Journal of Social Science Studies Vol. 5, No. 1, January 2025, pages 135 – 150

Civil Liability for Data Breach and Destruction of Digital Data as Corporate Assets within the Framework of Unlawful Acts

Ainor Rasid, Rommy Hardyansah, Rafadi Khan Khayru

Universitas Sunan Giri Surabaya, Indonesia

ARTICLE INFO

Article history:
Received 01 December 2024
Revised 08 December 2024
Accepted 15 December 2024

Key words:
Unlawful act,
Data breach,
Digital asset,
Immaterial compensation,
Data security,
PDP Law,
Cyber tort.

ABSTRACT

This normative legal study analyzes the construction of unlawful acts (onrechtmatige daad) in cases of data breach and destruction of digital data as corporate assets. The research focuses on how Article 1365 of the Indonesian Civil Code (BW) can be applied to deliberate or negligent security breaches, positioning data as a protected intangible asset. The method used is qualitative with content and comparative normative analysis of primary and secondary legal materials. The findings indicate that the elements of an unlawful ac unlawfulness, fault, loss, and causation can be fulfilled through progressive interpretation. Unlawfulness is established by violations of specific statutory duties under the Personal Data Protection Law, Trade Secrets Law, or the general duty of care derived from digital business norms. Fault, particularly negligence, is proven by deviation from security standards mandated by regulations such as Government Regulation 71 of 2019. Compensable losses include both material costs (emergency response, lost profits) and immaterial damage to corporate reputation, quantifiable through appropriate methodologies. A comparative perspective with the common law concept of cyber tort and Indonesian commercial court jurisprudence on immaterial loss provides valuable insights for refining legal constructs and compensation standards. This study concludes that the existing civil law framework is sufficiently flexible, yet recommends the development of judicial guidelines, professional valuation standards, and enhanced legal capacity to ensure effective and predictable legal recourse for digital asset violations.

INTRODUCTION

The growth of the digital economy has transformed business assets from tangible, measurable forms into high-value intangible assets, with digital data playing a central role. Data, in its various for such as customer databases, trade secrets, proprietary algorithms, and transaction records is at the core of modern companies' operations, differentiation, and competitive advantage. The reliance of digital business activities on reliable communication and secure identity management underscores that data security and management are essential to the sustainability of the digital economy (Sinambela et al., 2022). The economic value of data no longer lies in its storage medium, but rather in the information, knowledge, and patterns it contains, which can be processed for strategic decision-making, personalized marketing, and product innovation. This shift demands a new legal approach to viewing and protecting data not merely as a static object of copyright or trade secrets, but as a dynamic corporate asset that is vulnerable and requires special safeguards. Consequently, any action resulting in data leaks, destruction, or corruption can no longer be viewed merely as a technical glitch but as an attack on the integrity and economic value of the company itself (Umar et al., 2021).

Data security is a complex issue involving technical, managerial, and legal dimensions (Pratama et al., 2024). Threats to data can stem from intentional external cyberattacks, such as hacking, ransomware, and phishing, as well as from internal negligence, such as system configuration errors, the loss of storage devices, or employee behavior that violates security procedures. Individual traits and the level of competence employees hold in processing and analyzing organizational data have also been associated with how consistently security procedures are followed (Darmawan, 2017; Khairi & Darmawan, 2022). Data breach incidents that result

* *Corresponding author, email address:* ***rafadi.khankahyru@gmail.com***

in sensitive data being exposed to the public or unauthorized parties have the potential to cause multiple layers of losses. Direct losses may include the costs of system recovery, forensic investigations, and notifications to affected parties. However, indirect and long-term losses are often more significant, encompassing a decline in consumer trust, damage to brand reputation, loss of customers, legal claims, and sanctions from regulators. In a data-driven economy, a loss of trust can be fatal to a business's survival (Clarke, 2005).

Indonesia's traditional civil law framework, particularly the Civil Code (Burgerlijk Wetboek), does not yet explicitly recognize data as a distinct category of assets (da Santo et al., 2024). The development of the digital economy demonstrates that data serves not only as information but has become a strategic asset with economic value that plays a critical role in the continuity of business operations; consequently, the loss, damage, or leakage of data can result in legal consequences and financial losses for companies (Rahmani et al., 2024). Efforts to secure organizational data through emerging technological safeguards point to a shift in practice toward treating data as an asset requiring active protection rather than a mere byproduct of information systems (Costa et al., 2023). Obligations to disclose certain categories of organizational data have also begun to appear in other areas of corporate regulation, reflecting a broader legal trend toward treating data as an object of accountability (Mamesah et al., 2024). Article 1365 of the Civil Code (BW), which serves as the general basis for tort (onrechtmatige daad), is broadly defined: "Any act that violates the law and causes harm to another person obligates the person who, through their fault, caused such harm to compensate for it." This provision requires an evolutionary interpretation to encompass violations in the digital world. The fundamental question is whether actions such as data breaches or data destruction resulting from cybersecurity negligence can satisfy the elements of a "tort" as intended by Article 1365 of the Civil Code. To that end, it is necessary to analyze whether a failure to protect a company's data assets which is an implicit obligation in the reasonable management of a business can be considered a violation of a legal obligation or a subjective right of another party, or a violation of public morality and propriety in social interactions.

Law No. 27 of 2022 on Personal Data Protection (PDP Law) introduces a new though not yet comprehensive dimension in this context. The PDP Law primarily regulates the protection of personal data and establishes the obligations and responsibilities of Data Controllers and Data Processors. This is consistent with the view that the protection of privacy and personal data is becoming increasingly important in the digital age and must be guaranteed as part of the protection of individuals' fundamental rights. (Issalillah & Hardyansah 2024). A similar emphasis on protecting data privacy rights has emerged in sector-specific regulation, such as in banking, where customer data protection is treated as a distinct legal concern (Hardyansah et al., 2024). Violations of the provisions of the PDP Law, such as a failure to protect the security of personal data resulting in a data breach, can be categorized as statutory torts, as they violate the provisions of the law. However, the scope of the PDP Law is limited to personal data. Meanwhile, a company's data assets often consist of a mix of personal and non-personal data (such as operational data, research data, and metadata). The destruction or leakage of non-personal data of high commercial value is not directly regulated by the PDP Law; therefore, victims must rely on the general provisions of Article 1365 of the Civil Code. It is this gap that needs to be addressed through progressive legal interpretation.

The concept of cyber torts, which has developed within the common law system particularly in the United States offers an interesting comparative perspective. Cyber torts refer to unlawful acts that occur in or through cyberspace, encompassing a variety of actions such as cyber trespass, conversion of digital assets, negligent enablement of cybercrime, and the infliction of emotional distress through digital means (Brenner, 2007). Under this framework, data is treated as property or a protected legal interest. Unauthorized access to a computer system may be considered trespass to chattels, while the destruction or theft of data may be analogized to conversion. This approach acknowledges the unique nature of data as an asset and develops a specific tort doctrine to address the complexity of the resulting damages. The expanding use of big data, artificial intelligence, and interconnected systems across various industries illustrates how data has come to function as a core operational asset, lending weight to arguments for its legal protection as a proprietary interest (Putra & Arifin, 2021). An examination of the development of cyber torts and commercial court jurisprudence regarding immaterial damages in Indonesia can provide valuable guidance for establishing fair and proportionate standards of compensation for cases of digital data destruction.

The legal construction of an unlawful act under Article 1365 of the Civil Code for cases of data breaches and data destruction faces challenges in satisfying the element of "unlawfulness." In legal

doctrine, this element can be satisfied in three ways: by violating another person's subjective rights, by breaching a legal obligation, or by violating public morality and propriety. In cases of data destruction by internal or external parties, what subjective rights are violated? If data is considered an intangible asset, then ownership rights over that data can be claimed. However, Indonesian property law has not yet explicitly recognized data as an object of property rights. Alternatively, the violation can be viewed as a breach of the legal duty to maintain the confidentiality and security of data, which may arise from a contract, a fiduciary relationship, or statutory obligations such as those under the Personal Data Protection Act (PDP Act). Where such an obligation arises from a contract, the principle of good faith in contract performance offers a doctrinal basis for expecting parties to take reasonable measures in safeguarding data placed under their care (Irfansyah et al., 2024). However, these duties are often implicit and require interpretation, creating uncertainty. Furthermore, proving that the perpetrator (especially in the case of external cyberattacks) has a legal obligation toward the victim is difficult, unless there is a pre-existing contractual relationship.

Determining and proving damages in cases of digital data destruction is a highly complex issue. The damages resulting from a data breach are multifaceted and difficult to quantify accurately. Direct material damages, such as system recovery costs and notification expenses, are still relatively calculable. However, immaterial damages such as loss of reputation (goodwill), loss of business opportunities, and erosion of customer trust are abstract and speculative. Courts in Indonesia have not yet established consistent precedents or standardized methodologies for calculating this type of immaterial damage. Often, lawsuits can only seek nominal compensation for immaterial damages that do not reflect the actual losses. On the other hand, losses resulting from the destruction of operational data that halts production can be calculated based on the value of downtime, but this requires robust expert evidence and calculations. Organizational effectiveness depends on multiple interacting factors, which makes isolating the specific financial impact of a single data destruction incident from other operational variables particularly difficult (Darmawan, 2024). Beyond its effect on customers, the erosion of trust following a data incident may also weaken employee commitment within the organization, adding a layer of immaterial loss that is rarely accounted for in compensation claims (Eddine et al., 2023). Without clear assessment standards, efforts to obtain adequate compensation become ineffective.

The standard of liability is also a key issue. Is liability for data breaches a form of strict liability given the nature of data as a vital asset or is it based on fault? If it is based on fault, how high is the standard of duty of care that companies must meet in securing their data? On the one hand, data-holding companies are expected to implement adequate security measures in line with technological advancements (reasonable security measures). Failure to meet this standard may be considered negligence. Principles of ethics and accountability increasingly applied to managerial decisions involving artificial intelligence may offer a reference point for defining what constitutes responsible data governance within a company (Gani & Darmawan, 2022). However, determining what constitutes "adequate security measures" in an ever-evolving cyber threat landscape is a technical issue that also raises legal questions. Meeting evolving security standards also depends on an organization's capacity for continuous innovation in managing its human resources and internal capabilities, since technical safeguards alone cannot compensate for outdated organizational practices (Abdullah et al., 2021). Meanwhile, if the perpetrator of an external cyberattack remains unidentified, can the company, as the victim, sue other third parties such as IT service providers on the grounds of negligence in providing security? These questions highlight the immaturity of liability frameworks within the digital ecosystem.

The frequency and scale of cybersecurity incidents, including data breaches and ransomware attacks, continue to rise globally and in Indonesia. These attacks no longer target only government institutions or large technology companies but have also targeted small and medium-sized enterprises, healthcare institutions, and financial service providers. Each incident results in significant economic losses and disrupts operational stability. The capacity of organizations to learn collectively from prior security incidents plays a role in strengthening their long-term resilience against future attacks (Kurniawan & Darmawan, 2021). In this situation, a clear and effective civil legal framework for seeking damages is an urgent necessity. This framework serves not only as a post-incident remediation tool but also as a deterrent that encourages all actors in the digital ecosystem to improve their security standards. Without the threat of serious liability for damages, the incentive to invest in cybersecurity may diminish, creating negative externalities for the entire digital community. Appropriate leadership approaches are also needed to drive the organizational change

required to raise security standards across all levels of a company (Mardikaningsih & Darmawan, 2022).

The new Personal Data Protection Law that has come into effect has established new obligations and standards for personal data controllers. The growing use of artificial intelligence and big data in transforming organizational services shows that much of the data companies rely on extends beyond personal information, reinforcing the need for legal protection that also covers non-personal and operational data (Essa et al., 2024). However, as previously mentioned, its scope is limited. A study linking the PDP Law to the general legal framework for unlawful acts under the Civil Code holds strategic value. Such a study can help interpret and operationalize the security obligations under the PDP Law within the context of civil litigation. For example, a violation of Article 50 of the Personal Data Protection Act regarding the Data Controller's obligation to protect the security of personal data can directly serve as the basis for satisfying the element of "violating statutory provisions" under Article 1365 of the Civil Code. Thus, victims of data breaches involving personal data have a stronger basis for a lawsuit. However, further development is needed regarding how this relationship applies to non-personal data and how to assess the resulting damages.

From the perspective of legal scholarship, this topic offers opportunities to reinterpret and modernize classical civil law doctrines. The 19th-century concept of onrechtmatige daad is confronted with 21st-century realities. This process of adaptation represents a healthy and necessary dynamic within the law. In much the same way that organizations continually refine practices aimed at sustaining human resource quality, performance, and loyalty, legal doctrine must also evolve to remain responsive to the realities it is meant to govern (Darmawan et al., 2020). An in-depth study can contribute to the formation of Indonesian legal doctrine regarding "cyber tort" or unlawful cyber acts. This doctrine will serve as a theoretical foundation for judges, legal practitioners, and academics in addressing future digital disputes. Furthermore, by analyzing existing commercial court decisions regarding immaterial damages and business disruption, trends and principles can be identified that can be applied by analogy to cases of data destruction, thereby enriching Indonesia's body of jurisprudence in the field of cyber law.

This study aims to construct the application of Article 1365 of the Civil Code to data breaches and the destruction of digital data as corporate assets by analyzing the fulfillment of the elements of a tort. Furthermore, the study will examine the standards and methods for determining material and immaterial damages that may be claimed under Indonesian civil law, including the calculation of reputational damage and loss of business opportunities. The study will also analyze the concept of cyber torts in the common law system and the development of Indonesian commercial court jurisprudence regarding non-pecuniary damages as a basis for comparison to refine the legal framework. Theoretically, this study is expected to fill a gap in the discourse of Indonesian business civil law regarding the protection of data as an intangible asset and to develop a doctrinal framework for cyber torts. Practically, the research findings can serve as a reference for victimized companies in filing claims for damages, as a guideline for judges in adjudicating similar cases, and as input for policymakers in developing more comprehensive regulations.

RESEARCH METHOD

This study employs a qualitative literature review approach within the framework of normative legal research. The qualitative approach was chosen because it is well-suited to exploring, understanding, and interpreting the meaning of legal constructs, doctrines, and developments in case law within dynamic fields such as cyberlaw and data protection (Creswell, 2007). Normative legal research focuses on the examination of legal principles, positive norms, and the systematization of law to answer prescriptive questions (Marzuki, 2005). The primary objective is to construct a coherent legal argument grounded in textual evidence and court decisions to analyze the legal framework of tortious acts and standards of damages in cases of digital data destruction. Given its interpretive nature and its aim to fill regulatory gaps, a qualitative method involving in-depth literature review is the appropriate choice for unraveling the complexities of the relationship between classical civil law and the new digital reality.

All data used are secondary data, collected through documentation techniques from verified sources (Darmawan, 2015). Types of secondary data include primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials consist of laws and regulations, namely Article 1365 of the Civil Code (BW), Law No. 27 of 2022 on Personal Data Protection, Law No. 11 of 2008 on Electronic Information and Transactions along with its amendments, as well as related implementing regulations. Secondary legal sources include textbooks on civil law and cyberlaw, articles from accredited national and international academic

journals, scholarly works such as dissertations and theses, and official publications from relevant institutions. Tertiary legal sources, such as legal dictionaries and encyclopedias, were used to understand key terminology. Data collection was conducted systematically by identifying, cataloging, and analyzing these materials based on the main themes of the research namely, the construction of unlawful acts, standards of damages, and comparative perspectives on cyber torts to ensure a comprehensive scope of analysis.

The analytical techniques applied were qualitative content analysis and comparative normative analysis. Qualitative content analysis was used to extract patterns, themes, and ideas from secondary legal sources specifically academic literature and journals to understand the evolution of discourse and theoretical debates regarding the research topic (Krippendorff, 2004). Comparative normative analysis was applied to primary legal materials and case law. This technique involves legal interpretation (grammatical, systematic, historical, and teleological) of Article 1365 of the Civil Code and the provisions of the Personal Data Protection Act to examine the possibility of their application to data breach cases. Next, a comparative analysis was conducted on the concept of "cyber tort" in the common law system and relevant Indonesian commercial court decisions to identify principles that can be adopted or adapted. Through a synthesis of these various analytical techniques, this research will produce an in-depth critical review and a progressive legal framework to address all research questions.

RESULT AND DISCUSSION

The Legal Framework for Unlawful Acts Involving Data Breaches and the Destruction of Digital Data as Corporate Assets

The protection of digital data as a corporate asset and liability for its damage or leakage requires an adequate legal framework, especially when the entire data management process takes place electronically and across multiple systems. The extent to which personal data protection regulations are effectively enforced in the fintech sector is crucial, given the massive volume of data processed and the high risk of misuse or leaks that can result in both material and immaterial losses (Aziz et al., 2023). This is reinforced by a study highlighting the need to reconstruct legal mechanisms for restoring consumer rights in the event of personal data breaches in the digital finance and e-commerce sectors, as a form of system operators' liability for losses arising from negligence or data security breaches (Darmawan & Dirgantara, 2024). Large-scale data management also demands adherence to principles of fairness and the protection of vulnerable parties, as reflected in efforts to utilize big data while ensuring customer protection and preventing discrimination based on the information held (Bashori et al., 2024). Furthermore, patterns of legal violations arising from the use of digital technology indicate that the aspects of liability and proof of damages remain gaps that need to be clarified so that data is truly recognized as a valuable asset and protected by law (Sutanto et al., 2023). Companies' reliance on data processing and electronic systems in their business processes further underscores the importance of data security and compliance with data protection regulations (Osean et al., 2024).

Legal certainty regarding electronic transactions, the validity of agreements, and the allocation of obligations among parties constitute the second pillar underpinning the recognition of digital data as a valuable corporate asset. The validity of contracts formed electronically, including those involving artificial intelligence systems, requires a clear legal foundation to avoid uncertainty in the event of disputes regarding data damage or loss resulting from the performance of the agreement (Maulani et al., 2023). If, during the performance of the agreement, there is a breach of contract indicating fraud or negligence that results in the damage of data assets, then the legal framework for evidence and the determination of liability become crucial to resolving the dispute (Darmawan & Saputra, 2024). The principles of liability allocation and consumer protection in distribution agreements must also be consistently enforced so that each party bears its fair share of the risk, including risks related to the loss or damage of data assets during the course of the transaction (Kurniawan et al., 2024). In addition, the use of blockchain technology and data tracking systems can enhance the transparency and security trail of digital assets, while risk mitigation measures and the application of principles of fairness and redress in the digital space complement this protective framework in terms of risk management and law enforcement (Rahman et al., 2023; Eddine & Darmawan, 2024; Rianto et al., 2024). The global recognition of digital products and intellectual property rights for data-based works also reinforces the status of data as an asset of economic value that deserves protection from all forms of destruction or misuse (Apriyanto & Hardyansah, 2024).

Article 1365 of the Civil Code (BW) can be interpreted in an evolutionary manner to cover

digital violations such as data breaches. The application of Article 1365 of the Civil Code (BW) to cover data breaches and the destruction of digital data requires an evolutionary interpretation of the classic elements of a tort. The first element is the existence of an "unlawful act." Indonesian legal doctrine, which follows the legis et mores theory, states that an act can be deemed unlawful if it infringes upon another person's subjective rights, violates a legal obligation incumbent upon the perpetrator, violates public morality, or is contrary to the standards of propriety that must be upheld in social interactions. In the context of a data breach caused by an external cyberattack or internal negligence, a legal violation can be established through several avenues. First, as a violation of legal obligations set forth in specific laws. Law No. 27 of 2022 on Personal Data Protection (PDP Law), in Article 50, requires Data Controllers to protect Personal Data from processing disruptions, whether unlawful or inappropriate. Failure to fulfill this security obligation, resulting in a data breach, directly constitutes a violation of statutory provisions and thus satisfies the element of "unlawful conduct." Data breaches resulting from negligence or cyberattacks can be classified as civil liability through a violation of the PDP Act. This accountability framework establishes a company's failure to protect customer data as a basis for seeking redress for victims (Mujisulistyo et al., 2024).

UU Trade secrets serve as an important legal basis for protecting non-personal data in the digital context. For data that is not personal data such as operational data, proprietary algorithms, or trade secrets the legal basis for "unlawful acts" can be found in Law No. 30 of 2000 on Trade Secrets. Trade secrets are regulated under Law of the Republic of Indonesia No. 30 of 2000, which states that the scope of trade secret protection includes production methods, processing methods, sales methods, or other information in the fields of technology and/or business that has economic value and is not known to the general public (Dzulfania et al., 2024). Article 13 of this law states that no person shall, by unlawful means, obtain, disclose, or use a trade secret belonging to another party. Unauthorized access to a company's systems to steal or damage data classified as a trade secret clearly constitutes a violation of this law. Furthermore, a violation can be viewed as an act contrary to the standards of propriety in the business community. Standards of propriety in the modern digital society require every entity that manages critical digital assets to exercise a reasonable duty of care. A company that completely disregards basic cybersecurity practices and is therefore easily hacked may be deemed to have acted improperly and violated the social norms prevailing in the business community. Breaches of trade secrets and cybersecurity negligence can be classified as torts in modern digital society (Disemadi & Budi, 2023).

The element of fault encompasses dolus and culpa, forming the basis of the principle of liability in both criminal and civil law. The second element is "fault," which encompasses intent (dolus) and negligence (culpa). The principle of liability based on fault (Fault Liability or Liability based on fault) is a principle that is quite commonly applied in both criminal and civil law (Rahadita et al., 2023). In cases of data breaches resulting from external cyberattacks by unknown third parties, proving the external perpetrator's intent against the victim company may be difficult in a civil lawsuit. However, the element of fault can be shifted or shared. The focus often shifts to whether there was negligence on the part of the victim company itself or on the part of a third party with a legal relationship to the victim (e.g., an IT service provider). Negligence (culpa) occurs when a person fails to do what they are legally required to do, or acts in an improper manner. The standard for determining negligence is the "reasonable person" standard. In the context of data security, the question is: Has the company taken reasonable security measures in accordance with the nature, value, and risks associated with the data it holds? Failure to implement encryption, multi-factor authentication, regular security software updates, or security awareness training for employees can be used as evidence of negligence. Negligence in implementing reasonable security measures can serve as the basis for proving fault in data breach cases (Wright & Pilavci, 2021).

The ITE Law and Government Regulation No. 71 of 2019 establish security obligations for electronic systems that may serve as the basis for negligence per se. Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), together with Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions, provide clearer parameters regarding security obligations. Article 15 of Government Regulation No. 71 of 2019 requires Electronic System Operators to ensure the availability, reliability, security, and continuity of their electronic systems. A violation of this statutory obligation may be considered negligence per se that is, negligence that is automatically proven because it violates statutory provisions. Thus, if a data breach occurs and it can be proven that the company failed to meet the minimum security standards mandated by Government

Regulation No. 71 of 2019, the element of fault (in the form of negligence) is satisfied. This approach is particularly strong because it reduces the plaintiff's burden of proving an abstract standard of care; it is sufficient to prove a violation of applicable regulations. "Negligence per se" simplifies the proof of negligence because it suffices to demonstrate a violation of a statutory duty.

Digital losses as an element of tort liability encompass both material and immaterial dimensions recognized under civil law. The third element is "loss." Digital data, as a corporate asset, has economic value that can be subject to loss in various forms (Degtyarev & Boyarskiy, 2022). Direct material damages may include: the cost of digital forensic investigations to identify the source and scope of a breach; system and data recovery costs; the cost of providing legally required notifications to customers and authorities (as mandated by the Personal Data Protection Act); the cost of providing credit monitoring or identity protection services to victims; and fines or administrative sanctions imposed by regulators. Indirect material losses may include loss of profit due to business operational disruptions during system downtime, or the loss of customers who switch to competitors due to a loss of trust. Immaterial losses are primarily related to reputational damage (loss of goodwill) and erosion of brand trust. Data management through digital systems can also influence users' perceptions of fairness and trust, especially when decision-making processes take place through mechanisms that lack transparency (Rojak et al., 2024). Although difficult to quantify, these non-pecuniary damages are recognized under civil law, and compensation may be sought for them, provided that a causal link can be proven and the claim is supported by a reasonable calculation. Digital damages may take the form of actual costs or reputational harm, both of which are valid grounds for seeking compensation (Begnini & Ortiz, 2024).

Causal connection is a crucial element in linking a tortious act to damages resulting from a data breach. The fourth element is the "causal connection" between the tortious act and the resulting damages. Proving causation in data breach cases is technical in nature and requires specialized expertise (Rolle, 2023). The plaintiff must demonstrate that the damages suffered (e.g., recovery costs or loss of customers) were actually caused by the data breach incident itself, and not by other factors. This proof relies on electronic evidence and testimony from cybersecurity forensic experts. System access logs, firewall records, attack timelines, and malware analysis results must be pieced together to form a chronological narrative demonstrating how a security lapse (e.g., an unpatched vulnerability) was exploited by the attacker, leading to data exfiltration, and how the incident subsequently resulted in the various costs and damages as alleged (Geistfeld, 2017). Article 5 of the ITE Law, which recognizes electronic information as admissible evidence, provides a strong foundation for using this technical evidence in civil proceedings. Causality in a data breach is proven through a chain of electronic evidence that is admissible under the ITE Law.

Article 1367 of the Civil Code extends liability to employers for the acts of their subordinates within the scope of their employment. Article 1367 of the Civil Code, concerning the liability of employers and persons in a position of trust, broadens the scope of liability. Paragraph (1) states that an employer or a person entrusted with authority is liable for losses caused by subordinates or persons under their supervision, provided that such losses result from errors committed in the course of performing work (Dita & Winanti, 2023). This legal framework is highly relevant to data breaches caused by employees, whether due to malicious acts (insider threats) or negligence (e.g., clicking on a phishing link). The company, as the principal, may be held liable for damages resulting from such employee actions. However, the company may also use this provision to sue negligent employees if the resulting losses are substantial. Furthermore, liability may be shifted to the IT outsourcing service provider if the contract stipulates specific security obligations and it can be proven that the breach occurred due to their negligence. Article 1367 of the Civil Code allows for joint and several liability: the company, the employee, and the outsourcing party may all be held liable for damages.

Article 1365 of the Civil Code can be interpreted progressively to cover data breaches and the destruction of digital data. The legal construction of tort liability under Article 1365 of the Civil Code can effectively cover data breaches and the destruction of digital data. The element of "unlawful act" is satisfied through a violation of the Personal Data Protection Act (for personal data), the Trade Secrets Act (for confidential data), or standards of business due diligence. The element of "fault" may take the form of a company's negligence in implementing reasonable security measures, which is often elevated to "negligence per se" due to a breach of obligations under the Information and Electronic Transactions Act (ITE) and Government Regulation No. 71/2019 (Ningsih & Wahyudi, 2024). The element of "damages" may encompass various forms of material

and immaterial losses incurred. The element of "causal link" is proven through a chain of electronic evidence and expert testimony. Victims of data breaches have a strong basis for a civil lawsuit to seek damages from the direct perpetrator, from the company that failed to secure its systems, or from liable third parties. This framework recognizes data as a valuable asset protected by law and imposes a duty of care on every party that manages it. Article 1365 of the Civil Code (BW) affirms data as a legal asset, with civil lawsuits serving as an instrument of protection.

Standards and Determination of Compensation for Material and Immaterial Damages Resulting from a Data Breach

Articles 1366 and 1367 of the Civil Code establish the standard for damages to restore the aggrieved party to their original position. The standard for damages in Indonesian civil law, particularly those arising from unlawful acts, is regulated in Articles 1366 and 1367 of the Civil Code. These articles stipulate that damages include costs incurred to remedy the loss, lost profits, and interest. Compensation must restore the aggrieved party to the position they would have been in had the tort not occurred, to the extent that this can be estimated and proven. In the context of data breaches and the destruction of digital data, applying this standard requires a specialized methodology because the subject matter of the loss is intangible and dynamic. Damages are clearly distinguished into material damages, which can be directly quantified in monetary terms, and immaterial damages, which relate to non-economic values such as reputation and trust. Both types of damages may be claimed simultaneously in a single lawsuit, provided that a causal link to the defendant's actions can be proven. Both material and immaterial damages resulting from a data breach may be claimed simultaneously as long as causality is proven.

Damnum emergens covers all actual costs incurred as a result of the data breach incident response. Material damages consist of two main components: damnum emergens (actual losses suffered) and lucrum cessans (lost profits). Damnum emergens in the case of a data breach covers all incident response costs incurred by the victim company. These costs vary widely and must be carefully documented. Examples include the costs of a third-party digital forensic investigation to identify the source, method, and scope of the attack (Poyraz et al., 2020). The technical and volatile nature of digital evidence makes forensic investigation a crucial part of identifying the source, methods, and scope of an attack (Hartana et al., 2024). Biaya pemulihan sistem dan data, termasuk upaya rekonstruksi data yang rusak atau terenkripsi oleh ransomware. Biaya pemberitahuan hukum to customers, regulators such as the Personal Data Protection Authority, and other affected parties, as required by the Personal Data Protection Act. The costs of providing identity monitoring services or compensation to customers whose data has been compromised, as well as the costs of post-incident system security enhancements both corrective and preventive (Furnell et al., 2020). All of these costs constitute actual losses that directly deplete the company's cash reserves. Damnum emergens refers to tangible losses that can be calculated and proven as the basis for compensation.

Lucrum cessans refers to lost profits resulting from business disruptions following a data breach. The lucrum cessans component or lost profits is more complex to prove. These losses arise from disruptions to business operations that result in lost revenue. For example, if a data breach causes an e-commerce system to be completely down for several days, the revenue that would have been earned during that period can be claimed as lucrum cessans (Frimpong & Chen, 2021). Similarly, if a leak of trade secrets allows competitors to take advantage of them, causing the company to lose specific projects or contracts. Proving lucrum cessans requires robust historical financial data, such as average daily revenue, sales projections prepared prior to the incident, and an analysis demonstrating that the revenue decline was specifically caused by the data breach and not by other market factors. Without strong evidence, a lucrum cessans claim risks being rejected by the court as speculative. Lost profits can only be compensated if proven with concrete financial data and clear causality (Butkevičius, 2019).

The valuation of data assets in civil damages claims requires the adaptation of methods for valuing intangible assets. The method for assessing damages for data assets when the data is totally or partially destroyed requires a valuation approach (Prawoto, 2021). Three main approaches used in the valuation of intangible assets can be adapted. The cost approach calculates the cost required to recreate or replace the lost data. This includes the cost of re-collecting data, purchasing data from other sources, or reconstructing it through reverse engineering. The income approach estimates the present value of future income streams lost because the data can no longer be utilized. For example, if a customer database is lost, the discounted value of the expected profits from that database over its useful life can be calculated. The market approach seeks comparable

prices from transactions involving the sale of similar databases in the market. Companies' reliance on data analytics and big data in strategic decision-making further underscores that data is an asset with economic and strategic value; thus, the loss, corruption, or disruption of access to data can affect a company's performance and competitive advantage (Ali & Darmawan 2023). Although this approach is challenging due to the lack of a liquid market for business data, valuations can be based on corporate acquisitions in which the database is a key component of the company's value. The cost, revenue, and market approaches provide a complementary framework for assessing losses related to digital data assets (Raschke et al., 2020).

Non-economic damages in the form of reputational harm require a quantification methodology so that claims are not deemed speculative. Compensation for non-economic damages, particularly for reputational harm (loss of goodwill), is the most challenging aspect. Reputation is an intangible asset that is highly valuable but difficult to measure. Under Indonesian civil law, compensation for non-economic damages may be sought (Hartiwiningsih & Rustamaji, 2023). To ensure these claims are not deemed speculative, the aggrieved company must develop a quantification methodology. Methods that can be used include: Valuation based on the costs of reputation restoration, such as the costs of crisis communication campaigns, public relations, and marketing efforts to restore the company's image. Comparative analysis of business metrics before and after the incident, such as a decline in the customer churn rate, a decrease in brand value in periodic surveys, or a drop in website traffic and social media engagement that is statistically correlated with the timing of the incident. Brand valuation studies conducted by experts, which measure the impact of the incident on overall brand equity. Reputational losses can be the subject of a lawsuit if quantification is performed using cost-based methods, business metrics, and brand valuation (Moraru, 2024).

Causation of non-economic damages resulting from a data breach must be proven through a systematic chain of evidence. Proving causation between a data breach and non-economic damages, such as reputational harm, requires a meticulous approach. To be able to claim damages from a person who has committed a tort, in addition to the existence of fault, there must also be a cause-and-effect relationship or causal link between the tort, the fault, and the resulting damages; thus, the only damages for which compensation may be claimed are those actually caused by the tort in question (Budianto, 2023). The plaintiff must demonstrate that the decline in customer or business partner trust was specifically caused by media coverage or public awareness of the data breach incident, and not by other factors such as an economic crisis or unrelated scandals. Evidence that may be submitted includes: customer survey results asking why they canceled their subscriptions or reduced their purchases; media analysis showing an increase in negative sentiment toward the brand in the post-incident period; and written statements from business partners expressing concerns or canceling their cooperation due to the data security incident. This chain of evidence must be constructed systematically. Reputational causation requires measurable evidence that directly links the data breach to immaterial losses (Sugiarto et al., 2024).

The Personal Data Protection Act (PDP Act) adds a new dimension of compliance-related losses in the form of notification costs and administrative sanctions. The Personal Data Protection Act introduces a new dimension of compliance-related losses. Article 57 of the PDP Act requires Data Controllers to notify Data Subjects and the Authority of any personal data breaches. This notification process incurs significant administrative, communication, and logistical costs, especially if the number of Data Subjects reaches the thousands or millions. In addition, the Authority may impose administrative sanctions in the form of very large fines under Article 58 of the PDP Law. In a civil lawsuit, notification costs and potential administrative fines (if already determined) may be included as part of damnum emergens. The argument is that these costs and fines are a direct consequence of the defendant's negligence in protecting the data. However, for fines that have not yet been imposed, the court may wait for a final decision from the Authority before including them as certain damages. Compliance costs and administrative fines resulting from the PDP Act may qualify as damnum emergens if proven.

Article 1367 of the Civil Code (BW) allows for joint and several liability when more than one party is negligent. In cases where more than one party is at fault for example, a negligent employee and an external IT service provider who is also negligent the liability to pay damages may be joint and several (solidair) under Article 1367 of the Civil Code (BW). However, the court will determine the extent of each party's contribution to the loss. This determination depends heavily on a cause-and-effect analysis. If it can be proven that the data breach occurred due to a combination of vulnerabilities in the company's

internal systems and a failure of the service provider's intrusion detection system, then both parties may be deemed to have contributed and held liable on a proportional basis. A lawsuit may be filed against one or all of the liable parties. Joint and several liability gives the victim flexibility in filing a claim, while the proportion of liability is determined through a causality analysis (Perkasa & Saly, 2022).

Expert testimony serves as a crucial tool in proving damages resulting from a data breach. The role of expert testimony is central to determining the standard and amount of damages. Experts provide specialized knowledge that assists judges in conducting a more in-depth analysis of the available evidence and supplies the information upon which judges base their fair and appropriate decisions (Hidayat et al., 2024). At least three types of experts are required: a digital forensics expert, to establish the chronology of the attack, the point of entry, the techniques used, and the scope of the affected data; an accounting expert or appraiser, to assess the economic value of lost or damaged data, calculate damnum emergens and lucrum cessans using recognized methods, and evaluate reputational damage. Marketing or communications experts, to analyze the impact of an incident on market perception, customer loyalty, and brand value (Mardikaningsih et al., 2024). This expert report must be comprehensive, transparent in explaining its assumptions and methodology, and capable of withstanding cross-examination in court. The quality of expert testimony often determines whether the majority of claims for damages are accepted or rejected. The strength of the expert report determines the success of a damages claim in data breach cases (Romanosky et al., 2013).

Standards for damages in data breach cases require a composite approach with strict standards of proof. Based on the above analysis, it can be concluded that the standards and methods for determining damages for data breaches and the destruction of digital data under Indonesian civil law are composite in nature and require rigorous proof (Aura et al., 2025). These standards are based on the principle of full compensation, which encompasses actual costs, lost profits, and non-economic damages. The determination methods integrate a cost-accounting approach, valuation of intangible assets, and business impact analysis supported by electronic evidence and multidisciplinary expert testimony. Success in claiming adequate damages depends heavily on the victim's ability to document every loss, establish a strong chain of causation, and present reasonable and non-speculative calculations before the judge. With this systematic approach, Indonesian civil law actually possesses sufficient tools to provide substantive financial relief to victims of cybercrime, while simultaneously fostering a culture of accountability in the management of digital data. Indonesian civil law provides an adequate framework for financial relief and digital accountability.

A Comparative Perspective: Cyber Torts and Case Law on Non-Pecuniary Damages in Indonesian Civil Law

Cyber torts in common law reflect a progressive adaptation to digital harms. The development of the concept of cyber torts within the common law system particularly in the United States and the United Kingdom offers a legal perspective that is highly responsive to harms in the digital world (Kamilah, 2024). Cyber torts are adaptations of traditional tort doctrines such as negligence, trespass to chattels, conversion, and breach of confidence, designed to address harmful acts occurring through or against computer systems and data. Online criminal offenses include offenses against chattels, embezzlement, cyber harassment, and cyber defamation *(Dhantole & Pandey, 2024).* In the United States, courts have recognized negligence claims against data controllers who fail to implement reasonable security measures, as seen in cases against companies that have experienced data breaches. The elements of duty of care, breach of duty, causation, and damages are applied with due consideration to security standards in the technology industry. Furthermore, the doctrine of trespass to chattels originally intended for tangible objects has been expanded to protect computer systems from unauthorized access that results in damage or disruption. This evolution demonstrates the common law system's ability to fill regulatory gaps through progressive judicial interpretation, creating precedents that can serve as references for other jurisdictions. Cyber torts demonstrate the flexibility of the common law in protecting digital systems through the expansion of traditional tort doctrines.

The transformation of "breach of confidence" into "misuse of private information" has expanded privacy protections in the United Kingdom. In the UK, a significant evolution has taken place in the tort of breach of confidence, which has transformed into the tort of misuse of private information. This development was driven by the European Convention on Human Rights, which recognizes the right to respect for private life. This new tort no longer requires a specific relationship of trust; it is sufficient to prove that there was a reasonable expectation of confidentiality regarding the information and that the

use of that information without consent caused harm. In the case of Vidal-Hall v. Google Inc., the British court recognized that psychological distress resulting from a privacy violation can serve as the basis for independent damages, without the need to demonstrate direct financial loss. This principle is highly relevant to corporate data breach cases, as it acknowledges that harm is not always financial in nature but can take the form of eroded trust, infringement of data autonomy, and operational pressures that are immaterial yet real. The principle of misuse of private information affirms that immaterial harm resulting from a privacy violation is eligible for compensation.

Indonesian case law has begun to recognize non-economic damages, albeit with a cautious approach. Case law from commercial and general civil courts in Indonesia has, in fact, begun to recognize and award non-economic damages, albeit with great caution. Judgments related to corporate defamation or trademark infringement often award non-economic damages in addition to economic damages. In these cases, judges typically consider the extent of the negative publicity, the degree of the defendant's fault, and the impact on the plaintiff's reputation and market share. However, the methodology for calculating such damages is often not fully transparent and tends to rely on an "equitable assessment" rather than strict economic calculations. This approach indicates there is room to develop more structured standards of proof and quantification, as is done in common law through expert testimony on brand valuation and econometrics. The recognition of non-economic damages opens the door for Indonesia to adopt more measurable quantification methodologies.

Cyber torts emphasize a duty of care based on industry standards, which are relevant when adopted in the Indonesian context. An important lesson from common law cyber torts is the reinforcement of the duty of care based on industry standards and specific regulations. Courts in the U.S. often refer to security frameworks such as the Payment Card Industry Data Security Standard (PCI DSS) or industry-recognized reasonable security measures to determine whether negligence exists. In Indonesia, similar standards can be found in Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions, as well as various regulations issued by sectoral authorities (OJK, Bank Indonesia) regarding information technology risk management. Violations of these technical standards can and should be used as strong evidence of a breach of duty under Article 1365 of the Civil Code. Thus, the courts do not need to create new standards but need only adopt and enforce the standards already established by technical regulators, which serve as concrete parameters for the duty of due care in data management. Regulatory technical standards serve as concrete benchmarks for the courts in assessing negligence in data management.

Class actions offer efficiency in enforcing the law in cases of mass data breaches. The concept of representative action or class action in common law provides inspiration for efficient enforcement of the law in cases of mass data breaches involving many corporations or consumers. This mechanism allows a group of victims with similar claims to sue collectively, reducing the costs of individual litigation and creating a greater deterrent effect. PERMA No. 1 of 2002 defines a Class Action as a procedure for filing a lawsuit in which one or more individuals, acting as representatives of a group, file a lawsuit on their own behalf and simultaneously on behalf of a large group of people who share common facts or a common legal basis between the group representatives and the group members (Memah et al., 2023). Although Indonesia has a class action mechanism established under Supreme Court regulations, its use in cyber cases remains very limited. Courts could develop special procedures for data breach cases that allow for collective proof of general facts such as the occurrence of an attack and basic security negligence while the calculation of individual damages can be conducted later. This approach could address the difficulties faced by individual victims particularly small and medium-sized businesses in bearing the costs of expensive forensic and expert evidence. Class actions in the cyber realm have the potential to strengthen access to justice and reduce the costs of evidence for mass victims.

Common law offers a quantitative methodology for proving immaterial damages resulting from a data breach. When it comes to proving immaterial damages, common law has developed a methodology that can be adopted. Courts often accept expert reports that use techniques such as event studies to isolate the impact of a negative event (such as the announcement of a data breach) on a company's stock price. An abnormal decline in stock prices around the announcement date can serve as an accepted proxy for measuring reputational damage and loss of investor confidence. This is consistent with the focus on the impact of data management on trust, autonomy, and the relationship between data-controlling companies and users (Fared & Darmawan 2021). For privately held companies or those not listed on a stock exchange, alternative methods such as analyzing post-

incident customer churn rates, declines in brand equity as measured by periodic surveys, or estimating the costs required for a reputation recovery campaign may be used. The key to their acceptance is transparency in methodology, the use of reliable data, and the expert's ability to defend their assumptions in court. Data-driven methodologies and expert transparency make claims for immaterial damages more credible in court.

The remedial aspect of cyber torts emphasizes holistic redress through damages and injunctive relief. The remedial aspect of cyber torts also provides valuable insights. In addition to monetary damages, common law courts often grant injunctive relief that is, a court order to cease a certain action or to take specific actions. In the context of a data breach, this may take the form of an order directing the defendant to immediately patch system vulnerabilities, delete stolen data from their servers, or implement an independent security audit program. Commercial court judges in Indonesia have similar authority under civil procedure law to issue judgments that are condemnatory (imposing penalties) and constitutive (establishing a new legal status). The use of court orders mandating specific corrective actions can be an integral part of a more holistic remedy, as it addresses the root causes of security issues and prevents ongoing harm. Specific corrective orders strengthen remediation, prevent recurring harm, and enforce digital accountability.

The economic loss rule emphasizes the importance of choosing the appropriate legal basis for a claim in cases involving digital losses. The challenges posed by the economic loss rule in common law which limits negligence claims to purely economic losses without physical injury or property damage highlight the importance of selecting the appropriate legal basis for a claim. In Indonesia, the dichotomy between breach of contract and tort (based on Article 1365 of the Civil Code) already exists. In data breach cases involving third-party service providers, victims may combine both legal bases: a breach of contract claim for violating security clauses in the contract, and a tort claim for broader losses suffered by parties outside the contract or resulting from a violation of general legal obligations. The court must carefully allocate liability to prevent double recovery while ensuring that all valid losses are compensated. Combining breach of contract and tort claims allows for comprehensive recovery, provided that liability is allocated carefully.

Indonesia's Personal Data Protection Act (PDP Act) parallels common law practices in establishing data breaches as grounds for civil lawsuits. Indonesia's Personal Data Protection Act has parallels with data protection laws in various common law countries. Violations of obligations under the PDP Act, such as failing to protect data security or failing to report a breach, can directly serve as grounds for civil claims. Experience in the United Kingdom shows that the data protection regulator (ICO) often plays an active role, and its investigative findings can be used as evidence in individual or class-action civil lawsuits. In Indonesia, future findings from investigations by the Personal Data Protection Authority could serve as very strong preliminary evidence in civil lawsuits, expediting the process of proving the element of "unlawful conduct." The data regulator's findings have the potential to become key evidence that strengthens civil claims for violations of the Personal Data Protection Act.

A comparative analysis reveals convergence between common law cyber torts and Indonesian case law. Based on this comparative analysis, it can be concluded that the development of cyber torts in common law and the jurisprudence on non-economic damages in Indonesia complement one another and point toward convergence. Common law offers a more developed doctrinal framework and sophisticated methodologies for proving damages. Meanwhile, Indonesian jurisprudence demonstrates the courts' willingness to award non-economic damages, though it requires a more structured and scientific standard of proof. The legal framework and standards for damages in Indonesia can be refined by: first, explicitly adopting the security standards from Government Regulation No. 71 of 2019 and sector-specific regulations as parameters for the duty of care in tort cases; second, developing guidelines for the admissibility of expert evidence to quantify non-pecuniary damages based on valid economic methodologies; third, utilizing constitutive court rulings to mandate system improvements; and fourth, facilitating an efficient class-action mechanism for cases of mass data breaches. With these steps, Indonesian civil law can become a more effective and predictable instrument in delivering justice and redress to victims of digital data breaches. The convergence of doctrine and practice makes Indonesian civil law better prepared to face the challenges of the digital age.

CONCLUSION

Based on the normative study that has been conducted, it can be concluded that the legal framework for unlawful acts (PMH) under Article 1365 of the Civil Code can be effectively applied to

address data breaches and the destruction of digital data as corporate assets. The elements of an unlawful act an unlawful act, fault, damage, and a causal relationship can be satisfied through a progressive interpretation. An unlawful act can be established based on a violation of specific obligations under the Personal Data Protection Act (for personal data), the Trade Secrets Act, or standards of due diligence in digital business practices that require the implementation of reasonable security measures. The element of fault, whether intentional or negligent, can be proven by demonstrating a deviation from security standards mandated by regulations such as Government Regulation No. 71 of 2019. Damages include material losses (damnum emergens and lucrum cessans) and immaterial losses (reputational damage), which, although challenging, can be quantified using appropriate methodologies. Causal relationships are established through a chain of electronic evidence and expert testimony from digital forensics experts. Thus, the tort framework provides a sufficiently flexible legal foundation for civil liability regarding the destruction of data assets.

The findings of this study have important implications for three stakeholder groups. For data-holding companies, the primary implication is the need to view data security not merely as a technical or compliance issue, but as an integral part of legal risk management. Investments in security systems, policy documentation, and employee training not only prevent attacks but also serve as defensive evidence of compliance with the duty of care in the event of a lawsuit. Companies should also consider cyber insurance that covers incident response costs and potential third-party damages. For law enforcement and the judiciary, the implications of this research are a call to enhance technical capacity. Judges and attorneys need to be equipped with a basic understanding of digital forensics, information security standards, and methods for valuing intangible assets so they can properly assess evidence and expert testimony. High-quality rulings will establish case law that provides certainty and guidance for the parties involved. For policymakers and regulators, the implications of this research are the need for coordination to formulate more operational technical guidelines regarding "reasonable security measures" and incident reporting standards, which can serve as a standard reference for courts in assessing elements of negligence.

To refine the legal framework and standards for compensation, several policy recommendations are proposed. First, the Supreme Court, together with the Ministry of Communication and Information Technology and the Personal Data Protection Authority, needs to develop Technical Judicial Guidelines for Handling Civil Lawsuits Arising from Data Breaches and the Destruction of Digital Data. These guidelines must include an explanation of the elements of tort liability tailored to the characteristics of data as an asset, examples of admissible electronic evidence, as well as methods and principles for calculating material and immaterial damages that are acceptable to the courts. Second, professional associations such as the Indonesian Association of Digital Forensic Experts and the Indonesian Institute of Certified Public Accountants must develop and publish professional standards for the valuation of digital data and the calculation of business losses resulting from cyber incidents, so that expert reports possess reliable quality and consistency. Third, in the long term, consideration should be given to amending the Civil Code or enacting a special law that explicitly recognizes digital data as the subject of specific rights (such as property rights or economic interests) and establishes strict liability for certain actors in the chain of critical digital service providers. Fourth, legal education institutions should incorporate courses on Cyberlaw and Digital Assets into their core curriculum to prepare a generation of legal professionals and practitioners who understand these complexities from the outset. These steps are expected to build a legal ecosystem that is better prepared, fairer, and more effective in protecting digital assets, which form the backbone of the modern economy.

REFERENCES

Abdullah, M. H. A. B., Gardi, B., & Darmawan, D. (2021). Innovation in Human Resource Management to enhance Organizational Competitiveness in the Era of Globalization. *Journal of Social Science Studies*, 1(1), 51–58.

Ali, R., & Darmawan, D. (2023). Big Data Management Optimization for Managerial Decision Making and Business Strategy. *Journal of Social Science Studies,* 3(2), 139-144.

Apriyanto, R., & Hardyansah, R. (2024). Legal Dynamics and Challenges in Protecting Intellectual Property Rights For Digital Products in The Global Marketplace. *Journal of Social Science Studies*, 4(2), 261–276.

Aura, A., Priowirjanto, E. S., & Dewi, C. T. I. (2025). Privacy Protection Guarantee for Data Hacking Victims According to Indonesian Law. *Padjadjaran Journal of International Law*, 9(1), 1-15.

Aziz, A., Darmawan, D., Khayru, R. K., Wibowo, A. S., & Mujito. (2023). Effectiveness of Personal Data

Protection Regulation in Indonesia's fintech sector. *Journal of Social Science Studies*, 3(1), 23–28.

Bashori, B., Hardyansah, R., & Darmawan, D. (2024). Legal Analysis of Big Data and Analytics in Preventing Discrimination and Protecting Insurance Customers. *Journal of Social Science Studies*, 4(1), 185–192.

Begnini, I. M., & Ortiz, A. P. N. (2024). Compensation For Moral Damages in Case of Data Leakage: Jurisprudential Analysis of The Court of Justice of The State of Paraná. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, 10(1), 1022-1039.

Budianto, F. (2023). Tinjauan Hukum Mengenai Perbuatan Melawan Hukum dalam Transaksi Jual Beli Melalui Internet (E-Commerce) Dihubungakan dengan Buku III KUH Perdata. *Ekonomika45: Jurnal Ilmiah Manajemen, Ekonomi Bisnis, Kewirausahaan*, 11(1), 152-171.

Butkevičius, R. (2019). Universal Model of Lost Profits Calculation. *Ekonomika*, 98(2), 97-111.

Clarke, R. (2005). *Privacy as a Means of Protecting Personhood.* Oxford University Press, Oxford.

costa, S. da., Darmawan, D., & Isaac, A. de J. (2023). Safeguarding Employee Data with Blockchain in HR. *International Journal of Service Science, Management, Engineering, and Technology,* 4(3), 41–46.

Creswell, J. W. (2007). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (2nd ed.). Sage Publications, Thousand Oaks.

da Santo, M. F. O., Sari, L., Kamilah, A., & Reumi, F. (2024). *Pengantar Hukum Perdata: Teori & Referensi Komprehensif Dasar-Dasar Hukum Perdata di Indonesia*. PT. Sonpedia Publishing Indonesia, Jambi.

Darmawan, D. (2015). *Metodologi Penelitian*, Metromedia, Surabaya.

Darmawan, D. (2017). The Effects of The Big Five Personality on Job Performance. *Management & Accounting Research Journal*, 2(1), 36–42.

Darmawan, D. (2024). Distribution of Six Major Factors Enhancing Organizational Effectiveness. *Journal of Distribution Science*, 22(4), 47-58.

Darmawan, D., & Dirgantara, F. (2024). Reconstruction of the Legal Mechanism For Consumer Rights Recovery Regarding Personal Data Leaks In The Financial Technology And E-Commerce Sectors In Indonesia. *Journal of Social Science Studies*, 4(1), 75–84.

Darmawan, D., & Saputra, R. (2024). Legal Construction of Breach of Contract Indicating Fraud in Business Cooperation Agreements. *Journal of Social Science Studies*, 4(2), 319–332.

Darmawan, D., Mardikaningsih, R., Sinambela, E. A., Arifin, S., Putra, A. R., Hariani, M., Irfan, M., Al Hakim, Y. R., & Issalillah, F. (2020). The Quality of Human Resources, Job Performance and Employee Loyalty. *International Journal of Psychosocial Rehabilitation*, 24(3), 2580-2592.

Debora, Brenner, S. W. (2012). *Cybercrime and the Law: Challenges, Issues, and Outcomes*. Northeastern University Press, Boston.

Degtyarev, S. L., & Boyarskiy, D. A. (2022). Impact of valuation concepts (categories) in modern conditions on the recovery of "digital losses." *SHS Web of Conferences*, *134*, 00097–00097.

Dhantole, S., & Pandey, S. K. (2024). Cyber Torts: Unfolding Trends of Common Law. *Educational Administration: Theory and Practice*, 30(5), 7923-7931.

Disemadi, H. S., & Budi, H. S. (2023). Enhancing Trade Secret Protection amidst E-commerce Advancements: Navigating the Cybersecurity Conundrum. *Jurnal Wawasan Yuridika*, *7*(1), 21–43.

Dita, S. A., & Winanti, A. (2023). Analisis Asas Vicarious Liability dalam Pertanggungjawaban Pengganti atas Perbuatan Melawan Hukum Pegawai Bank. *Jurnal USM Law Review*.

Dzulfania, R., Karyati, S., & Haerani, R. (2024). Tinjauan Yuridis Pengaturan Rahasia Dagang Menurut Hukum Positif di Era Digital di Indonesia. *Iuris Notitia: Jurnal Ilmu Hukum*, 2(2), 64-70.

Eddine, B. A. S., & Darmawan, D. (2024). Supply chain management optimization with IoT and blockchain technology to increase efficiency and transparency. *Journal of Social Science Studies*, 4(2), 31–36.

Eddine, B. A. S., Darmawan, D., Mardikaningsih, R., & Sinambela, E. A. (2023). The Effect of Knowledge Management and Quality of Work Life on Employee Commitment. *Journal of Human Sciences,* 10(1), 87-100.

Essa, N. E., Mardikaningsih, R., & Ismail, A. B. (2024). Service Transformation through Technology the Role of AI and Big Data in Service Science. *Journal of Social Science Studies,* 4(1), 193-200.

Fared, M. A., & Darmawan, D. (2021). Use of Consumer Behaviour Data for Personalised Advertising in Digital Marketing. *Studi Ilmu Sosial Indonesia,* 1(2), 93-108.

Frimpong, B., & Chen, L. (2021). *The Effects of Data Breaches on Public Companies: A Mirage or Reality?* 674–683.

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. *Computer Fraud & Security*, *2020*(12), 6–12.

Gani, A., & Darmawan, D. (2022). Ethics and Accountability in Artificial Intelligence-Based

Managerial Decision Making. *Journal of Social Science Studies,* 2(1), 147-152.

Geistfeld, M. A. (2017). Protecting Confidential Information Entrusted to Others in Business Transactions: Data Breaches, Identity Theft, and Tort Liability. *Depaul Law Review*, *66*(2), 4.

Hardyansah, R., Karwati, K., & Saktiawan, P. (2024). Legal Analysis of Open Banking and Bank Customer Data Privacy Rights in Indonesia. *Journal of Social Science Studies*, 4(1), 93-104.

Hartana, P. C., Mardikaningsih, R., & Halizah, S. N. (2024). Legal Construction and Enforcement Challenges of Credit Card Data Hacking Crimes in E-Commerce Systems. *Journal of Social Science Studies,* 4(2), 503-516.

Hartiwiningsih, & Rustamaji, M. (2023). Reconstruction of State Economic Losses in Criminal Acts of Corruption in Indonesia. *RGSA: Revista de Gestão Social e Ambiental*, *17*(4), e03453–e03453.

Hidayat, D. R. D., Rifani, F. A., Rivaldo, A., Setiawan, W. F., & Siswajanthy, F. (2024). Kajian Yuridis terhadap Peran Saksi Ahli dalam Proses Peradilan Perdata. *CAUSA: Jurnal Hukum dan Kewarganegaraan*, 5(2), 31–40.

Irfansyah, M. F., Darmawan, D., & Hardyansah, R. (2024). Implementation of the Principle of Good Faith in Contract Performance. *Bulletin of Science, Technology and Society*, *3*(2), 51-56.

Issalillah, F., & Hardyansah, R. (2024). Relevance of Privacy within the Sphere of Human Rights: A Critical Analysis of Personal Data Protection. *Bulletin of Science, Technology and Society*, 3(1), 31–39.

Kamilah, A. (2024). Carding sebagai Cyber Crime dan Penegakan Hukumnya Melalui Tort dalam Perspektif Hukum Perdata Internasional. *Jurnal Hukum Mimbar Justitia (JHMJ)*, 10(2), 361-385.

Khairi, M., & Darmawan, D. (2022). Developing HR Capabilities in Data Analysis for More Effective Decision Making in Organizations. *Journal of Social Science Studies*, 2(1), 223-228.

Krippendorff, K. (2004). *Content Analysis: An Introduction to Its Methodology* (2nd ed.). Sage Publications, Thousand Oaks.

Kurniawan, M. A., Darmawan, D., & Negara, D. S. (2024). The principle of division of obligations and consumer protection in product distribution agreements: A study of business law and its practice in Indonesia. *Journal of Social Science Studies*, 4(1), 219–226.

Kurniawan, Y., & Darmawan, D. (2021). The adaptive learning effect on individual and collective learning. *Journal of Social Science Studies*, *1*(1), 93-98.

Mamesah, D. A., Gautama, E. C., & Mardikaningsih, R. (2024). Industrial Waste Reporting Obligations and Public Data Disclosure in Modern Corporate Law. *Journal of Social Science Studies*, 4(1), 155-164.

Mardikaningsih, R., & Darmawan, D. (2022). Situational Leadership Strategies to Improve Change Management and Team Performance. *Journal of Social Science Studies,* 2(1), 247–252.

Mardikaningsih, R., Darmawan, D., & Hariani, M. (2024). Inclusive Public Communication in the Digital Era: A Literature Study on Multicultural Approaches in Communication Policy. *Studi Ilmu Sosial Indonesia,* 4(2), 385-402.

Marzuki, P. M. (2005). Penelitian Hukum: Edisi Revisi (Jakarta: Kencana Prenada Media Group, 2005), 93. *Kencana Prenada Media*.

Maulani, A., Hardyansah, R., Darmawan, D., Mendonca, C. N., & de Jesus Isaac, A. (2023). Juridical analysis of the validity of electronic contracts made by artificial intelligence in Indonesian law. *Journal of Social Science Studies*, 3(1), 139–144.

Memah, A. R., Warong, R. N., & Lengkong, N. (2023). Kajian Yuridis Gugatan Class Action dalam Hukum Positif di Indonesia. *Lex Privatum*, 11(3), 1-9.

Moraru, I. (2024). Variables of quantifying reputational damages resulting from unfair competition actions. *Eastern European Journal of Regional Studies*, 120–136.

Mujisulistyo, Y. F., Darmawan, D., & Dirgantara, F. (2024). Reconstruction of the Legal Mechanism for Consumer Rights Recovery Regarding Personal Data Leaks in the Financial Technology and E-Commerce Sectors in Indonesia. *Journal of Social Science Studies*, 4(1), 75-84.

Ningsih, U. H., & Wahyudi, E. (2024). Repressive Protection for Journalists for Leakage Of Personal Data By Telecommunications Service Providers. *JARES (Journal of Academic Research and Sciences),* 9(2), 40-53.

Osean, R., Negara, D. S., & Putra, A. R. (2024). Digital Transformation in Manufacturing and Legal Aspects of Data Protection and Workers. *Journal of Social Science Studies*, 4(1), 21-32.

Perkasa, J., & Saly, J. N. (2022). *Legal Liability of Marketplace Companies Against Leaking of User Data Due to Third Party Breaking According to Law Number 8 of 1999 Concerning Consumer Protection (Case Example: Tokopedia User Data Leaking in 2020).*

Poyraz, O. I., Canan, M., McShane, M. K., Pinto, C. A., & Cotter, T. S. (2020). Cyber assets at risk: monetary impact of U.S. personally identifiable information mega data breaches. *Geneva Papers on Risk and Insurance-Issues and Practice*, *45*(4), 616–638.

Pratama, A. M., Syaiful, S., & Rahman, M. F. (2024). *Buku Ajar Keamanan Data dan Informasi*. Kaizen Media Publishing.

Prawoto, A. (2021). *Penilaian Bank, Asuransi Dan Aset Tidak Berwujud: Berdasarkan Standar Penilaian Indonesia & Praktik Penilaian Indonesia*. Penerbit Andi, Bandung.

Putra, A. R., & Arifin, S. (2021). Supply Chain Management Optimization in the Manufacturing Industry through Digital Transformation: The Role of Big Data, Artificial Intelligence, and the Internet of Things. *Journal of Social Science Studies*, 1(2), 161-166.

Rahadita, I. B. A., Ardhya, S. N., & Dantes, K. F. (2023). Perlindungan Konsumen Dalam Upaya Pengajuan Ganti Kerugian Atas Penipuan Jual Beli Ponsel Ilegal Pada Transaksi Elektronik Melalui E-Commerce. *Jurnal Ilmu Hukum Sui Generis*, 3(4), 149-159.

Rahman, R. S., Hardyansah, R., Darmawan, D., Negara, D. S., & Khayru, R. K. (2023). Legal perspective of investment risk mitigation on peer-to-peer lending platforms. *Journal of Social Science Studies*, 3(1), 177–184.

Rahmani, M. F., Gautama, E. C., & Issalillah, F. (2024). Legal Framework for Free Contraception in Community Clinics: Consent and Data Protection. *Journal of Social Science Studies*, 4(1), 465-482.

Raschke, R. L., Lee, M. T., Charron, K. F., & Tandy, P. R. (2020). Digital Liability Risk: A Note on Estimating Exposure, Costs, and Implications. *Journal of Business Accounting and Finance Perspective*, 2(1), 1.

Republik Indonesia. (1847). *Kitab Undang-Undang Hukum Perdata (KUHPerdata/Burgerlijk Wetboek)*. Staatsblad Tahun 1847 Nomor 23. Sekretariat Negara. Jakarta.

Republik Indonesia. (2000). *Undang-Undang Republik Indonesia Nomor 30 Tahun 2000 tentang Rahasia Dagang*. Lembaran Negara Republik Indonesia, Tambahan Lembaran Negara Republik Indonesia. Sekretariat Negara Republik Indonesia. Jakarta.

Republik Indonesia. (2008). *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia, Tambahan Lembaran Negara Republik Indonesia. Sekretariat Negara Republik Indonesia. Jakarta.

Republik Indonesia. (2019). *Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia. Sekretariat Negara Republik Indonesia. Jakarta.

Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia, Tambahan Lembaran Negara Republik Indonesia. Sekretariat Negara Republik Indonesia. Jakarta.

Rianto, R., Darmawan, D., & Negara, D. S. (2024). The application of restorative justice in resolving speech cases in the digital space: A normative analysis of the Electronic Information and Transactions Law and the Criminal Code. *Journal of Social Science Studies*, 3(1), 295–306.

Rojak, J. A., Fajar, A. S. M., & Fauzi, A.(2024). Digital Technology and Large Data in Contemporary Social Structures. *Journal of Social Science Studies*, 4(1), 437-446.

Rolle, B. (2023). Fair Data Protection Damages: Tension between Troublemakers, Legal Techs and Real Harm. *European Data Protection Law Review*, *9*(2), 136–147.

Romanosky, S., Hoffman, D., & Acquisti, A. (2013). *Empirical Analysis of Data Breach Litigation*. *11*, 74–104.

Sinambela, E. A., Darmawan, D., & Halizah, S. N. (2022). Digital Inequality and Unequal Opportunity for Young Entrepreneurs in Online Economies. *Studi Ilmu Sosial Indonesia*, 2(1), 169-190.

Soekanto, S. & Mamudji, S. (2009). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Rajawali Pers, Jakarta.

Sugiarto, A. J., Lie, G., & Putra, M. R. S. (2024). Perlindungan Kepada Nasabah Bank Terhadap Kebocoran Data (Studi Kasus Kebocoran Data pada Bank Indonesia). *Deleted Journal*, *2*(1), 107–114.

Sutanto, H., Darmawan, D., & Saputra, R. (2023). Legal violation patterns in digital technology on liability and proof. *Studi Ilmu Sosial Indonesia*, 3(2), 277–308.

Umar, H., Purba, R. B., Safaria, S., Mudiar, W., Harsono, H., & Karyaningsih, K. (2021). *The New Strategy in Combating Corruption (Detecting Corruption: HU-Model)*. Merdeka Kreasi Group, Medan.

Wright, S., & Pilavci, E. (2021). Data breach liabilities of company directors. Journal of Data Protection & Privacy, 4(3), 283-293.

***Rasid, A., R. Hardyansah, R. K. Khayru: Civil Liability for Data Breach and Destruction of Digital Data as Corporate Assets within the Framework of Unlawful Acts, *Journal of Social Science Studies* 5(1), 135 – 150.**