ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

Civil Liability Of E-Commerce Platforms For Personal Data Breaches: Reconstructing The Chain From Statutory Duty To Consumer Compensation Under Indonesian Law

Desy Artha Pratiwi,
Faculty of Law, Universitas Muhammadiyah Metro, Indonesia,
Amail: not_desyartha@yahoo.co.id

Abstract

The growth of electronic commerce has placed personal data at the centre of consumer transactions and, with it, has exposed consumers to harm when platforms fail to protect that data. This article examines the civil-law consequences of personal data breaches committed by e-commerce platforms under Indonesian law. It asks how platform duties, breach, attribution, causation, damage and compensation should be connected within a single coherent private-law analysis. The study applies normative legal research using statutory, conceptual and comparative approaches, examining Law Number 27 of 2022 on Personal Data Protection, the Indonesian Civil Code, Law Number 8 of 1999 on Consumer Protection and the electronic-system framework, with the European General Data Protection Regulation and the case law of the Court of Justice of the European Union as comparators. The article finds that Indonesian law already contains every ingredient required for a civil claim but distributes them across regimes that are not doctrinally connected, and that the compensation right in Article 12(1) of the PDP Law remains procedurally incomplete because the implementing regulation contemplated by Article 12(2) has not yet been enacted. It develops a Civil Liability Chain comprising legal duty, breach, attribution, causation, damage, civil liability and remedy, and tests that chain against the Tokopedia data-breach incident as a doctrinal illustration rather than as a retrospective application of the 2022 statute. The article argues that effective consumer redress requires an explicit causal and remedial bridge between statutory data-protection duties and Indonesian civil liability.

Keywords: personal data breach; e-commerce platform; civil liability; causation; consumer compensation.

A. INTRODUCTION

The rapid expansion of electronic commerce has transformed the legal relationship between businesses and consumers. In an e-commerce transaction, personal data is no longer merely supplementary information. It forms part of registration, payment, delivery, customer communication, fraud prevention and the personalisation of commercial services. That dependence creates a corresponding legal risk: the more deeply a platform relies on personal data, the graver the consequences when that data is accessed, disclosed or used without authorisation. Indonesia responded to this development through Law Number 27 of 2022 on Personal Data Protection (the PDP Law), which establishes a specific framework for the processing of personal data and imposes duties on personal data controllers and processors.[1] The statute therefore provides a stronger normative foundation for assessing the conduct of digital businesses when personal information entrusted to them is compromised.

Yet a data breach does not answer all of the legal questions that arise after an incident. The difficult question for private law is not simply whether an e-commerce platform owed a duty to protect

[1]Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, State Gazette of the Republic of Indonesia Number 196 of 2022, Supplement to the State Gazette Number 6820.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

personal data, but when a failure to discharge that duty becomes a civil wrong capable of supporting a consumer claim. Answering it requires a distinction between the occurrence of a security incident and the existence of compensable harm. A consumer may suffer a direct financial loss, a consequential loss caused by the later misuse of leaked data, or an injury that is primarily privacy-related. The PDP Law recognises the right of a data subject to claim and receive compensation for violations in the processing of personal data, but that right must still operate within a coherent structure of breach, attribution, causation, damage and remedy.[2]

The Indonesian legal framework is plural in a practical sense. The PDP Law establishes specialised obligations for personal-data processing; Article 1365 of the Civil Code supplies the general basis for liability arising from an unlawful act causing loss; the Consumer Protection Law provides consumer-oriented rights and remedies; and Government Regulation Number 71 of 2019 regulates electronic systems and transactions.[3] These instruments are complementary, but they do not automatically produce a single answer when a large-scale data breach occurs. The legal task is to explain how a specialised statutory duty becomes relevant to private-law liability without collapsing regulatory compliance and civil responsibility into the same concept.

Recent scholarship confirms that the broader field of platform responsibility is already well populated. Afifah examines the responsibility of e-commerce platforms under the 2022 PDP Law, including security, transparency, consent and sanctions.[4] Putra, Fibrianti and Prasetya compare the liability of e-commerce service providers in Indonesia and Europe, placing platform liability directly within the contemporary data-protection debate.[5] Maulana and Sodikin address the legal responsibility of e-commerce businesses for data leaks alongside the constitutional contestation of cross-border data transfer.[6] Mansawan, Sassan and Bernard emphasise institutional oversight, business compliance and consumer legal literacy.[7] The implication for the present article is important: it is no longer convincing to claim that the legal responsibility of e-commerce platforms is itself a research gap.

The more focused gap lies in the civil-law consequences of that responsibility. Existing studies frequently present administrative, civil and criminal consequences together, or discuss consumer protection at a general level. Such approaches usefully describe the regulatory landscape, but they leave little room for a detailed examination of the sequence through which a data breach becomes a private-law claim. The civil-law study by Purnomo and Rijadi on personal-data protection in Indonesian e-commerce, for example, identifies continuing weaknesses in enforcement, supervision and accessible remedies, yet does not construct the intermediate doctrinal steps.[8] What remains insufficiently developed is a doctrinal explanation connecting the platform's legal duty to the consumer's eventual claim through the questions of breach, attribution, causation and legally recognisable harm.

---

[2]Law Number 27 of 2022, art. 12(1).

[3]Indonesian Civil Code (Kitab Undang-Undang Hukum Perdata), art. 1365; Law Number 8 of 1999 concerning Consumer Protection; Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

[4]Nurul Afifah, "Tanggung Jawab Hukum Platform E-Commerce terhadap Keamanan Data Pribadi Pengguna: Analisis Berdasarkan UU PDP 2022" [The Legal Responsibility of E-Commerce Platforms for the Security of Users' Personal Data: An Analysis Based on the 2022 PDP Law], Jurnal Legalitas 2, no. 1 (2024): 29–38, https://doi.org/10.58819/jle.v2i1.165.

[5]Tegar Islami Putra, Nurul Fibrianti, and Rizky Andeza Prasetya, "Liability of E-Commerce Service Providers for Processing Consumer Personal Data (Comparative Study of Indonesia & Europe)," Journal of Private and Commercial Law 9, no. 1 (2025): 72–109, https://doi.org/10.15294/jpcl.v9i1.9370.

[6]Muhammad Hasyim Maulana and Sodikin, "Legal Protection for E-Commerce Consumers Against Personal Data Leaks," International Journal of Research and Innovation in Social Science 9, no. 11 (2025): 4234–4243, https://doi.org/10.47772/IJRISS.2025.91100329.

[7]Isak Semuel Kejne Mansawan, Jonhi Sassan, and Jefri Bernard, "Legal Protection of E-Commerce Consumers' Personal Data Under Indonesian Law," Jurnal Ilmu Hukum Kyadiren 7, no. 1 (2025): 538–554, https://doi.org/10.46924/jihk.v7i1.320.

[8]Mahendra Bisma Wisdha Wardana Purnomo and Prasetijo Rijadi, "The Civil Law Perspective on Legal Consequences of Safeguarding Consumer Personal Data in Indonesian E-Commerce Activities," YURIS: Journal of Court and Justice 3, no. 4 (2024), https://doi.org/10.56943/jcj.v3i4.803.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

Comparative experience shows that these intermediate questions are decisive rather than technical. Article 82 of the European General Data Protection Regulation grants a right to compensation for material and non-material damage, subject to an exemption where the controller proves it is in no way responsible for the event giving rise to the damage.[9] Interpreting that provision, the Court of Justice of the European Union has held that an infringement of the regulation does not by itself confer a right to compensation, because damage and a causal link must be established in addition to the infringement, while no threshold of seriousness may be imposed on non-material damage.[10] In a subsequent judgment the Court held that unauthorised disclosure by a third party does not by itself demonstrate that the controller's technical and organisational measures were inappropriate, and that it falls to the controller to prove the appropriateness of those measures.[11] These holdings correspond closely to the analytical difficulties that Indonesian courts will face, and they provide a tested comparative benchmark that Indonesian scholarship has largely left unused.

Causation is particularly difficult because a data breach often sits at the beginning of a longer chain of events. Personal information may be exposed by an unauthorised intrusion, transferred or sold to a third party, and later used for phishing, identity fraud or unauthorised transactions. In other cases, information may be disclosed without any immediate financial loss while still affecting privacy, security, reputation or the individual's control over information about themselves. Article 1365 of the Civil Code does not treat the occurrence of an incident as sufficient in itself; the unlawful act must cause loss through the legally relevant elements of civil responsibility.[12] The challenge is therefore to distinguish a factual connection from a legally sufficient causal connection.

The same difficulty appears in the assessment of damage. Traditional consumer disputes usually involve readily measurable losses, but personal-data cases may involve direct economic loss, the costs of mitigation and recovery, consequential loss, and non-material or privacy-related harm. The existence of a statutory compensation right is important, yet compensation cannot be detached from proof of the legally cognisable injury for which it is claimed. The private-law analysis must therefore move beyond the statement that consumers have a right to compensation and ask what must be established before that right can be effectively exercised.

The Tokopedia data-breach incident is useful for testing this problem because it demonstrates the scale and complexity of a modern e-commerce breach, and because subsequent literature has revisited it through the newer legal framework.[13] The incident occurred in 2020, before the enactment of the PDP Law. For that reason this article does not treat Tokopedia as a direct enforcement case under that statute. The case is used instead as a doctrinal illustration: if comparable facts were assessed under the current legal framework, how would the elements of civil liability be arranged? This distinction avoids applying the 2022 statute retrospectively while retaining the case's value as a test of legal reasoning.

Against this state of the art, the research gap is best understood as an **integration gap within civil liability** rather than as a lack of research on data protection or e-commerce platforms. The literature has established the existence of platform duties, regulatory obligations and consumer rights, but it has not integrated them into one private-law sequence connecting legal duty, breach, attribution,

[9]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 82(1)–(3).

[10]Case C-300/21, UI v Österreichische Post AG, ECLI:EU:C:2023:370, judgment of 4 May 2023.

[11]Case C-340/21, VB v Natsionalna agentsia za prihodite, ECLI:EU:C:2023:986, judgment of 14 December 2023.

[12]Indonesian Civil Code, art. 1365.

[13]Ragil Putri Anindya and Achmad Edi Subiyanto, "Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi" [The Responsibility of the Tokopedia Platform in the Data Leakage Case under the Personal Data Protection Law], RIGGS: Journal of Artificial Intelligence and Digital Business 4, no. 3 (2025): 1105–1112, https://doi.org/10.31004/riggs.v4i3.2105.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

causation, consumer harm, liability and compensation. The contribution of this article is the **Civil Liability Chain**, which reconstructs that sequence and uses it to clarify when a personal-data breach may become a compensable civil injury. Two elements of the chain are advanced as novel: an **intervening-event test** for determining when the later misuse of leaked data remains legally attributable to the original security failure, and a **separation of common breach issues from individual damage issues** in collective proceedings.

This article addresses three questions. First, how should the civil obligations of e-commerce platforms to protect consumers' personal data be constructed under Indonesian law? Second, how should the causal relationship between a personal-data breach and consumer loss be established as a basis of civil liability? Third, how should consumer compensation for personal-data breaches be reconstructed within the Indonesian civil-law framework?

B. RESEARCH METHOD

This study is normative legal research, which examines law as a system of norms contained in legislation, legal principles and doctrine. Three approaches are combined.

The **statutory approach** examines the PDP Law, the Indonesian Civil Code, the Consumer Protection Law, Government Regulation Number 71 of 2019 and the Supreme Court Regulation on class action procedure, together with Constitutional Court Decision Number 151/PUU-XXII/2024, which has altered the reading of Article 53(1) of the PDP Law. The **conceptual approach** examines the doctrines of unlawful act, fault, attribution, causation and damage, including the doctrines of conditio sine qua non , adequate causation (adequate veroorzaking) and the relativity of the violated norm (Schutznormtheorie), which govern the passage from a statutory duty to a private-law claim. The **comparative approach** uses Article 82 of the General Data Protection Regulation and the interpretative case law of the Court of Justice of the European Union, not as a source of binding law in Indonesia, but as a tested doctrinal benchmark for questions that Indonesian courts have not yet resolved.

Legal materials consist of primary materials in the form of the legislation and decisions listed above, and secondary materials in the form of peer-reviewed journal articles and credible reporting concerning the Tokopedia incident. The materials are analysed prescriptively and qualitatively. The Tokopedia incident is used as a **doctrinal illustration** rather than as a case study of an adjudicated dispute; the article makes no claim about the actual legal liability of any party in that incident, and the framework is applied on the hypothesis that comparable facts arose under the present legal regime.

C. RESULTS AND DISCUSSION

1. The Position of the E-Commerce Platform within Civil Liability

a. The E-Commerce Platform as a Personal Data Controller

An e-commerce platform is not merely a digital marketplace. In the ordinary course of business, the platform determines what personal information is needed, why it is collected, how it is processed, how long it is retained and which parties may access it. That practical control is legally significant because the PDP Law defines a personal data controller through the role it plays in determining the purposes of, and exercising control over, the processing of personal data.[14] The legal position should therefore be assessed from the platform's actual function rather than from the contractual label attached to the service.

[14]Law Number 27 of 2022, art. 1(4).

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

Where the platform determines the purposes and controls the processing, its position as controller carries a corresponding set of duties: lawful processing, respect for the rights of data subjects, protection against unlawful processing, supervision of the parties involved in processing, and accountability for the processing carried out under its control.[15] The controller's role is thus the first link in the Civil Liability Chain, because it identifies the party against whom the statutory duty is primarily assessed.

The controller concept also matters because consumers ordinarily have no access to the platform's internal security architecture. A consumer cannot readily determine which servers store their information, which processors receive access, what security controls are in place, or how incidents are investigated. The legal framework consequently places the primary governance burden on the actor that possesses the relevant organisational and technical control.

At the same time, controller status should not be equated with civil liability. It establishes the source of the legal duty, not the outcome of a compensation claim. The analysis must still establish whether the duty was breached and whether that breach caused legally recognisable harm. This distinction keeps the private-law inquiry separate from the broader question of regulatory compliance.

b. Security and Supervisory Obligations

Among the most important duties is the obligation to prevent unauthorised access. The PDP Law requires the controller to protect personal data from unlawful processing, to supervise every party involved in processing under its control, and to prevent unauthorised access by employing a security system and by processing personal data through electronic systems in a reliable, secure and responsible manner.[16] The statute further establishes the controller's responsibility and accountability for the processing it carries out.[17] Together these provisions show that data security is not merely a technical concern; it is a legal obligation capable of supplying the benchmark for a subsequent civil-law analysis.

The security obligation should nevertheless not be read as a guarantee that no cyberattack can ever succeed. A digital platform may face sophisticated attacks even after adopting substantial safeguards. Civil liability therefore requires a distinction between the occurrence of an external attack and the existence of a legally relevant failure by the platform. The pertinent question is whether the platform implemented and maintained the security measures reasonably required by the applicable legal framework and by the risks associated with its processing activities. The comparative position is instructive: the Court of Justice of the European Union has held that the fact of unauthorised disclosure by a third party is not sufficient to presume that the measures adopted by the controller were inappropriate.[18]

Post-breach conduct is also legally relevant. The PDP Law requires notification following a failure of personal data protection and identifies the information that must be communicated to the data subject and to the competent institution.[19] This creates a temporal dimension to platform responsibility: the duty exists before the breach through preventive security measures and continues after the breach through response, notification and recovery obligations.

The governance dimension of these duties has recently been strengthened. In Decision Number 151/PUU-XXII/2024 the Constitutional Court granted a petition concerning the appointment of a personal data protection officer and held that the conjunction "and" in Article 53(1)(b) of the PDP Law is contrary to the 1945 Constitution unless read as "and/or," with the consequence that the duty to

[15]Law Number 27 of 2022, ch. V (Rights of Data Subjects and Obligations of Personal Data Controllers and Processors).
[16]Law Number 27 of 2022, arts. 37–39.
[17]Law Number 27 of 2022, art. 47.
[18]Case C-340/21, VB v Natsionalna agentsia za prihodite.
[19]Law Number 27 of 2022, art. 46.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

appoint such an officer is triggered by the fulfilment of any one of the listed criteria rather than all of them cumulatively.[20] For a large e-commerce platform, which conducts regular and systematic monitoring of personal data on a large scale, the appointment obligation is therefore engaged.[21] That obligation is relevant to the civil analysis because the presence or absence of an accountable governance function is a concrete indicator when a court assesses whether the required standard of care was met.

Government Regulation Number 71 of 2019 provides the broader electronic-system framework within which e-commerce platforms operate.[22] The relationship between that regulation and the PDP Law creates a layered environment in which general obligations of system reliability and security are connected with specialised personal-data duties. The Consumer Protection Law adds a third layer by imposing on business actors a duty to compensate consumers for loss resulting from goods or services they trade.[23]

c. From Statutory Obligation to Civil Obligation

The existence of a statutory obligation does not automatically create civil liability. It establishes the first analytical stage: legal duty. Article 1365 of the Civil Code then provides the general private-law mechanism through which an unlawful act causing loss may generate an obligation to compensate.[24] The specialised obligations under the PDP Law supply a concrete standard against which the platform's conduct may be assessed, while Article 1365 supplies the general civil-liability structure.

Two further provisions complete the structure and have been underused in the Indonesian literature. Article 1367 of the Civil Code attaches responsibility not only to a person's own conduct but also to the conduct of those for whom that person is responsible and of things under their supervision; this is the natural domestic anchor for the attribution of processor failures to a controlling platform.[25] Article 1366 confirms that liability may arise from negligence and imprudence, not only from positive acts, which matters where the alleged wrong consists in an omission such as the failure to patch a known vulnerability.[26]

This relationship is important because it prevents the conclusion that a regulatory breach necessarily produces a civil judgment. The court must still consider attribution, causation and damage. A platform may attract regulatory criticism yet not be liable for every loss claimed by every user. Conversely, a statutory duty may become an important foundation for a civil claim where its breach can be connected to a specific consumer injury. The first stage of the framework can therefore be stated as: **controller status → legal duty → security and governance obligation → breach assessment.**

2. Constructing Civil Liability for Personal Data Breaches

a. Breach of Duty as the Basis of Civil Liability

The civil consequences of a personal data breach should begin with a clear identification of the duty allegedly violated. A data breach is a factual event; civil liability is a legal conclusion. The two are not interchangeable. The relevant question is whether the platform failed to discharge a duty imposed by law, and whether that failure is capable of supporting a private-law claim.

[20]Constitutional Court of the Republic of Indonesia, Decision Number 151/PUU-XXII/2024, 30 July 2025, declaring the word "and" in art. 53(1)(b) of Law Number 27 of 2022 contrary to the 1945 Constitution unless read as "and/or."

[21]Constitutional Court Decision Number 151/PUU-XXII/2024.

[22]Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

[23]Law Number 8 of 1999, art. 19.

[24]Indonesian Civil Code, art. 1365.

[25]Indonesian Civil Code, art. 1367.

[26]Indonesian Civil Code, art. 1366.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

Article 1365 provides the general foundation for unlawful-act liability where an unlawful act causes loss through fault.[27] In data-breach disputes the unlawful conduct may consist in a failure to implement required security measures, a failure to supervise relevant processors, a failure to respond to a known vulnerability, or another failure inconsistent with the controller's statutory duties. The PDP Law therefore supplies specific content to a general duty of care that would otherwise remain abstract.

The distinction matters because the literature sometimes moves directly from breach to liability. That move is too quick for civil law. A breach may establish a prima facie violation of duty, but attribution, causation and damage remain independent analytical questions. This is precisely the point on which the Court of Justice of the European Union insisted when it held that an infringement of the data-protection regulation does not in itself confer a right to compensation.[28] The Civil Liability Chain deliberately makes those stages visible rather than assuming the conclusion at the outset.

b. Attribution of the Violation to the Platform

E-commerce data processing frequently involves multiple actors: cloud providers, payment processors, logistics companies, analytics services and other processors. The platform's use of third parties does not by itself extinguish its legal obligations, because the PDP Law requires the controller to supervise the parties involved in processing under its control, and because Article 1367 of the Civil Code already recognises responsibility for persons and things within one's sphere of supervision.[29] The attribution inquiry therefore focuses on the platform's sphere of legal and organisational control.

Attribution should not, however, be reduced to a blanket form of vicarious liability. A court should identify the specific duty, the relevant failure, and the extent to which the risk fell within the platform's control. A third-party act may be relevant to the causation analysis without automatically relieving the platform of responsibility. Platform governance, processor oversight and internal security controls therefore remain important factual matters in a civil claim.

Some recent literature characterises platform responsibility for data breaches as strict liability; Afifah, for example, uses that terminology in discussing e-commerce platforms.[30] The term requires caution. Strict liability alters the role of fault in the liability analysis, whereas a negligence-based claim turns on a failure to meet a required standard of care. The occurrence of a cyberattack should not be treated as conclusive proof of strict liability without a separate doctrinal basis in the applicable law. Indonesian law does contain risk-based liability in defined settings, but the PDP Law does not expressly adopt such a regime for security failures, and the general regime of Articles 1365 to 1367 of the Civil Code remains fault-based.

c. Causation between the Data Breach and Consumer Loss

Causation is the most difficult link in many data-breach disputes, because leaked information may subsequently be used by different actors, making it difficult to determine which damage was caused by the original breach.[31] That difficulty is not incidental; it is central to the civil-law inquiry.

Three situations illustrate the problem. First, a security failure may directly facilitate an unauthorised transaction, producing a relatively immediate financial loss. Second, leaked information may later be used for phishing or identity fraud, so that the consumer's loss emerges through one or more intervening events. Third, information may be exposed without immediate financial loss, while

[27]Indonesian Civil Code, art. 1365.
[28]Case C-300/21, UI v Österreichische Post AG.
[29]Law Number 27 of 2022, art. 37; Indonesian Civil Code, art. 1367.
[30]Afifah, "Tanggung Jawab Hukum Platform E-Commerce terhadap Keamanan Data Pribadi Pengguna."
[31]Purnomo and Rijadi, "The Civil Law Perspective on Legal Consequences of Safeguarding Consumer Personal Data."

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

the consumer nevertheless experiences privacy-related or security-related harm. These situations should not be treated as identical.

Indonesian doctrine offers the tools required to differentiate them. The conditio sine qua non test identifies the factual antecedents of the loss but, applied alone, extends liability indefinitely along the chain of consequences. The doctrine of adequate causation (adequate veroorzaking) narrows the inquiry to consequences that could reasonably be expected to follow from the conduct in the ordinary course of events. The doctrine of the relativity of the violated norm (Schutznormtheorie) adds a further and, in this context, decisive filter: the statutory duty relied upon must have been intended to protect the very interest for which the claimant seeks redress. Because the security obligations of the PDP Law are directed precisely at protecting data subjects against unauthorised access to their information, a consumer who suffers loss through the misuse of information exposed by a security failure asserts an interest that the norm was designed to protect. That correspondence is what converts a regulatory duty into a foundation for a private claim.

The causal test therefore asks whether the platform's breach caused the injury, directly or through a legally sufficient sequence of events. An intervening act does not necessarily break the chain of causation. In some circumstances the subsequent misuse of leaked information is precisely the consequence that makes the security duty meaningful, and is therefore adequate in the doctrinal sense. In other cases the chain may be too remote. The task is to determine the legal significance of the intervening event rather than assume either extreme. The framework may be expressed as: **breach → exposure → intervening event → consumer harm → legally sufficient causal connection.**

d. Fault and the Standard of Care

Article 1365 connects unlawful-act liability with fault, and Article 1366 confirms that negligence suffices.[32] In the digital environment, the assessment of fault should be related to the security and governance obligations imposed by the PDP Law. The relevant question is not whether the platform can guarantee perfect cybersecurity, but whether it took the measures that the legal framework reasonably required in light of the nature and risks of its processing.

This permits a court to examine concrete indicators: security governance, access controls, monitoring, processor supervision, vulnerability management, incident-response procedures, the appointment and independence of a data protection officer, and internal accountability. Such indicators are more useful than an abstract assumption that any successful cyberattack proves negligence.

The distinction is also a matter of fairness. A platform that implements reasonable safeguards but is defeated by an exceptionally sophisticated attack should not automatically be treated in the same way as a platform that ignores known vulnerabilities or fails to maintain basic security controls. The standard should therefore be contextual, evidence-based and anchored in duties already established by legislation.

e. The Relationship between the PDP Law and Article 1365 of the Civil Code

The PDP Law and Article 1365 should be understood as complementary rather than competing legal bases. The PDP Law identifies specialised duties arising from personal-data processing. Article 1365 provides the general mechanism through which unlawful conduct causing loss may generate civil responsibility. The two operate at different levels of the analysis.

The first level is statutory duty: what was the controller required to do? The second is civil breach: did its conduct violate that duty in a legally relevant manner? The third is causation and damage: did the breach cause a compensable injury? Only once those questions are answered can

[32]Indonesian Civil Code, art. 1366.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

compensation be considered. This sequence avoids the recurring problem of treating every statutory violation as though it automatically determined the availability and quantum of civil compensation. The result may be summarised as: **specific statutory duty → breach → attribution → causation → damage → civil liability.** Compensation is the remedial consequence of the completed chain, not its starting point.

3. Compensation and the Recovery of Consumer Loss

a. The Consumer's Right to Compensation and Its Procedural Gap

Civil liability has little practical value if the injured consumer cannot obtain an effective remedy. The PDP Law expressly recognises the right of a data subject to sue for and receive compensation for violations involving the processing of personal data.[33] That provision strengthens the remedial dimension of personal-data protection and gives consumers a statutory basis for seeking redress.

The right is, however, procedurally incomplete. Article 12(2) of the PDP Law delegates the further regulation of violations in the processing of personal data and the procedure for imposing compensation to a government regulation.[34] At the time of writing that implementing regulation has not been enacted, and the supervisory institution contemplated by the statute has not been established, with supervisory functions exercised in the interim by the responsible ministry. The practical consequence is significant for the argument of this article: the statutory compensation right currently depends for its operation on the general civil-law framework rather than on a dedicated data-protection remedy. This is the clearest possible evidence of the integration gap identified above, and it makes the doctrinal bridge between the PDP Law and Articles 1365 to 1367 of the Civil Code a matter of practical necessity rather than academic preference.

The right to compensation should in any event remain connected to the civil-liability chain. A breach does not automatically produce identical compensation for every affected person. The claimant must identify the harm and establish its legal connection to the violation. This is especially important in large-scale incidents, where many thousands of people may be affected by the same breach yet experience very different consequences. The remedial principle can therefore be formulated as **violation plus legally attributable harm → right to compensation**, rather than **data breach → automatic compensation.**

b. Classification of Consumer Losses

Personal data breaches can generate several forms of loss. Material loss includes direct financial loss, the costs of account recovery, and reasonable expenditure incurred to mitigate the consequences of the breach. These forms of damage are usually evidenced through transaction records, receipts and similar documents.

Non-material harm is more difficult to assess. The exposure of personal information may affect privacy, dignity, reputation, personal security or an individual's sense of control over information about themselves. Whether such harm is legally compensable must be determined through the applicable legal basis and the evidence; it should neither be dismissed merely because it lacks an immediate price nor treated as automatically compensable simply because data was exposed. The comparative position supports a middle course: the Court of Justice of the European Union has declined to impose any threshold of seriousness on non-material damage, while insisting that the damage itself be demonstrated.[35]

[33]Law Number 27 of 2022, art. 12(1).
[34]Law Number 27 of 2022, art. 12(2).
[35]Case C-300/21, UI v Österreichische Post AG.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

A third category is consequential loss, where the harm occurs after the original breach through the subsequent misuse of the information. The legal challenge is to determine whether the intervening conduct remains sufficiently connected to the platform's breach, which returns the analysis to the doctrine of adequate causation discussed above.

c. Causation as a Limit on Compensation

The availability of compensation must be limited by the causal relationship established in the liability analysis. The occurrence of a breach may be necessary to the claim, but necessity is not sufficiency. The claimant must also demonstrate that the alleged loss is sufficiently connected to the breach and that the connection is legally attributable.

This approach is especially important where a third party intervenes. If leaked information is later used for phishing, a court should examine whether the intervening act was too remote or whether it represents a foreseeable and legally adequate consequence of the original security failure. The answer cannot be predetermined for every case. The compensation inquiry therefore follows: **breach → intervening event → injury → causal assessment → compensable damage.** The model acknowledges the realities of digital misuse without turning the platform into a guarantor of every subsequent event.

d. Proof of Loss and Informational Asymmetry

Data-breach disputes are marked by a structural evidentiary imbalance. Consumers ordinarily cannot inspect a platform's security architecture, incident logs, access histories, processor agreements or internal risk assessments; the platform and its service providers possess those records. Recent Indonesian research has identified weak remedies and implementation difficulties as continuing problems in personal-data protection, including from a civil-law perspective.[36]

Indonesian law is not without a response. Article 28 of the Consumer Protection Law already places the burden of proving the absence of fault on the business actor in consumer compensation disputes.[37] Read together with the controller's statutory accountability obligation, this provides a domestic basis for the allocation that comparative practice has reached by a different route: the Court of Justice of the European Union has held that it is for the controller to prove the appropriateness of its technical and organisational measures.[38] The convergence is significant, because it shows that a balanced evidentiary approach does not require the importation of foreign law; it requires the coordinated application of provisions Indonesian law already contains.

This asymmetry does not justify automatic liability. It supports a division of evidentiary responsibility in which the platform demonstrates compliance with matters falling principally within its control — what security measures were in place, how the incident occurred, which data were affected and what response measures were taken — while the consumer remains responsible for identifying and substantiating the harm claimed. That allocation is more realistic than requiring consumers to reconstruct a platform's internal technical environment on their own.

e. Forms of Redress for Consumers

Compensation should not be understood exclusively in monetary terms. Monetary compensation remains important where material or non-material harm is established, but data-breach remedies may also require restorative measures. Depending on the circumstances these may include account recovery, correction of inaccurate information, erasure where legally justified, heightened security measures, or other steps aimed at restoring the consumer's control over personal information.

[36]Purnomo and Rijadi, "The Civil Law Perspective on Legal Consequences of Safeguarding Consumer Personal Data."
[37]Law Number 8 of 1999, art. 28.
[38]Case C-340/21, VB v Natsionalna agentsia za prihodite.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

A broader remedial approach is especially relevant where the harmful consequences continue after the breach. A payment made after the fact may not address a situation in which compromised data continues to circulate or remains vulnerable to misuse. Effective redress should therefore be capable of addressing both past harm and, where legally appropriate, continuing risk. This does not mean that every consumer should receive an identical remedy; the remedy should correspond to the nature and extent of the legally recognisable harm established in the individual case.

f. Individual Claims and Collective Redress

Large-scale breaches raise an access-to-justice problem, because the number of affected consumers can make individual litigation expensive and inefficient. Indonesian law already provides the instruments: the Consumer Protection Law permits claims by a group of consumers, by a consumer protection non-governmental organisation and by the government, and the Supreme Court Regulation on class action procedure supplies the procedural framework.[39] Collective mechanisms can therefore play an important role where many consumers share common factual and legal questions.

A collective process should not, however, assume that every consumer suffered identical damage. The existence of the breach, the platform's duty and certain aspects of attribution may be common questions, whereas causation, the type of harm and the amount of compensation may differ among individuals. A sound collective-remedy model should therefore separate **common breach issues** from **individual damage issues**, certifying the former for collective determination while reserving the latter for individualised assessment. Such differentiation allows collective litigation to improve efficiency without sacrificing the principle that compensation should correspond to the harm actually attributable to the responsible actor.

g. Reconstruction of the Compensation Mechanism within the Civil Liability Chain

The remedial stage completes the chain: **legal duty → breach → attribution → causation → damage → civil liability → remedy.** The final stage can be organised through three questions: what harm did the consumer experience, is that harm causally connected to the breach, and what remedy is appropriate to restore the consumer's legal and practical position?

This reconstruction avoids two opposite errors. The first is to assume that every data breach produces automatic and identical compensation. The second is to recognise only direct financial loss and thereby overlook legally significant privacy or consequential harms. The civil-law model should accommodate different forms of injury while insisting that compensation remain grounded in proof and causation. The approach makes the remedial function of the PDP Law concrete: the right to claim compensation is not an isolated statutory promise but is integrated with the civil-law requirements that determine when a platform's breach becomes a legally attributable and compensable injury.

4. Doctrinal Test of the Framework through the Tokopedia Data Breach

a. The Case as a Doctrinal Illustration

The Tokopedia data-breach incident provides a useful factual illustration for testing the Civil Liability Chain. Contemporaneous reporting described unauthorised access involving a very large volume of user information offered for sale online, and the incident has become a recurring reference

[39]Law Number 8 of 1999, arts. 45–46; Supreme Court Regulation (PERMA) Number 1 of 2002 concerning Class Action Procedure.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

point in Indonesian discussions of platform responsibility.[40] Subsequent legal scholarship has revisited it through the framework of the 2022 statute.[41]

The temporal point must remain explicit. Because the incident occurred before the PDP Law entered into force, this article does not treat Tokopedia as a direct enforcement case under that statute, and makes no assertion about the actual liability of any party. The case is used to ask a narrower question: **if comparable facts were assessed under the current legal framework, how would the elements of civil liability be organised?** This avoids retrospective application while allowing the case to test the explanatory value of the proposed framework.

b. Legal Duty

The first stage asks whether the platform would owe a legally enforceable duty to protect the data it controls. Under the present framework a platform that determines the purposes of, and controls, the processing of personal data qualifies as a controller and becomes subject to statutory duties concerning security, supervision and accountability.[42] Its commercial role is thus connected with a data-governance role that generates specific legal obligations. This stage establishes the normative baseline; it does not yet establish liability or compensation.

c. Breach and Attribution

The next stage assesses whether the security failure reflects a breach of duty and whether that failure can be attributed to the platform. A successful intrusion is not, by itself, proof of negligence. The analysis must examine security controls, access management, vulnerability handling, monitoring, processor oversight and incident governance, including whether an accountable data protection function was in place.

Attribution becomes especially important where multiple service providers are involved. The platform cannot simply point to a third-party service to escape every duty, because the PDP Law requires controllers to supervise the parties involved in processing under their control and because Article 1367 of the Civil Code recognises responsibility within one's sphere of supervision.[43] Conversely, third-party involvement should not automatically render the platform liable for every act committed beyond its reasonable sphere of control. The issue is whether the relevant failure remained within the platform's legally attributable sphere.

d. Causation and Consumer Harm

The illustration becomes most instructive at the causation stage. A breach may expose information while the eventual consequence emerges later and through another actor. The platform's failure may be an antecedent cause without being the sole factual event in the chain. A court must therefore determine whether the subsequent misuse is too remote or remains an adequate consequence of the original failure, and whether the interest asserted falls within the protective purpose of the security norm.

The same reasoning applies to damage. Consumers may differ in the consequences they experience. Some may suffer direct financial losses; others may incur recovery costs; others may experience privacy or security harm without immediately measurable financial loss. The framework

[40]Fanny Potkin, "Indonesia's Tokopedia Probes Alleged Data Leak of 91 Million Users," Reuters, 3 May 2020; Lily Hay Newman, "ShinyHunters Is a Hacking Group on a Data Breach Spree," WIRED, 21 May 2020.

[41]Anindya and Subiyanto, "Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data."

[42]Law Number 27 of 2022, arts. 1(4) and 39.

[43]Law Number 27 of 2022, art. 37; Indonesian Civil Code, art. 1367.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

therefore does not treat every affected user as having an identical compensable claim, and it explains why a collective proceeding would need to separate the common questions from the individual ones.

e. Civil Liability and Remedy

If duty, breach, attribution, causation and legally recognisable damage are established, the final stages of the chain concern civil liability and remedy. The Civil Code provides the general basis for an unlawful-act claim, while the PDP Law provides a specialised compensation right in the context of personal-data processing.[44] The two regimes should be read together: the PDP Law supplies the specialised duty and remedial context, while private law supplies the general logic for attributing loss and determining compensation. The case therefore illustrates why "data leak" is not itself the conclusion. The legal conclusion depends on the completed chain: **controller → duty → breach → attribution → causation → damage → liability → compensation.**

f. Results of the Framework Test

The doctrinal test supports the usefulness of the Civil Liability Chain as an organising device. It converts a broad and often repetitive discussion of platform responsibility into a sequence of legal questions that can be answered by reference to specific primary rules and evidence. It also guards against two opposite errors: automatic liability merely because a breach occurred, and an overly narrow conception of consumer harm that recognises only immediate financial loss.

The practical conclusion is modest but important. The current Indonesian framework already contains the ingredients needed for a civil analysis, but those ingredients are distributed across different legal regimes and, in the case of the compensation procedure, remain incomplete pending implementing regulation. The contribution of this article is to connect them into a single private-law pathway without turning every breach into automatic liability or every affected consumer into an identical compensation claimant.

Table 1. The Civil Liability Chain for Personal Data Breaches

STAGE	CORE LEGAL QUESTION	PRIMARY LEGAL BASIS / BENCHMARK
LEGAL DUTY	What statutory obligation applies to the platform?	PDP Law arts. 1(4), 20–50, 37–39, 46–47; GR 71/2019; Consumer Protection Law art. 19
BREACH	Was that duty violated in a legally relevant way?	PDP Law arts. 39, 46; Civil Code arts. 1365–1366
ATTRIBUTION	Can the failure be attributed to the platform's sphere of control?	PDP Law art. 37; Civil Code art. 1367
CAUSATION	Did the breach cause the injury through a legally sufficient sequence?	Civil Code art. 1365; adequate causation; relativity of the norm
DAMAGE	What harm is legally recognisable and provable?	Civil Code art. 1365; PDP Law art. 12(1); GDPR art. 82 and CJEU case law, comparatively
CIVIL LIABILITY	What private-law consequence follows?	Civil Code arts. 1365–1367
COMPENSATION AND REDRESS	What form of remedy restores the consumer's position?	PDP Law art. 12; Consumer Protection Law arts. 19, 45–46; PERMA 1/2002

[44]Law Number 27 of 2022, art. 12; Indonesian Civil Code, art. 1365.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

D. CONCLUSION

This article concludes that civil liability for e-commerce data breaches cannot be determined solely from the fact that a security incident has occurred. The analysis must begin with the platform's legal position as a personal data controller and with the specific duties imposed by the PDP Law, which supply the normative baseline against which the platform's conduct is assessed. Articles 1365 to 1367 of the Civil Code then supply the general private-law framework through which an attributable breach causing legally recognised loss may generate an obligation to compensate.

The central contribution is the Civil Liability Chain, which links legal duty, breach, attribution, causation, damage, civil liability and compensation. The chain clarifies why a data breach is not identical to civil liability, and why a statutory right to compensation does not remove the need to establish legally attributable harm. It also provides a way to distinguish direct financial loss, consequential loss and non-material or privacy-related harm without assuming that every affected consumer suffers the same injury. Two of its elements are advanced as novel: the intervening-event test, which uses adequate causation and the relativity of the violated norm to decide when the later misuse of leaked data remains attributable to the original failure; and the separation of common breach issues from individual damage issues in collective proceedings.

Three practical implications follow. First, the compensation right in Article 12(1) of the PDP Law should be operationalised through the implementing regulation contemplated by Article 12(2), which should address the classification of recoverable loss and the procedure for claiming it. Second, courts should apply Article 28 of the Consumer Protection Law in data-breach disputes so that the platform bears the burden of demonstrating the adequacy of the measures within its control. Third, collective proceedings under the Consumer Protection Law and the Supreme Court Regulation on class actions should be structured so that common breach issues are determined collectively while damage is assessed individually.

This study has limitations. It is doctrinal and normative; it does not measure how Indonesian courts in fact decide data-breach claims, and no adjudicated Indonesian decision applying the PDP Law to a platform data breach was available for analysis. The Tokopedia incident is used as an illustration rather than as a decided case, and the comparative material is drawn from a single jurisdiction. Further research should therefore examine judicial decisions as they emerge, evaluate the implementing regulation once enacted, and extend the comparison to jurisdictions whose civil-law tradition is closer to Indonesia's, so that the Civil Liability Chain can be tested against actual adjudication rather than against doctrine alone.

BIBLIOGRAPHY

Journal Articles and Reports

Afifah, Nurul. "Tanggung Jawab Hukum Platform E-Commerce terhadap Keamanan Data Pribadi Pengguna: Analisis Berdasarkan UU PDP 2022" [The Legal Responsibility of E-Commerce Platforms for the Security of Users' Personal Data: An Analysis Based on the 2022 PDP Law]. Jurnal Legalitas 2, no. 1 (2024): 29–38. https://doi.org/10.58819/jle.v2i1.165.

Anindya, Ragil Putri, and Achmad Edi Subiyanto. "Tanggung Jawab Platform Tokopedia dalam Kasus Kebocoran Data Menurut Undang-Undang tentang Perlindungan Data Pribadi" [The Responsibility of the Tokopedia Platform in the Data Leakage Case under the Personal Data Protection Law]. RIGGS: Journal of Artificial Intelligence and Digital Business 4, no. 3 (2025): 1105–1112. https://doi.org/10.31004/riggs.v4i3.2105.

Creative Commons Attribution 4.0 International License

ISSN. 3090-0514 (online)
ISSN. 3090-1065 (Print

Mansawan, Isak Semuel Kejne, Jonhi Sassan, and Jefri Bernard. "Legal Protection of E-Commerce Consumers' Personal Data Under Indonesian Law." Jurnal Ilmu Hukum Kyadiren 7, no. 1 (2025): 538–554. https://doi.org/10.46924/jihk.v7i1.320.

Maulana, Muhammad Hasyim, and Sodikin. "Legal Protection for E-Commerce Consumers Against Personal Data Leaks." International Journal of Research and Innovation in Social Science 9, no. 11 (2025): 4234–4243. https://doi.org/10.47772/IJRISS.2025.91100329.

Newman, Lily Hay. "ShinyHunters Is a Hacking Group on a Data Breach Spree." WIRED, 21 May 2020.

Potkin, Fanny. "Indonesia's Tokopedia Probes Alleged Data Leak of 91 Million Users." Reuters, 3 May 2020.

Purnomo, Mahendra Bisma Wisdha Wardana, and Prasetijo Rijadi. "The Civil Law Perspective on Legal Consequences of Safeguarding Consumer Personal Data in Indonesian E-Commerce Activities." YURIS: Journal of Court and Justice 3, no. 4 (2024). https://doi.org/10.56943/jcj.v3i4.803.

Putra, Tegar Islami, Nurul Fibrianti, and Rizky Andeza Prasetya. "Liability of E-Commerce Service Providers for Processing Consumer Personal Data (Comparative Study of Indonesia & Europe)." Journal of Private and Commercial Law 9, no. 1 (2025): 72–109. https://doi.org/10.15294/jpcl.v9i1.9370.

Legislation

Republic of Indonesia. Indonesian Civil Code (Kitab Undang-Undang Hukum Perdata).

Republic of Indonesia. Law Number 8 of 1999 concerning Consumer Protection. State Gazette of the Republic of Indonesia Number 42 of 1999, Supplement to the State Gazette Number 3821.

Republic of Indonesia. Law Number 27 of 2022 concerning Personal Data Protection. State Gazette of the Republic of Indonesia Number 196 of 2022, Supplement to the State Gazette Number 6820.

Republic of Indonesia. Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. State Gazette of the Republic of Indonesia Number 185 of 2019, Supplement to the State Gazette Number 6400.

Republic of Indonesia. Supreme Court Regulation (PERMA) Number 1 of 2002 concerning Class Action Procedure.

European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). OJ L 119/1.

Court Decisions

Constitutional Court of the Republic of Indonesia. Decision Number 151/PUU-XXII/2024, 30 July 2025.

Court of Justice of the European Union. Case C-300/21, UI v Österreichische Post AG. ECLI:EU:C:2023:370, judgment of 4 May 2023.

Court of Justice of the European Union. Case C-340/21, VB v Natsionalna agentsia za prihodite. ECLI:EU:C:2023:986, judgment of 14 December 2023.

Creative Commons Attribution 4.0 International License