi penelitian yang digunakan untuk membahas isu-isu dalam penelitian ini mencakup metodologi penelitian hukum normatif (juri normatif) serta penelitian hukum empiris (juri empiris). Penelitian ini menggunakan pendekatan deskriptif dan analitis, dengan menggunakan data primer dan sekunder. Legislasi perlindungan data memainkan peran penting dalam memerangi kejahatan siber. Legislasi ini menetapkan struktur hukum yang komprehensif untuk melindungi kerahasiaan dan integritas data pribadi. Kerja sama antar pemerintah, organisasi, dan masyarakat luas dapat menjamin bahwa undang-undang tentang perlindungan data pribadi secara efektif melindungi masyarakat dari kejahatan siber.

Kata Kunci: *Hukum Siber, Model, Transisi, kejahatan siber, Hukum Perlindungan Data Pribadi.*

Abstract

Presently, the global community is experiencing a growing level of interconnectedness via digital means. The internet has become an integral component of daily existence. Nevertheless, the progress of technology brings out novel obstacles that society and the government must confront. Cybercrime encompasses many malevolent acts conducted over the internet. Its objective is to safeguard persons and organisations against cyber threats and uphold the security and reliability of data in the digital realm. The objective of this study is to ascertain the evolution of the cyber legal framework: the presence and consequences of cybercrime legislation prior to the implementation of the Personal Data Protection legal. The research methodology used to address the issues in this study encompasses normative legal research methodologies (normative juridical) as well as empirical legal research (empirical juridical). This study employs a descriptive and analytical approach, using both primary and

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens
secondary data. Data protection legislation plays a crucial role in combating cybercrime. It establishes a comprehensive legal structure to safeguard the confidentiality and integrity of persons' data. Cooperation among governments, organisations, and the public at large can guarantee that legislation on personal data protection effectively safeguards society against cybercrime.

Keywords: *Cyber Law, Model, Transition, cybercrime, PDP Law.*

INTRODUCTION

The cyber legal framework is constantly evolving in response to technological advancements and the emergence of new dangers. It is essential to consistently revise and modify existing legislation in order to address these difficulties. (Sinaga et al. 2023), (Muharam and Budianto 2022), (Amin, 2021). In addition to this, it is essential for legal professionals and governmental entities to swiftly adjust to the rapid pace of technology advancements in order to uphold security measures and safeguard society from cybercriminal activities (Maria Utama, Iza Rumesten RS 2008). Comprehending these alterations and guaranteeing the robustness of current cyber legislation is vital in safeguarding users (Putri and Fahrozi 2021). Understanding these changes and ensuring the strength of existing cyber laws is crucial in protecting users (Ulya Amaliya 2009). The personal data protection (PDP) legislation is an essential component of cyber law. The primary objective of the PDP Act is to safeguard the confidentiality and integrity of people' data. This includes personal details such as name, address, phone number, and financial data (Carolin and Apriani 2022),(Nursiyono and Huda 2023), (Delpiero, Reynaldi, and Ningdiah 2021). The significance of personal data protection regulations has escalated in light of the current surge in data breach incidents (Christine and Kansil 2022). In a world that is becoming more interconnected, personal data has great value and may be used by unscrupulous entities (Rahmatullah 2021). Hence, the PDP legislation serves the purpose of thwarting cybercrime by establishing a well-defined legal structure to safeguard persons' data.

Individuals and organisations must fully understand the crucial aspects of the law regarding personal data protection (Wicaksana and Munandar 2020). A primary prerequisite is the need to get explicit agreement prior to the collection and use of persons' personal data (Andraputri and Ruhaeni 2023). This empowers people to have authority over the use of their data. In addition, the PDP legislation grants people the right to access, rectify, and erase personal data gathered by organizations. (Sitorus 2023). This ensures clarity and protects personal confidentiality. The PDP legislation imposes regulations on enterprises regarding managing and protecting personal data. (Carundeng 2022). This includes implementing appropriate security measures and notifying the relevant authorities of any data breaches (Hasibuan and Salsiah 2022). Some nations use the transition model in personal data protection law to enforce new legislation gradually (Puspitasari and Izzatusholekha 2023). This gives organizations and people sufficient time to make preparations and adjust to the required modifications.

This transition approach enables enterprises to implement essential system modifications and guarantee personal data protection legislation adherence. This also allows people to comprehend their rights and seek clarification by asking questions in case of any uncertainty (Disemadi 2021). Nevertheless, this transition paradigm may provide difficulties, particularly in ensuring continuous adherence and sufficient data safeguarding (Mardiana and Meilan 2023). Hence, governments and regulatory agencies must provide unambiguous and encouraging instructions for enforcing personal data protection legislation.

To comprehend the significance of personal data protection regulations in combating cybercrime, examine a case study that illuminates its ramifications. In 2018, a major corporation

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens
had a data breach that led to the theft of personal data belonging to millions of consumers (Ni'mah 2023). Cybercriminals use this information to engage in fraudulent activities and steal identities (Sulistianingsih, Ihwan, and Setiawan 2023). This results in substantial monetary losses for people and tarnishes the company's image (Thaher 2022). Nevertheless, due to current personal data protection legislation, these organizations must provide reparation to those impacted by data breaches (Novinna 2020). Furthermore, the corporation faced fines and had to enhance security protocols to mitigate the risk of future data breaches (Hertianto 2021). This case study highlights the crucial role of personal data protection legislation in safeguarding persons and organizations from cybercrime (Mantili and Dewi 2020). It establishes a transparent legal structure for addressing data breaches and ensuring equitable restitution for impacted persons.

Although personal data protection laws provide evident advantages, they also present obstacles and receive critiques that must be addressed (Kesuma and Budiartha 2021). A primary obstacle is the organization's ability to adhere to regulations consistently. Numerous firms still need a comprehensive understanding and must effectively follow the rules outlined in the PDP legislation (Rezkia 2020). Furthermore, there is also contention that regulations safeguarding personal data may impose a high cost on enterprises, particularly those of smaller scale and limited resources (Baiq 2021). Lack the necessary resources or competence to fulfil the demands of this legislation (Pakpahan, Chandra, and Dewa 2020). Nevertheless, it is crucial to remember that personal data protection regulations aim to safeguard both people and society at large. This legislation effectively ensures the preservation of personal data privacy and security.

The involvement of governments and regulatory organizations is crucial in ensuring compliance with legislation concerning personal data protection. They provide explicit and encouraging direction to people and organizations to ensure adherence to this legislation (Kosegeran 2022). Furthermore, governments and regulatory organizations need to possess sufficient enforcement authority to combat infringements of laws pertaining to safeguarding personal data (Salsabila, Hosen, and Manik 2022). This encompasses the capacity to scrutinize instances of data breaches, enforce appropriate penalties, and safeguard the rights of impacted persons (Anggitafani 2021). Businesses are required to comply with personal data protection legislation. Implementing optimal strategies for handling and safeguarding consumer personal data is essential (Amboro and Puspita 2021). Businesses should adhere to the best practice of collecting and using personal data only with the entire agreement of the individual in question.2). Employ appropriate security protocols to safeguard personal data from unauthorized intrusion. 3). Regularly perform security audits to verify personal data protection legislation adherence. 4). Enforce a privacy policy that is unambiguous and readily available to relevant persons. 5). Provide comprehensive training to staff on the significance of safeguarding personal data and the optimal procedures that must be adhered.

Adapting to changes in the cyber legal context requires making regulation revisions, enhancing institutional capacity, promoting public education, and fostering international collaboration. Maintaining cyber security, safeguarding privacy, and guaranteeing that the legal system can effectively address the ever-changing issues posed by information technology.

RESERACH METHODOLOGY

This study employs a doctrinal research technique, using legal and philosophical methodologies. The legal papers used in this study include primary, secondary, and tertiary sources. The acquisition of technical legal documents was accomplished via literature reviews (documentation studies) and web searches. Analysing legal documents in research involves doing a descriptive analysis.

RESULT AND DISCUSSION

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens

The evolving legal framework around cyber matters and the need for adjustment

Cyber law is a legal area that governs actions in the digital realm and evolves with advancements in information and communication technologies. Over the last several years, there have been substantial modifications to cyber legislation, necessitating adjustment from all relevant parties. (Purba et al. 2023). The alterations in the cyber legal framework are mainly attributed to shifts in societal technology utilization patterns. Previously, a few individuals used the internet for restricted objectives, such as interpersonal correspondence or information retrieval (Jelanti et al. 2023). Nevertheless, the Internet has become an essential component of daily existence, serving as a tool for many activities such as communication, online shopping, and financial transactions. The advancement of technology also influences the kind of criminal activities that take place in the digital realm. Instances of crimes such as identity theft, internet fraud, and cyber attacks are more prevalent. Hence, legislation about cyber offenses must adapt in tandem with technological advancements. It is crucial to adjust to the evolving cyber legal environment in order to guarantee security and equity in the digital realm. Initially, the government must enact legislation that is relevant to contemporary technolog (Benu et al. 2020). Legislation should include a wide range of cybercrimes and provide suitable penalties for those responsible for such offenses. In addition, the government must enhance the police's capabilities to address cybercrime cases.

In addition to governments, people must also adjust to the evolving cyber legal environment. Every person needs to possess information and comprehension of cyber legislation to safeguard oneself and avert falling prey to cybercrime. One may do this by examining relevant legislation, using suitable security measures, and safeguarding the confidentiality of personal information. The business sector plays a crucial role in adjusting to changes in the cyber legal environment. Technology firms must prioritize their goods and services' safety and legal compliance.

Additionally, they should have a proficient team to manage and respond to cyber threats effectively. People, governments, and educational institutions must adapt to the evolving cyber legal environment. Educational institutions should include cyber law education in their curriculum to ensure that students comprehend the significance of cyber law and acquire the necessary skills to protect themselves. In the current age of digital technology, the importance of cyber legislation must be considered. All stakeholders, including people, governments, organizations, and educational institutions, must adapt to the evolving cyber legal environment. This adaptation aims to transform cyberspace into a secure and equitable user environment.

Data controllers are legally obligated to guarantee the legitimate and safe processing of personal data while granting people the right to access, rectify, and erase their data. Like other data protection laws, the PDP Law acts as a deterrent against cybercrime by mandating organizations to adopt suitable security measures and adhere to data protection standards. This highlights the need to acquire permission for data processing and gives people the authority to safeguard their personal information, enabling them to exercise control over the security of their data. Ultimately, comprehending data security laws and their function in thwarting cybercrime is vital in the contemporary era of technology. The laws, including GDPR, CCPA, and the PDP Act, aim to safeguard people's data and ensure organizations are responsible for their data processing procedures. Countries and organizations may establish a more secure digital atmosphere, safeguard people against possible cyber hazards, and foster a culture of data protection and cybersecurity by enacting these laws. The purpose of personal data protection legislation is to safeguard the rights and privacy of persons regarding the gathering, handling, and retention of their personal information.

The primary stipulations of legislation on safeguarding personal data and its consequences for people and enterprises.

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens

The core tenets of legislation on safeguarding personal data and its ramifications for both people and enterprises. Personal data protection is seeing fast growth in the current digital age (Mulyana 2021), The fundamental principles of law concerning protecting personal data and its consequences for individuals and businesses. Personal data protection is seeing rapid expansion in the present era of digital technology (Mikel Kelvin 2016). To address these issues, governments worldwide have implemented legislation and regulations to safeguard people's data against unauthorized access, use, and disclosure (Cone et al. 2007). The primary law in Indonesia that regulates personal data protection is Law No. 11 of 2020, respecting Personal Data Protection. The primary sections of the legislation seek to build a comprehensive structure for safeguarding personal data, which applies to both people and corporations. A key component is the need for permission.

By legal regulations, personal data may only be collected, processed, and used with the explicit agreement of the individual to whom the data pertains. Individuals can determine whether firms may acquire and use their data. These rules aim to empower people with more authority over their personal data and guarantee that corporations adhere to ethical standards while managing such data. Another crucial stipulation in the legislation is the need for enterprises to disclose to people the specific objectives for which their data is gathered, processed, and used. The purpose of this is to guarantee openness and responsibility in the management of personal data. Businesses must provide unambiguous and succinct information on the objective and precise particulars of the personal data that will be gathered. Individuals are entitled to be informed about how their personal data will be used and the degree to which it will be disclosed to third parties. The legislation also delineates the rights of persons to their data. Individuals are entitled to retrieve their data, rectify any mistakes, and demand the erasure of their data whenever it becomes unnecessary for the original collection objectives. This gives people more authority over their data, enabling them to verify and guarantee that it is precise. Busicompleteust builds internal processes to enable these rights and promptly react to individual requests. The repercussions of this legislation on people are substantial. This empowers people with more authority and safeguards their data, augmenting their privacy rights.

Individuals possess the authority to choose the methods by which their data is gathered, handled, and used, as well as the entitlement to retrieve, revise, and erase their data. This enables people to make well-informed decisions about sharing their data with companies while safeguarding them from unauthorized use and disclosure. The influence on the corporate world is significant. Businesses must now have robust data protection policies and processes to ensure compliance with legal requirements. It is essential to guarantee that personal data is gathered and used in line with the designated objectives for each individual while also implementing suitable security measures to safeguard personal data from unauthorized access and disclosure. Failure to comply with the law may lead to significant fines and harm the image of enterprises. Law No. 11 of 2020 on Personal Data Protection in Indonesia contains significant regulations to safeguard personal data. This empowers people with more autonomy over their data and strengthens their rights to privacy. Conversely, the business sector must have thorough data protection policies and processes to adhere to legal requirements. This legislation represents a notable advancement towards Indonesia's more secure and privacy-oriented digital environment.

By using this transition model, firms may effectively adjust to changing personal data protection legislation, mitigate the risk of legal infractions, and foster a culture of compliance with data privacy regulations. Companies may ensure compliance with rules and safeguard people's privacy rights by comprehending the ramifications and implementing suitable measures.

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens

An Illustrative Analysis That Underscores The Significance Of Legislation About The Safeguarding Of Personal Data In Combating Cybercrime.

Personal data security is a significant problem in the contemporary digital age. The escalation of cybercrime has underscored the need for robust legislation and regulations to safeguard persons and organizations from the perils of the digital realm. (Sen et al. 2022). This essay seeks to elucidate a case study that underscores the significance of legislation pertaining to the safeguarding of personal data in combating cybercrime (Amin 2021). Cybercrime, including various illicit acts conducted via digital platforms, has emerged as a pervasive menace to society. (Kashyap and Chaudhary 2023). Cybercriminals consistently exploit weaknesses in order to cause chaos for people and enterprises, engaging in activities such as hacking, data breaches, identity theft, and online fraud.

The repercussions of being a target of this kind of offense may have severe and profound effects on one's financial situation and mental well-being. An illustrative example showcasing the significance of personal data protection regulations in combating cybercrime is the well-renowned Equifax hack. In 2017, Equifax, a prominent credit reporting agency in the United States, had a significant cyber assault that resulted in the breach of personal data belonging to about 147 million individuals. The security breach compromised confidential information, including individuals' names, addresses, social security numbers, and credit card particulars, endangering millions of people to potential identity theft and financial crime. The Equifax hack underscores the immediate need for comprehensive regulation to secure personal data and impose liability on organizations for failing to protect sensitive information. The United States has enacted the Data Security and Breach Notification Act to react to these instances. This law requires corporations to adopt appropriate security measures to safeguard personal data and quickly inform persons who may be impacted in the case of a breach.

This legislation acts as a disincentive for organizations to prioritize safeguarding data and promotes proactive measures to reduce the danger of cyberattacks. Without a doubt, enforcing legislation on safeguarding personal data is crucial in combatting cybercrime. The legislation sets up a legal structure for managing and protecting personal information and encourages a culture of obligation and liability. Organizations must provide resources to implement robust cybersecurity safeguards, train their workers on the best practices for data protection, and regularly monitor for possible risks. Furthermore, personal data protection regulations allow people to exert enhanced authority over their data. Individuals are granted the right to be informed about collecting, using, and disclosing their personal information. The presence of transparency promotes confidence among people and organizations, hence enhancing collaborative efforts in combating cybercrime. Ultimately, the Equifax hack case study exemplifies the essential role of personal data protection legislation in combating cybercrime. This serves as a reminder of the inherent risks in the digital realm and underscores the need for legislation that holds entities accountable for safeguarding individuals' personal information. Through implementing robust data protection measures and cultivating a culture of accountability, both people and organizations may collaboratively battle cybercrime and effectively reduce its detrimental consequences. In the current digital environment, safeguarding personal data is no longer a luxury but an essential need.

Data protection rules incentivize corporations to exercise more caution in handling personal data and enhance their adherence to rigorous security protocols. Within a worldwide framework, this case emphasizes the need for collaboration among nations and multinational corporations to combat cybercrime that may exploit legal and regulatory gaps in different jurisdictions. This case study highlights personal data protection legislation's crucial significance in safeguarding people's private rights, enhancing data security, and establishing a legal framework for enforcing privacy regulations.

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens

Obstacles and disapproval of legislation for the safeguarding of personal data

Personal data security is a significant problem in the contemporary digital age. The escalation of cybercrime has underscored the need for robust legislation and regulations to safeguard persons and organizations from the perils of the digital realm (Buchan 2021). This essay seeks to elucidate a case study that underscores the significance of legislation pertaining to the safeguarding of personal data in combating cybercriminal activities (Jha 2021). Cybercrime, including a variety of illegal actions conducted via digital platforms, has emerged as a pervasive menace to society (Manullang 2022). Cybercriminals consistently exploit weaknesses to cause chaos for people and organisations, engaging in activities such as hacking, data breaches, identity theft, and online fraud. The repercussions of being a target of this kind of offence may be profoundly detrimental, including significant financial and emotional distress. An illustrative example showcasing the significance of personal data protection regulations in combating cybercrime is the well renowned Equifax hack. In 2017, Equifax, a prominent credit reporting agency in the United States, had a significant cyber breach that resulted in the unauthorised access and exposure of the personal data of about 147 million individuals. The security breach compromised confidential information, including individuals' names, addresses, social security numbers, and credit card particulars, so endangering millions of people to potential identity theft and financial crime. The Equifax hack underscores the immediate need for comprehensive regulation to secure personal data and enforce accountability on organisations for their failure in protecting sensitive information. The United States enacted the Data Security and Breach Notification Act as a reaction to these instances. This legislation requires corporations to adopt appropriate security measures to safeguard personal data and quickly inform persons who are impacted by any breaches.

To address these issues and critiques, it is necessary to enhance and establish data protection legislation that considers technical advancements and offers robust safeguards for individual privacy rights, while also taking into consideration the requirements and difficulties faced by businesses.

The function of governments and regulatory agencies is to uphold laws pertaining to safeguarding personal data.

The government and regulatory agencies play a crucial role in enforcing laws that protect personal data. In the current digital landscape, where the sharing of personal information is becoming more prevalent, safeguarding people's data is of utmost significance. (Atta and Haq 2019). In light of the persistent risk of data breaches and identity theft, it is imperative for governments to enact robust legislation and create regulatory organisations to safeguard personal data (Katagiri 2021). The Indonesian government has acknowledged the significance of safeguarding personal data and has implemented substantial measures to ensure compliance. The enactment of the Law on Personal Data Protection has established a legal framework governing the acquisition, storage, and use of personal data. This legislation imposes complete accountability on the government and regulatory entities for the enforcement and implementation of the law.

The government's primary responsibility in upholding personal data privacy legislation is establishing and maintaining an efficient regulatory framework. This entails the creation of a regulatory entity responsible for supervising the execution and enforcement of data protection legislation. The National Cyber and Crypto Agency (BSSN) is the primary regulatory authority in Indonesia to oversee this responsibility. Implementing BSSN is crucial in guaranteeing adherence to personal data protection legislation, including governmental and non-governmental entities. BSSN's primary role is to formulate legislation and recommendations that elucidate the organizational prerequisites and duties for safeguarding personal data. BSSN facilitates the comprehension of legal obligations for the corporate sector and serves as a

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens
resource for people to comprehend their entitlements to their personal information. The function of BSSN in this aspect is crucial, as it serves as an intermediary between governments, organizations, and people, ensuring that rules regarding protecting personal data are comprehended and adhered to appropriately.

Furthermore, BSSN is accountable for overseeing and managing the execution of steps to safeguard personal data. BSSN guarantees that organizations safeguard personal data in compliance with the law via regular audits and inspections. BSSN has the jurisdiction to enforce fines and sanctions on the accountable parties if breaches or abuses are discovered.

It is essential for governments and regulatory agencies to establish and maintain a robust framework to safeguard personal data. Through the establishment of explicit legislation, implementation of monitoring mechanisms, and enforcement of laws, they actively enhance data security and privacy for both society and enterprises.

They ensure compliance and implement best practices for organizations to adhere to personal data protection legislation.

During this age of digitalization, corporations own vast quantities of personal data. The data, ranging from consumer information to staff records, is a precious asset that requires protection. (Fairburn 2021). Adhering to data privacy rules is not just a legal obligation but also an essential practice for every conscientious firm (Milano 2021). Personal data protection laws, often known as privacy laws, are policies implemented to ensure the confidentiality and rights of people's personal information (Pitchan and Omar 2019). The rules pertaining to this matter differ across different countries, but they often adhere to similar principles like permission, purpose constraints, data minimization, accuracy, retention limitations, integrity, and accountability. In order to adhere to this legislation, firms are required to use optimal methodologies that give precedence to safeguarding data and ensuring privacy. To guarantee compliance and establish a robust data protection framework, it is important to take into account the following major factors: 1. Awareness and Training: Companies must prioritise the dissemination of knowledge among their staff on the significance of safeguarding data and ensuring privacy. Training sessions should include subjects such as protocols for managing data, steps to ensure security, and the repercussions of failing to comply. This fosters a culture of responsibility and guarantees that all individuals comprehend their responsibilities in safeguarding personal data. 2. Data Mapping and Classification: Businesses are required to do a comprehensive assessment of all the personal data they gather, handle, and retain. This entails determining the nature of the data, its specific whereabouts, and the intended objective for its acquisition. This activity facilitates comprehension of the extent of managing personal data and empowers firms to enforce suitable security measures. 3. Data Minimization and Purpose Restriction: Businesses should only gather and keep personal data that is essential for the intended objective. The act of excessively gathering and retaining data not only heightens the likelihood of data breaches but also contravenes the concept of purpose restriction. Businesses may mitigate risk by adopting a data reduction strategy, which involves reducing the quantity of personal data they manage. 4. permission Management: Acquiring legitimate permission from persons is a fundamental need in the majority of data protection legislations.

By implementing these optimal strategies, companies may establish a culture that adheres to personal data protection regulations, minimise the likelihood of legal infractions, and foster public confidence in the creation of equitable legislation.

CONCLUSSION

Legal Ramifications of Cybercrime Prior to the implementation of the Personal Data Protection Law Prior to the implementation of the Personal Data Protection Law, the legislation concerning cybercrime encountered several obstacles in properly safeguarding persons' digital

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens

existence. An essential obstacle is the need for comprehensive legislation pertaining to the security of personal data. Cybercriminals often target personal data, including names, addresses, and financial information, with the intention of engaging in identity theft, fraud, or other malevolent acts. Insufficient legislative protections to safeguard personal data will leave individuals and organisations susceptible to cyber dangers. Moreover, the lack of any legislation on cybercrime complicates the process of prosecuting and penalising offenders. Conventional legal frameworks, such as those pertaining to theft or fraud, fail to fully include the distinct characteristics of cybercrime, hence posing difficulties in prosecuting cybercriminals. Implementation of the Personal Data Protection Legislation The implementation of the Personal Data Protection Law represents a noteworthy achievement in tackling the difficulties presented by cybercrime. The purpose of this legislation is to safeguard persons' data by enforcing stringent restrictions pertaining to its acquisition, retention, and use by both organisations and individuals.

The Personal Data Protection Act empowers people with more authority over personal data, enabling them to grant or refuse permission for its collection and use. Cybercrime laws have seen substantial changes in both their presence and consequences over the years. The evolution of cyber law, which encompasses the formulation of targeted legislation to address cybercrime, has been crucial in maintaining the legal framework's pertinence amongst the rapid advancement of technology. Prior to the implementation of the Personal Data Protection Act, there were difficulties in adequately safeguarding persons' data and bringing offenders to justice under cybercrime legislation. Nevertheless, the implementation of this legislation has bolstered the legal structure, so enhancing security, privacy, and responsibility in the realm of digital technology. With the continuous progress of technology, it is crucial for the legal system to maintain its flexibility in order to successfully fight cybercrime. Governments and organisations must regularly assess and revise their rules to tackle growing risks, safeguard personal information, and provide a secure cyberspace for all individuals.

REFERENCE

Amboro, F. Y. P., and V. Puspita. 2021. "Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia Dan Norwegia)." *CoMBInES-Conference on Management* 2(1):1–45.

Amin, M. E. 2021. "Harmonization of Cyber Crime Laws with the Constitutional Law in Indonesia." *International Journal of Cyber Criminology* 15(1):79–94. doi: 10.5281/zenodo.4766534.

Anak Agung Gde Sidhi, Satrya Dharma, dkk. 2011. "Kajian Yuridis Keabsahan Jual Beli Secara Elektronik (e-Commerce) Dengan Menggunakan Kartu Kredit." *Skripsi Fakultas Hukum Universitas Udayana*, 1–11.

Andraputri, C. A. N., and N. Ruhaeni. 2023. "Pelaku Penyalahgunaan Penyebaran Data Pribadi Jurnalis Di Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Bandung Conference Series* 1(1):34–56.

Anggitafani, R. F. 2021. "Perlindungan Hukum Data Pribadi Peminjam Pinjaman Online Perspektif POJK No. 1/POJK. 07/2013 Tentang Perlindungan Konsumen Sektor Keuangan Dan Aspek …." *Journal of Islamic Business Law*.

Atta, Qamar, and Ul Haq. 2019. "Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan." *Computer Network and Information Security* 1(1):62–69. doi: 10.5815/ijcnis.2019.01.06.

Baiq, P. A. 2021. "Perlindungan Hukum Terhadap Data Pribadi Dalam Transaksi E-Commerce: Perspektif Hukum Islam Dan Hukum Positif." *DIKTUM: Jurnal Syariah Dan Hukum* 2(1):34–45.

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens
Benu, YSIP, SMSS Putri, C. F. B. Hartanto, R. Marginingsih, and ... 2020. *Human Resource Management (HRM) In Industry 5.0*. books.google.com.

Buchan, R. 2021. "Cyber Espionage and International Law." *Research Handbook on International Law and Cyberspace* 231–52.

Carolin, F. P., and R. Apriani. 2022. "Analisis Pengaturan Perlindungan Data Pribadi Pengguna Fintech Lending Dalam Peraturan OJK Nomor 06/Pojk. 07/2022." *Jurnal Ilmiah Wahana Pendidikan*.

Carundeng, R. B. 2022. "Data Pribadi Konsumen Yang Diretas Berdasarkan Peraturan Menteri Komunikasi Dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam." *LEX PRIVATUM* 1(1):45–78.

Christine, B., and C. S. T. Kansil. 2022. "Hambatan Penerapan Perlindungan Data Pribadi Di Indonesia Setelah Disahkannya Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *Syntax Literate; Jurnal Ilmiah* 2(2):34–57.

Cone, Benjamin D., Cynthia E. Irvine, Michael F. Thompson, and Thuy D. Nguyen. 2007. "A Video Game for Cyber Security Training and Awareness." 26:63–72. doi: 10.1016/j.cose.2006.10.005.

Del-real, Cristina, María José, Rodriguez Mesa, and Cristina Del-real. 2023. *From Black to White : The Regulation of Ethical Hacking in Spain From Black to White : The Regulation of Ethical Hacking in Spain*. Vol. 32.

Delpiero, M., F. A. Reynaldi, and I. U. Ningdiah. 2021. "Analisis Yuridis Kebijakan Privasi Dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data." *Padjadjaran Law Review* 3(2):23–46.

Disemadi, H. S. 2021. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia." *Jurnal Wawasan Yuridika*.

Fairburn, N. 2021. "Beyond Murphy's Law: Applying Wider Human Factors Behavioural Science Approaches in Cyber-Security Resilience: An Applied Practice Case Study Discussing Approaches to Assessing Human Factors Vulnerabilities in Cyber-Security Systems." *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 12788:123–38.

Hasibuan, E. S., and L. Salsiah. 2022. *Urgensi Undang-Undang Perlindungan Data Pribadi Terhadap Kejahatan Pelanggaran Data Di Indonesia*. journal.unigres.ac.id.

Hertianto, M. R. 2021. "Sistem Penegakan Hukum Terhadap Kegagalan Dalam Perlindungan Data Pribadi Di Indonesia." *Kertha Patrika*.

Iancu, Elena-ana. n.d. "Preventing Computer Crime by Knowing the Legal Regulations That Ensure the Protection of Computer Systems." doi: 10.24818/TBJ/2023/13/3.03.

Jelanti, S. E. Desi, M. Ak, S. E. Yuliana, R. Ramadhaniyati, and ... 2023. *Ekonomi Mikro Dalam Digitalisasi*. books.google.com.

Jha, M. 2021. "Cyber Security: Terms, Laws, Threats and Protection." *Proceedings - 2021 International Conference on Computing Sciences, ICCS 2021* 148–51.

Kashyap, Amit Kumar, and Mahima Chaudhary. 2023. "Cyber Security Laws And Safety In E-Commerce In India." *Law and Safety* 2(1):207–2016.

Katagiri, N. 2021. "Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks." *Journal of Cybersecurity* 7(1). doi: 10.1093/cybsec/tyab009.

Kesuma, AANDH, and I. N. P. Budiartha. 2021. "Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial Dalam Transaksi Elektronik." *Jurnal Preferensi* ….

Kosegeran, G. 2022. "Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin." *LEX PRIVATUM*.

Mabizar. 2021. "Cyber Security Diplomacy and International Law.Pdf." 1–56.

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens
Mantili, R., and P. E. T. Dewi. 2020. "Prinsip Kehati-Hatian Dalam Penyelenggaraan Sistem Elektronik Dalam Upaya Perlindungan Data Pribadi Di Indonesia." *Jurnal Aktual Justice*.

Manullang, Sardjana Orba. 2022. "The Legality of Devious Cyber Practices : Readiness of Indonesia ' s Cyber Laws." 10(2):489–502. doi: 10.33019/society.v10i2.482.

Mardiana, N., and A. Meilan. 2023. "Urgensi Perlindungan Data Pribadi Dalam Prespektif Hak Asasi Manusia." *Jurnal Rechten: Riset Hukum* 1(2):12–23.

Maria Utama, Iza Rumesten RS, Irsan. 2008. "Digital Signature Dalam Sengketa E-Commerce Contract Berdasarkan Undang - Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elktronik." *Majalah Ilmiah Fakultas Hukum Universitas Sriwijaya* 45(2):2535–49.

Mikel Kelvin. 2016. "Pengaturan Kebebasan Berekspresi Melalui Media Digital Menurut Hukum Internasional Dan Penerapannya Di Indoensia." *Skripsi Bagian Hukum Internasional Fakultas Hukum Universitas Hasanudin Makasar*, 1–118.

Milano, F. 2021. "Detection of Cyber-Attacks of Power Systems through Benford's Law." *IEEE Transactions on Smart Grid* 12(3):2741–44. doi: 10.1109/TSG.2020.3042897.

Muharam, Novi Asih, and Azis Budianto. 2022. "Carding Crime Analysis as A Form of Cyber Crime in Indonesia ' s Criminal Law." *ICLSSEE* 1(1):1–6. doi: 10.4108/eai.16-4-2022.2320085.

Mulyana, Deddy. 2021. "The Practice of McJournalism in Indonesia ' s Cyber Media." 37(2):1–18.

Ni'mah, M. 2023. "Tinjauan Hukum Perlindungan Data Pribadi Nomor Darurat Pada Platfrom Kredivo." *UMSIDA*.

Novinna, V. 2020. "Perlindungan Konsumen Dari Penyebarluasan Data Pribadi Oleh Pihak Ketiga: Kasus Fintech 'Peer to Peer Lending.'" *Jurnal Magister Hukum Udayana*.

Nursiyono, J. A., and Q. Huda. 2023. "Analisis Sentimen Twitter Terhadap Perlindungan Data Pribadi Dengan Pendekatan Machine Learning." *Jurnal Pertahanan &Bela Negara*.

Pakpahan, E. F., L. R. Chandra, and A. A. Dewa. 2020. "Perlindungan Hukum Terhadap Data Pribadi Dalam Industri Financial Technology." *Veritas et Justitia*.

Pitchan, Muhammad Adnan, and Siti Zobidah Omar. 2019. "Dasar Keselamatan Siber Malaysia : Tinjauan Terhadap Kesedaran Netizen Dan Undang-Undang Cyber Security Policy : Review on Netizen Awareness and Laws." 35(1):103–19.

Purba, O., A. Syamil, A. Nooraini, S. Sepriano, and ... 2023. *Dasar Hukum & Analisis Tata Kelola Ibu Kota Negara Dari Berbagai Bidang*. books.google.com.

Puspitasari, D., and I. Izzatusholekha. 2023. "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Mengatasi Masalah Keamanan Data Penduduk." *Journal Of Science Law* 1(2):34–45.

Putri, D. D. F., and M. H. Fahrozi. 2021. "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan RUU Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. Com)." *Borneo Law Review*.

Rahmatullah, I. 2021. "Pentingnya Perlindungan Data Pribadi Dalam Masa Pandemi Covid-19 Di Indonesia." *Adalah: Buletin Hukum &Keadilan*.

Ratna Kusuma Wardani. 1999. "Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Jual Beli Secara Online Sesuai Dengan Undang - Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen." *Penelitian Kementrian Riset, Teknologi Dan Pendidikan Tinggi Universitas Jember*, 1–68.

Rezkia, NUHP. 2020. *Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Registrasi Sim Card*. repository.unhas.ac.id.

Salsabila, R., M. Hosen, and H. Manik. 2022. "Perlindungan Hukum Kerahasian Data Pribadi Konsumen Pengguna Produk Provider Telekomunikasi Di Indonesia." *Zaaken: Journal of Law* 3(2):1–18.

Sen, Amrita, Gunamani Jena, Subhashree Jena, and P. Devabalan. 2022. "A Case Study on

Journal of Law, Economics, and Engineering
ISSN 3123 - 5107
Vol. 1, No. 2 Tahun 2025
website: https://jolens.org/index.php/jolens
Defending against Cyber Crimes." 13(1):1931–38. doi: 10.47750/pnr.2022.13.S01.229.

Setiyawan, R. 2021. "Indonesian Online Shopping Practices in the COVID- 19 Pandemic Era : A Study of Culture and Cyber." *Jurnal Hukum Novelty* 12(01):29–44.

Sinaga, G. G., A. S. Jusuf, Y. Kornelius, and ... 2023. "Peran Otoritas Jasa Keuangan Terhadap Perbankan Sebagai Upaya Perlindungan Data Pribadi Nasabah Bank (Studi Kasus Kebocoran Data Nasabah Bank Syariah." *Jurnal Pendidikan Hukum* 2(3):56–78.

Sitorus, S. Y. H. 2023. *Data Pribadi Pengguna Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi Ditinjau Dari Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data*. repository.uki.ac.id.

Sulistianingsih, D., M. Ihwan, and A. Setiawan. 2023. "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)." *Masalah-Masalah …* 3(2):1–54.

Thaher, I. 2022. "Politik Hukum: Perlindungan Data Pribadi Pada Aplikasi Pedulilindungi Di Indonesia." *Jurnal Pendidikan Tambusai*.

Ulya Amaliya. 2009. "E-Commerce Di Singapura Dan Indonesia : Sebuah Perbandingan Kebijakan." *Jurnal Ilmu Sosial Dan Ilmu Politik* 1(e-commerce):1–21.

Wicaksana, R. H., and A. I. Munandar. 2020. "Perlindungan Data Pribadi Dengan Narrative Policy Framework: Kasus Serangan Siber Selama Pandemi Covid-19 (A Narrative Policy Framework Analysis of Data." *IPTEKKOM (Jurnal Ilmu Hukum)*.