

Force Majeure in Electronic Agreements in the Digital Era: An Indonesian Civil Law Perspective

Widi Wiranti¹, Sandra Megayanti²

¹Faculty of Law, University of Bengkulu, Bengkulu, Indonesia,
widi.wiranti@unib.ac.id

²Faculty of Law, University of Bengkulu, Bengkulu, Indonesia,
sandra.megayanti@unib.ac.id

Corresponding Author: widi.wiranti@unib.ac.id

Abstract

Force majeure in electronic agreements presents a legal issue due to increasing reliance on electronic systems, digital networks, software, servers, payment infrastructure, and third-party technology providers. Technological disruptions may prevent or delay contractual performance, raising the question of whether they constitute force majeure or breach of contract under Indonesian civil law. This study examines the regulation of force majeure in electronic agreements, the criteria for classifying technological disruptions as force majeure or breach of contract, and the legal consequences of such classification. Using a normative juridical method with statutory and conceptual approaches, the analysis is based on Articles 1244, 1245, and 1338 of the Indonesian Civil Code and Law Number 1 of 2024 amending Law Number 11 of 2008 concerning Electronic Information and Transactions. The study finds that force majeure in electronic agreements is governed by the interaction of contract law principles and electronic transaction regulations. Technological disruptions cannot automatically be classified as force majeure; assessment must consider foreseeability, control, negligence, mitigation efforts, causation, contractual provisions, and risk allocation. Legal consequences may include exemption from damages, postponement of performance, or termination of the agreement where the impediment is permanent. Thus, classification requires a case-specific assessment under Indonesian civil law.

Keywords: breach of contract; contractual liability; electronic agreements; force majeure; technological disruption.

A. INTRODUCTION

The development of digital technology has significantly transformed legal relationships in business and commercial activities. Transactions that were previously conducted through conventional mechanisms are increasingly carried out through electronic systems using digital technologies and internet networks. This transformation has not only changed the manner in which transactions are conducted but has also

expanded the use of electronic agreements as legal instruments governing rights and obligations in digital transactions (Sepriadi et al., 2026).

Electronic agreements are increasingly used in various commercial activities, including transactions through online marketplaces, digital banking services, digital applications, and business cooperation conducted through electronic media. These agreements enable parties to establish contractual relationships without being physically present, thereby providing greater efficiency in terms of time, cost, and accessibility. However, the increasing use of electronic agreements also creates legal challenges concerning the validity of agreements, evidentiary issues, identification of the contracting parties, and, particularly, the performance of contractual obligations through electronic systems.

Unlike conventional agreements, the formation and performance of electronic agreements may depend substantially on the availability and reliability of electronic systems, networks, software, servers, payment infrastructure, and other technological services. Consequently, the performance of contractual obligations may be affected not only by the intentions, capacity, and conduct of the contracting parties but also by technological conditions beyond their immediate control. This technological dependence creates a specific legal issue when a disruption prevents or delays the performance of contractual obligations.

In practice, technological disruptions may take various forms, including server downtime, internet network failures, payment system disruptions, software or infrastructure failures, and cyberattacks. Such disruptions may prevent a party from performing an obligation within the time or manner stipulated in the agreement. The resulting legal issue is whether the disruption should be regarded as force majeure, which may affect the party's contractual liability, or as a breach of contract for which the party

remains liable. This distinction is particularly important because the occurrence of a technological disruption does not, by itself, establish the existence of force majeure.

Under Indonesian civil law, force majeure is closely related to the liability arising from non-performance of contractual obligations. Articles 1244 and 1245 of the Indonesian Civil Code provide the principal legal basis for determining the consequences of circumstances that prevent a debtor from fulfilling its obligations, while Article 1338 establishes the binding force of agreements and the principle of contractual freedom. In the context of electronic agreements, these general principles operate alongside the legal framework governing electronic transactions, including Law Number 1 of 2024 concerning the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. However, these provisions do not establish specific parameters for determining when a technological disruption should be legally classified as force majeure rather than breach of contract.

Several previous studies have addressed related aspects of this issue. Kamilah et al. (2025), in “The Doctrine of Force Majeure in the Law of Obligations: Implications for Business Contracts in the Digital Era,” examine the application of the force majeure doctrine in the law of obligations and its implications for business contracts in the digital era. The study emphasizes the challenges of applying force majeure in digital contracts and the importance of formulating specific force majeure clauses. Nevertheless, it does not develop specific legal parameters for determining whether a technological disruption constitutes force majeure or results from the negligence of the party concerned.

Putri et al. (2026), in “Breach of Contract in the Digital Era: Legal Liability in Electronic Agreements,” examine forms of breach of contract in electronic agreements and the resulting legal liability under civil law and regulations governing electronic transactions. The study recognizes that system disruptions, cyberattacks, and

technological infrastructure failures may be relevant to force majeure. However, it does not specifically examine the allocation of liability when the disruption originates from technological systems or infrastructure operated by third parties, such as platform providers, network providers, or electronic system operators.

Similarly, Sepriadi et al. (2026), in “The Legal Relationship between Electronic Contracts and Digital Transaction Security,” examine the relationship between electronic contracts and digital transaction security, including risks affecting the performance of electronic transactions. The study primarily focuses on transaction security and protection in the use of electronic systems and does not specifically analyze the legal consequences of technological disruptions under the doctrine of force majeure or the resulting liability of the contracting parties.

These studies demonstrate that the existing literature has addressed force majeure in digital business contracts, breach of contract in electronic agreements, and security risks in electronic transactions. Nevertheless, a specific legal framework for distinguishing technological disruptions that constitute force majeure from those that constitute breach of contract remains insufficiently developed under Indonesian civil law. More specifically, the existing literature has not adequately integrated the cause and nature of the disruption, its foreseeability, the degree of control exercised by the contracting parties, the existence and scope of contractual force majeure clauses, reasonable mitigation efforts, causation, and contractual allocation of technological risks into a single analytical framework. The issue is particularly significant where a technological disruption originates from a third-party provider because the party bound by the primary agreement may have limited or no direct control over the system or infrastructure that causes the disruption.

The novelty of this study therefore lies in developing a contextual legal framework for qualifying technological disruptions as force majeure or breach of contract in electronic agreements under Indonesian civil law. Rather than merely applying the general doctrine of force majeure to electronic transactions, this study proposes an integrated assessment based on seven interrelated parameters: the nature and cause of the disruption, foreseeability, the parties' degree of control, fault or negligence, reasonable mitigation efforts, causation, and contractual allocation of risk, including risks arising from third-party technology providers. This framework is intended to clarify the legal boundary between circumstances that may justify exemption from contractual liability and technological disruptions that remain attributable to the party responsible for contractual performance.

Accordingly, this study contributes to the development of Indonesian civil law by clarifying the legal criteria for determining the qualification of technological disruptions and the resulting consequences for contractual liability. The analysis focuses not only on whether a disruption prevents or delays performance but also on whether the disruption was beyond the reasonable control of the affected party, whether reasonable preventive or mitigating measures were undertaken, and how the parties had allocated technological risks through their agreement. Based on these considerations, this study addresses the following research questions, **First**, how is force majeure regulated in electronic agreements under Indonesian civil law; **second**, what criteria are used to determine whether technological disruptions in the performance of electronic agreements constitute force majeure or breach of contract; and **third**, what are the legal consequences of classifying such technological disruptions as force majeure for the liability of parties in electronic agreements?

B. RESEARCH METHODS

This study employs a normative juridical research method, which focuses on examining legal norms, legal principles, and legal doctrines relating to *force majeure* in the performance of electronic agreements. The approaches employed in this study include the statutory approach and the conceptual approach. The statutory approach is conducted by analyzing legal provisions governing agreements, breach of contract, *force majeure*, and electronic transactions, including the Indonesian Civil Code (*Kitab Undang-Undang Hukum Perdata*), Law No. 1 of 2024 amending Law No. 11 of 2008 on Electronic Information and Transactions, and other relevant laws and regulations. Meanwhile, the conceptual approach is employed to examine the concepts of *force majeure*, breach of contract, performance of contractual obligations, and the legal liability of the parties in electronic agreements.

The legal materials used in this study consist of primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations relating to contract law, *force majeure*, breach of contract, and electronic transactions. Secondary legal materials comprise legal books, scholarly journals, research findings, and the views and doctrines of legal scholars relevant to the subject matter of the study. Tertiary legal materials include legal dictionaries, encyclopedias, and other reference sources used to support the understanding of legal terms and concepts analyzed in this study.

The legal materials are analyzed qualitatively through juridical and conceptual analysis. The analysis is conducted by identifying, interpreting, and systematically examining the relevant legal norms and legal concepts concerning *force majeure*, breach of contract, and electronic agreements. The analysis begins by examining the legal basis and principles governing *force majeure* under Indonesian civil law, particularly Articles 1244, 1245, and 1338 of the Indonesian Civil Code, in conjunction with the legal framework governing electronic transactions. The relevant provisions are then interpreted

and connected with the concepts of *force majeure*, contractual liability, and breach of contract to determine their applicability to technological disruptions occurring in the performance of electronic agreements.

Furthermore, technological disruptions are analyzed based on several interrelated legal considerations, namely the nature and cause of the disruption, foreseeability, the degree of control exercised by the contracting parties, the existence of fault or negligence, reasonable preventive and mitigating efforts, the causal relationship between the disruption and the non-performance of contractual obligations, and the contractual allocation of technological risks. Where the disruption originates from a third-party technology provider, such as a platform provider, network provider, cloud service provider, payment gateway, or electronic system operator, the analysis further considers the affected party's degree of control over the third-party system and the contractual allocation of such risks. The results of the analysis are subsequently synthesized to determine whether the technological disruption qualifies as *force majeure* or constitutes a breach of contract and to identify the resulting legal consequences for the liability of the contracting parties.

C. ANALYSIS AND DISCUSSION

a. Regulation of force majeure in the performance of electronic agreements under Indonesian civil law

Force majeure, commonly understood in Indonesian law as *keadaan memaksa*, is an important concept in contract law that provides legal protection to a party who is unable to perform its contractual obligations due to circumstances beyond its control. In contractual practice, *force majeure* is commonly regulated through a specific contractual clause that determines the circumstances that may qualify as *force majeure*, the procedures for notifying the other party, and the legal

consequences arising from the occurrence of such circumstances. A well-drafted *force majeure* clause therefore serves not merely as an instrument for relieving a party from contractual liability, but also as a mechanism for allocating risks between the parties and providing greater certainty concerning the consequences of events that interfere with contractual performance.

Under Indonesian civil law, *force majeure* is not governed by a single provision containing a comprehensive definition. Its principal legal basis can be found in the provisions concerning compensation for breach of contract, particularly Articles 1244 and 1245 of the Indonesian Civil Code (*Kitab Undang-Undang Hukum Perdata* or *KUHPerdata*) (Khairandy, 2005, p. 105). Article 1244 establishes, in principle, the debtor's obligation to compensate for costs, losses, and interest when an obligation is not performed or is performed late, unless the debtor can demonstrate that the failure or delay resulted from an unforeseen circumstance for which the debtor cannot be held responsible and that no bad faith was involved (Khilmi & Triana, 2025). Article 1245 further provides that compensation is not required where the debtor is prevented from performing the obligation due to *force majeure* or an unforeseen and involuntary circumstance. These provisions therefore constitute an important normative basis for determining whether a party may be exempted from liability for damages when contractual performance is prevented by circumstances beyond its control (Tori & Tedjomurti, 2021).

The application of Articles 1244 and 1245 of the *KUHPerdata* demonstrates that the existence of an event that interferes with contractual performance does not automatically establish *force majeure*. The relevant circumstance must be assessed in relation to the debtor's obligations, the nature of the event, the parties' contractual arrangements, and the extent to which the event was beyond the debtor's control. In

general, circumstances that may support a claim of *force majeure* include events that could not reasonably have been foreseen at the time the contract was concluded, could not reasonably have been prevented or overcome, and were not attributable to the party seeking exemption from liability. Consequently, the determination of *force majeure* requires a case-by-case assessment rather than an automatic classification based solely on the occurrence of an external event.

In civil law doctrine, *force majeure* is commonly distinguished into absolute and relative *force majeure*. Absolute *force majeure* refers to circumstances in which contractual performance becomes objectively impossible, whereas relative *force majeure* refers to circumstances in which performance remains theoretically possible but is prevented or substantially hindered by extraordinary circumstances. This distinction may affect the legal consequences arising from the event, particularly whether the contractual obligation is temporarily suspended, whether performance remains possible after the obstacle has ceased, or whether the contractual relationship may ultimately be terminated. Nevertheless, the classification of an event as absolute or relative *force majeure* cannot be determined solely by reference to its general characteristics. It must also take into account the contractual provisions, the nature of the obligation, and the actual circumstances affecting performance.

The regulation of *force majeure* is also closely connected with the principle of freedom of contract as reflected in Article 1338 of the *KUHPerdata*. This provision establishes the binding force of agreements and reflects the principle that parties are generally free to determine the contents of their contractual relationship, subject to applicable legal requirements. Within this framework, the parties may formulate a *force majeure* clause that identifies specific events, establishes notification and

mitigation obligations, and determines the consequences of such events for contractual performance. Contractual regulation is particularly significant because the statutory provisions on *force majeure* under the *KUHPerdata* are formulated in general terms and do not specifically address the increasingly diverse forms of disruption that may arise in contemporary contractual relationships (Tampoli, 2021).

The development of information and communication technology has significantly transformed the formation and performance of contracts. Contractual relationships are no longer limited to conventional face-to-face transactions or physically signed documents. Parties may now conclude and perform agreements through electronic systems, including by exchanging electronic offers and acceptances, making electronic payments, transmitting contractual documents, and using digital platforms to fulfill their respective obligations. These developments have increased the practical importance of determining how general principles of contract law, including *force majeure*, apply to electronic contractual relationships.

In Indonesia, electronic transactions are regulated under Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended, most recently, by Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (the *ITE Law*). Article 18 paragraph (1) recognizes that electronic transactions embodied in electronic contracts are binding upon the parties. Meanwhile, Article 19 provides that parties engaging in electronic transactions must use an Electronic System agreed upon by the parties. These provisions confirm the legal recognition of electronic contracts while simultaneously demonstrating that electronic contractual performance depends upon technological systems and infrastructure whose

operation may involve service providers, electronic agents, network infrastructure, and other technological components.

The technological characteristics of electronic contracts create forms of disruption that are different from those commonly encountered in conventional contractual relationships. System failures, network interruptions, server unavailability, cyber-related incidents, platform failures, and disruptions to digital payment systems may interfere with a party's ability to perform its contractual obligations. For example, a party may be unable to transmit a required document, process a payment, deliver digital goods, or complete a transaction within the agreed period because the electronic system used to perform the obligation becomes unavailable. Such circumstances raise a fundamental legal question: under what conditions can a technological disruption be classified as *force majeure*, and when should it instead be regarded as a breach of contract (*wanprestasi*)?

This question is particularly significant because the existence of a technological disruption does not necessarily establish the absence of fault on the part of the party whose performance has been affected. A system failure may result from an external event beyond the party's reasonable control, but it may also arise from inadequate system maintenance, failure to implement reasonable security measures, insufficient technological capacity, or negligence in selecting and managing a service provider. Accordingly, the legal assessment cannot be based merely on the fact that a technological system experienced a disruption. It must examine the cause, foreseeability, preventability, contractual allocation of risk, and the affected party's efforts to mitigate the consequences of the disruption (Republik Indonesia, 2024).

The existing legal framework presents a particular challenge in this regard. The *KUHP* provides the general legal basis for *force majeure* and exemption from liability for damages through Articles 1244 and 1245, while Article 1338 provides a basis for the parties to regulate their contractual relationship, including through a *force majeure* clause. On the other hand, the *ITE Law* establishes the legal framework for electronic transactions and recognizes the binding nature of electronic contracts. However, these provisions do not establish specific and comprehensive criteria for determining when a technological disruption affecting an electronic contract constitutes *force majeure*. The absence of specific statutory parameters leaves considerable room for legal interpretation in distinguishing a genuine *force majeure* event from a technological failure that remains within the contractual responsibility of the affected party.

The problem becomes more complex when the technological infrastructure involved in contractual performance is operated by a third party. In such circumstances, a party may argue that it should not be held liable because the failure originated from an external electronic system or service provider. Nevertheless, the involvement of a third party does not automatically eliminate the contractual responsibility of the party bound by the agreement. The relevant legal assessment must consider whether the third-party disruption was genuinely beyond the party's reasonable control, whether the risk had been allocated contractually, whether the party had taken reasonable preventive measures, and whether the party complied with its obligations to notify and mitigate the effects of the disruption.

Therefore, the application of *force majeure* to electronic contracts requires an integrated examination of general contract law and the specific characteristics of electronic transactions. The provisions of Articles 1244 and 1245 of

the *KUHPerdata* provide the primary normative framework for assessing exemption from liability, while Article 1338 provides a basis for contractual risk allocation through *force majeure* clauses. At the same time, the *ITE Law* provides legal recognition and establishes the regulatory framework for electronic contracts and electronic transaction systems. The interaction between these legal regimes indicates that the electronic nature of a contract does not displace the general principles of contractual liability; rather, it introduces additional factual and legal considerations that must be taken into account when determining whether non-performance is attributable to *force majeure*.

Against this background, the central legal issue is the absence of clear and specific parameters for determining whether technological disruptions in the performance of electronic contracts should be qualified as *force majeure* or *wanprestasi*. This uncertainty may create legal risks for both contracting parties, particularly in determining the allocation of liability, the continuation or suspension of contractual obligations, and the entitlement to compensation. A clearer legal framework is therefore necessary to ensure that the application of *force majeure* does not become an instrument for avoiding contractual responsibility when the disruption could reasonably have been prevented or overcome, while at the same time ensuring legal protection for parties genuinely affected by circumstances beyond their control.

Accordingly, this study examines the application of the doctrine of *force majeure* to technological disruptions in the performance of electronic contracts under Indonesian law. The study focuses on the legal basis for *force majeure*, the relevance of Articles 1244, 1245, and 1338 of the *KUHPerdata*, the position of electronic contracts under the *ITE Law*, and the legal criteria that may be used to

distinguish technological disruptions constituting *force majeure* from those constituting *wanprestasi*. Through this analysis, the study seeks to contribute to a more precise understanding of risk allocation and contractual liability in the increasingly digital environment of Indonesian contract law.

b. Qualification of technological disruptions as force majeure or breach of contract in the performance of electronic agreements

The development of information technology has increasingly transformed the manner in which contractual obligations are performed. In electronic agreements, contractual performance may depend upon internet networks, servers, software, electronic payment systems, data centers, cloud service providers, and other technological infrastructure. Although such technological dependence provides efficiency and facilitates the implementation of contractual relationships, it also introduces new risks that may interfere with the fulfillment of contractual obligations. These risks may include system failures, network interruptions, server downtime, software malfunctions, electronic payment failures, data center disruptions, and service interruptions originating from third-party technology providers (Abigail et al., 2025). The emergence of such disruptions raises an important legal issue: whether a technological disruption should be qualified as *force majeure* or, instead, as a breach of contract (*wanprestasi*) (Kamilah et al., 2025).

The qualification of a technological disruption must principally be assessed within the legal framework governing *force majeure* under Indonesian civil law. Articles 1244 and 1245 of the Indonesian Civil Code (*Kitab Undang-Undang Hukum Perdata* or *KUHPerdata*) provide the principal statutory basis for determining whether a failure to perform a contractual obligation may result in

exemption from liability for costs, damages, and interest. These provisions indicate that an event affecting contractual performance may justify exemption from liability where the non-performance or delay results from circumstances for which the debtor cannot reasonably be held responsible. Consequently, the mere occurrence of a technological disruption does not automatically release a party from contractual liability. Rather, the nature and cause of the disruption, its impact on contractual performance, and the circumstances surrounding the affected party's inability to perform must be examined (Tai, 2018).

One of the principal parameters in determining whether a technological disruption constitutes *force majeure* is **foreseeability**. An event may support a claim of *force majeure* where, at the time the agreement was concluded, it could not reasonably have been anticipated by the party responsible for performance. In the technological context, however, foreseeability requires careful examination because technological failures vary considerably in nature and degree. Extraordinary disruptions affecting critical digital infrastructure may differ substantially from routine system failures, maintenance problems, or service interruptions that can reasonably be anticipated as part of ordinary technological operations.

The relevant inquiry is therefore not limited to whether the affected party actually anticipated the occurrence of the disruption. Rather, the assessment should consider whether a reasonable party, in light of the nature of the contractual activity and the technological infrastructure involved, could have anticipated the relevant risk when entering into the agreement. This objective approach is important to prevent ordinary technological risks from being improperly characterized as *force majeure*. Where a particular technological risk is reasonably foreseeable and forms

part of the ordinary operational risks of the business, the party responsible for performance may be expected to take appropriate preventive measures.

A second parameter concerns whether the technological disruption was **beyond the reasonable control of the party responsible for performance**. The stronger the evidence that the source of the disruption was outside the party's capacity to control, prevent, or manage, the stronger the basis for considering *force majeure*. Conversely, where the disruption originates from circumstances falling within the party's operational responsibility, reliance on *force majeure* becomes more difficult to justify.

For example, where a company fails to perform its contractual obligations because its internal electronic system becomes unavailable as a result of inadequate maintenance, insufficient system capacity, or an avoidable configuration failure, the disruption should not automatically be treated as *force majeure*. The relevant assessment should instead examine the cause of the failure and whether the party had a reasonable opportunity to prevent or mitigate the resulting disruption. Thus, the concept of control should be understood not merely in terms of direct physical control over a technological system, but also in terms of the party's reasonable capacity to manage the technological risks associated with its contractual obligations. A third parameter is the absence of fault or negligence on the part of the party invoking *force majeure*.

A technological disruption that results from the party's own negligence generally provides a weak basis for exemption from contractual liability. Parties that rely on technological systems to perform contractual obligations may reasonably be expected to adopt measures appropriate to the nature and level of technological risks involved. Negligence in this context may include failure to

conduct appropriate system maintenance, failure to implement adequate backup mechanisms, neglect of necessary security updates, failure to establish reasonable system recovery procedures, or failure to implement appropriate risk-management measures. Therefore, the legal assessment should distinguish between technological failures that genuinely arise from circumstances beyond the party's reasonable control and failures that result from inadequate system management, poor preparation, or insufficient risk mitigation (Widiyaningsih et al., 2025).

The fourth parameter concerns the ability to prevent, overcome, or mitigate the effects of the disruption. The assessment of *force majeure* should not focus exclusively on the occurrence of an external event but should also consider the conduct of the party after the disruption occurs. A party affected by a technological disruption may be expected, depending on the circumstances, to take reasonable measures to mitigate its consequences and resume contractual performance.

In electronic contractual relationships, such measures may include the use of backup servers, alternative networks, redundant systems, data recovery mechanisms, alternative payment channels, or other reasonably available technological solutions. If a disruption could reasonably have been overcome through available measures but the affected party failed to take such measures, its reliance on *force majeure* may be subject to challenge. Accordingly, the existence of a technological disruption should be considered together with the affected party's efforts to minimize its impact on contractual performance.

A fifth parameter is the causal relationship between the technological disruption and the failure to perform the contractual obligation. The party invoking *force majeure* should establish that the disruption materially caused the non-performance or delay. The mere temporal coincidence between a system failure

and the failure to perform does not necessarily establish the required causal connection.

The causal assessment should therefore consider whether the contractual obligation could reasonably have been performed through alternative means despite the technological disruption. Where alternative methods were reasonably available and could have enabled performance, but the affected party failed to use them without adequate justification, the causal connection between the technological disruption and the non-performance may be weakened. Accordingly, the existence and strength of causation must be assessed on a case-by-case basis by considering the nature of the contractual obligation, the technological system involved, the degree of dependence on that system, and the availability of reasonable alternatives.

In addition to these five parameters, the contractual *force majeure* clause plays an important role in determining how technological risks are allocated between the parties. Consistent with the principle of freedom of contract, parties may expressly identify circumstances that they agree will constitute *force majeure*, including system failures, network disruptions, failures of technology service providers, data center incidents, or other technological events that may interfere with contractual performance. The clause may also establish notification requirements, mitigation obligations, procedures for suspending performance, and the consequences of a disruption that continues beyond a specified period (Putri et al., 2026).

Nevertheless, the inclusion of a particular technological event in a *force majeure* clause should not necessarily be interpreted as eliminating all further legal assessment. The actual circumstances of the event remain relevant, particularly where the contractual clause requires the event to be beyond the affected party's

control or excludes circumstances caused by its own negligence. Consequently, contractual designation and factual qualification should be examined together. A clause may allocate a particular technological risk between the parties, but its application still depends upon the wording of the clause, the circumstances of the event, and the obligations imposed upon the parties.

A particularly complex issue arises where a technological disruption originates from a third-party service provider. Electronic contractual performance may depend upon cloud computing providers, payment gateways, internet service providers, data centers, digital platforms, or other technology service providers. A disruption occurring within the infrastructure of such a provider may directly affect the ability of a contracting party to perform its contractual obligations.

However, the involvement of a third party does not, by itself, establish *force majeure*. The relevant question is whether the disruption affecting the third-party provider was a risk that the contracting party could reasonably have anticipated, controlled, or mitigated. The assessment should consider, among other factors, the contractual allocation of risk, the nature and importance of the third-party service, the availability of alternative providers or systems, and the preventive measures adopted by the affected party.

The use of a third-party technology provider should therefore be distinguished from an event that genuinely lies beyond the reasonable control of the contracting party. Where the disruption constitutes an ordinary operational risk associated with the use of a particular service provider, the contracting party may be expected to anticipate that risk and adopt appropriate contingency measures. Conversely, where the third-party disruption results from an extraordinary event that could not reasonably have been anticipated or prevented and directly prevents contractual

performance, the circumstances may provide a stronger basis for invoking *force majeure*. The ultimate qualification must nevertheless be determined by reference to the specific contractual arrangements and factual circumstances.

This distinction is particularly important because contractual responsibility cannot automatically be transferred to a third-party service provider merely because the latter operates the technological infrastructure necessary for performance. As between the contracting parties, the party that has undertaken the contractual obligation generally remains responsible for determining whether it can perform that obligation and for managing the technological arrangements upon which performance depends, subject to the terms of the agreement and applicable law. Accordingly, reliance upon an external technology provider may constitute an element of the *force majeure* analysis, but it should not operate as an automatic exemption from liability.

Conversely, a technological disruption may constitute breach of contract (*wanprestasi*) where the failure to perform is attributable to the fault or negligence of the party responsible for performance. In electronic agreements, such circumstances may arise where a party fails to maintain technological infrastructure for which it is responsible, fails to implement agreed security or recovery mechanisms, disregards contractual system requirements, or relies upon a technological disruption even though the relevant risk was reasonably foreseeable and could have been prevented or mitigated.

The distinction between *force majeure* and *wanprestasi*, therefore, should not be based solely on the existence of a technological disruption. The decisive assessment concerns the source of the disruption, foreseeability, the degree of control available to the affected party, the existence of fault or negligence, the

possibility of prevention or mitigation, the causal relationship with the failure to perform, and the contractual allocation of technological risks. These factors collectively determine whether the affected party may legitimately rely upon *force majeure* or should remain responsible for the consequences of non-performance.

Evidentiary considerations are also essential in determining the legal qualification of a technological disruption. A party invoking *force majeure* should be able to demonstrate not only that a technological disruption occurred, but also the nature, cause, duration, and consequences of the disruption and its direct effect on contractual performance. In the context of electronic agreements, relevant evidence may include official notifications from technology service providers, system logs, records of *downtime*, technical reports, incident reports, system documentation, and evidence demonstrating the preventive and mitigation measures undertaken by the affected party.

Such evidence is important because technological disruptions may be difficult to evaluate solely on the basis of the affected party's assertion. Technical evidence can assist in determining whether the disruption originated from an external event, whether it was reasonably foreseeable, whether it could have been prevented or overcome, and whether it actually prevented contractual performance. Evidentiary assessment therefore constitutes an important mechanism for distinguishing genuine *force majeure* from technological failures attributable to inadequate system management or negligence.

Based on the foregoing analysis, a technological disruption cannot automatically be qualified as either *force majeure* or breach of contract (*wanprestasi*). Its legal classification requires a contextual and case-by-case assessment. The relevant considerations include the foreseeability of the disruption,

its source, the degree of control available to the affected party, the existence or absence of fault or negligence, the possibility of preventing or mitigating its consequences, the causal relationship between the disruption and non-performance, the terms of the contractual *force majeure* clause, and the measures undertaken by the affected party.

Where a technological disruption arises from an extraordinary circumstance beyond the affected party's reasonable control, could not reasonably have been anticipated or prevented, is not attributable to its fault or negligence, and directly prevents contractual performance, the circumstances may provide a legal basis for invoking *force majeure*. Conversely, where the disruption arises from a technological risk within the party's reasonable sphere of responsibility, could reasonably have been anticipated or mitigated, or results from inadequate technological management, the affected party may remain liable for breach of contract.

Accordingly, the application of *force majeure* to electronic agreements requires a legal approach that integrates the general principles of Indonesian contract law with the specific characteristics of technology-dependent contractual performance. Such an approach is necessary to maintain an appropriate balance between protecting parties from extraordinary events genuinely beyond their control and preventing the *force majeure* doctrine from being used as a means of avoiding contractual responsibility for technological risks that should reasonably have been anticipated, managed, or mitigated.

c. Legal consequences of technological disruptions qualified as *force majeure* on the liability of the parties in electronic agreements

Technological disruptions that satisfy the legal characteristics of *force majeure* give rise to legal consequences that differ from disruptions resulting from the fault or negligence of a contracting party. Once a technological disruption is established as *force majeure*, the principal legal issue is the extent to which the affected party may be relieved from liability for the non-performance or delayed performance of its contractual obligations. This issue is particularly significant in electronic agreements because contractual performance may depend upon electronic systems, networks, software, servers, data centers, payment systems, and third-party technology providers. Accordingly, the legal consequences of *force majeure* should be determined not only by reference to the general principles of contract law but also by considering the contractual arrangements made by the parties and the specific characteristics of the electronic contractual relationship (Abigail et al., 2025).

The principal statutory basis for exemption from liability arising from *force majeure* is found in Articles 1244 and 1245 of the Indonesian Civil Code (*Kitab Undang-Undang Hukum Perdata* or *KUHPerdata*). Article 1244 generally places the debtor under an obligation to compensate for costs, losses, and interest in cases of non-performance or delayed performance, unless the debtor can establish that the failure resulted from an unforeseen circumstance for which the debtor cannot be held responsible and that no bad faith was involved. Article 1245 further provides that compensation is not required where the debtor is prevented from performing the obligation due to *force majeure* or an unforeseen and involuntary circumstance. These provisions establish that the principal consequence of a valid *force majeure* claim is exemption from liability for damages resulting from the non-

performance or delay, insofar as the statutory and contractual requirements have been satisfied.

Such exemption, however, should not be interpreted as an automatic extinguishment of all contractual obligations. The legal consequences of *force majeure* depend upon the nature and duration of the impediment, the type of contractual obligation affected, the terms of the agreement, and the possibility of continued performance after the impediment ceases. Where a technological disruption is temporary and contractual performance remains possible once the disruption has ended, the appropriate consequence may be the postponement or extension of the period for performance. By contrast, where the disruption makes performance permanently impossible, the consequences may extend to termination or other forms of adjustment, subject to the contractual provisions and applicable law.

The distinction between temporary and permanent impediments is particularly relevant in electronic agreements. A temporary server failure, network interruption, or payment-system outage may prevent a party from performing an obligation at the agreed time while leaving the underlying performance objectively possible once the system is restored. In such circumstances, the existence of *force majeure* does not necessarily justify termination of the contractual relationship. The parties may instead continue performance after the technological impediment has ceased. Conversely, where a technological event permanently eliminates the means necessary for contractual performance, it becomes necessary to determine whether performance remains possible through alternative means or whether the contractual relationship should be terminated or otherwise adjusted in accordance with the agreement and applicable law (Labibah et al., 2026).

One possible consequence of a temporary *force majeure* event is therefore postponement or extension of contractual performance. Where the technological disruption genuinely prevents performance for a limited period, the affected party may have grounds to delay performance for the duration of the impediment. Such postponement should not be understood as a permanent release from the contractual obligation. Once the impediment has ceased and performance becomes reasonably possible, the obligation may resume in accordance with the contractual arrangements. For this reason, an electronic agreement should, where appropriate, specify the consequences of a technological *force majeure* event, including whether performance will be postponed, the applicable extension period, the obligation to renegotiate, or the circumstances in which termination may occur (Sidauruk et al., 2024).

Another important consequence concerns the allocation of risks between the parties. Technological risks may arise from systems operated directly by one of the parties, shared technological infrastructure, or third-party technology providers. Where the agreement expressly allocates a particular technological risk to one party, that allocation should be taken into account when determining the consequences of the disruption. Where the agreement is silent or ambiguous, the allocation of risk must be assessed in accordance with the applicable principles of contract law, the nature of the contractual obligation, the circumstances of the disruption, and the parties' respective responsibilities.

Thus, *force majeure* should not be viewed solely as a mechanism for eliminating liability for damages. It also functions as a framework for determining how the economic and legal consequences of an extraordinary event should be distributed between the contracting parties. This aspect is particularly important in

electronic contracts because technological dependencies may involve several interconnected systems and service providers, making it necessary to determine which risks were reasonably assumed by each party when entering into the agreement.

Even where a technological disruption has been established as *force majeure*, the affected party remains subject to good faith and reasonable mitigation requirements. Exemption from liability does not ordinarily mean that the affected party may remain passive while the consequences of the disruption continue to increase. Depending upon the circumstances, reasonable mitigation measures may include activating backup systems, restoring data, migrating temporarily to alternative infrastructure, using alternative networks or payment channels, or adopting other technically and commercially reasonable measures to reduce the impact of the disruption.

The requirement of mitigation is closely connected with the principle of good faith in contractual performance. A party affected by *force majeure* should make reasonable efforts to minimize the adverse consequences of the disruption and, where possible, restore contractual performance. The extent of the mitigation obligation should nevertheless be assessed proportionately. The affected party should not be required to undertake measures that are impossible, excessively burdensome, or commercially unreasonable in the circumstances. The relevant standard is therefore one of reasonable efforts rather than an absolute obligation to eliminate every consequence of the technological disruption.

Notification to the other party may also constitute an important contractual consequence of *force majeure*. Electronic agreements may establish a requirement that the affected party notify the other party within a specified period and provide

relevant information concerning the nature, cause, duration, and anticipated impact of the technological disruption. Timely notification allows the other party to take appropriate steps to minimize its own losses and facilitates communication concerning the continuation of contractual performance.

Where the contract expressly establishes a notification procedure, failure to comply with that requirement may affect the affected party's ability to rely upon the contractual *force majeure* mechanism, depending upon the wording and legal effect of the clause. This is particularly relevant where delayed notification causes additional losses that could reasonably have been avoided. Accordingly, notification should be understood not merely as an administrative formality but as part of the contractual mechanism for transparency, risk management, and mitigation (Sinaga et al., 2023).

The legal consequences become more complex where the technological disruption originates from a third-party technology provider. Electronic contractual performance may depend upon cloud service providers, payment gateways, data centers, internet service providers, digital platforms, or other technology providers. A disruption occurring within the infrastructure of such a provider may directly affect the ability of a contracting party to perform its obligation under the primary contract.

In this situation, two contractual relationships must be distinguished. The first is the primary contractual relationship between the contracting parties, while the second is the separate contractual relationship between one of the contracting parties and the technology provider. A technological failure in the second relationship does not automatically determine the rights and obligations arising from the first. The parties to the primary agreement must still examine whether the

third-party disruption satisfies the requirements of *force majeure*, whether the relevant risk was allocated by contract, and whether the affected party took reasonable steps to prevent or mitigate the consequences.

For example, if a party relies upon a cloud service provider and that provider experiences an extraordinary and unforeseeable infrastructure failure that directly prevents contractual performance, the disruption may provide a basis for invoking *force majeure* in the primary contractual relationship if the applicable requirements are satisfied. However, if the party selected an unreliable provider, failed to maintain reasonable backup arrangements, or could have used an alternative system without disproportionate difficulty, the third-party failure may not necessarily justify exemption from contractual liability. The involvement of a third party therefore constitutes a relevant factual circumstance, rather than an automatic ground for exemption.

Where the technological disruption is temporary, the principle of contractual preservation may support postponement or extension of performance rather than immediate termination. The purpose is to preserve the contractual relationship where performance remains possible after the impediment has ceased. However, where the disruption continues for an extended period or permanently prevents performance, the parties may need to consider contractual mechanisms concerning renegotiation, suspension, termination, or other forms of adjustment.

Accordingly, the legal consequences of a technological *force majeure* event may generally take several forms. First, the affected party may be exempted from liability for damages arising from non-performance or delayed performance that is directly caused by the *force majeure* event. Second, where the impediment is temporary, the parties may be entitled to postpone or extend the period for

performance, subject to the terms of the agreement. Third, where the impediment is permanent or fundamentally prevents contractual performance, the contractual relationship may, depending upon the circumstances and applicable contractual provisions, be subject to termination, renegotiation, or other contractual adjustment.

These consequences should not, however, be applied mechanically. The appropriate legal consequence depends upon the contractual *force majeure* clause, the nature of the affected obligation, the duration and severity of the technological disruption, the causal connection between the disruption and the non-performance, the parties' risk allocation, and the mitigation measures undertaken by the affected party.

Therefore, classification of a technological disruption as *force majeure* does not mean that the parties are entirely released from their contractual relationship. The principal exemption concerns liability for losses caused by non-performance or delay that is genuinely attributable to the *force majeure* event. Obligations that remain capable of performance may continue to bind the parties. In addition, the affected party may remain required to provide notification, cooperate with the other party, undertake reasonable mitigation measures, and resume performance once the impediment has ceased and performance becomes possible.

The application of *force majeure* in electronic agreements should consequently be based on a proportionality and risk-allocation approach. The doctrine should protect a party that is genuinely prevented from performing its contractual obligations by an extraordinary event beyond its reasonable control, while preventing technological risks that should reasonably have been anticipated and managed from being shifted improperly to the other contracting party.

Based on the foregoing analysis, the legal consequences of technological disruptions classified as *force majeure* are not limited to exemption from liability for damages. Depending upon the circumstances, they may also include postponement or extension of contractual performance and, where performance becomes permanently impossible, termination, renegotiation, or other forms of contractual adjustment. Nevertheless, the application of these consequences remains dependent upon the terms of the agreement, the applicable legal framework, the nature and duration of the technological disruption, the causal relationship with the failure to perform, and the affected party's compliance with its obligations of good faith, notification, and reasonable mitigation. This approach is necessary to maintain a balance between protecting parties from extraordinary technological disruptions and preserving the legitimate contractual interests of the other party.

D. CONCLUSION

This study concludes that technological disruption in the performance of electronic agreements does not automatically constitute *force majeure* or breach of contract (*wanprestasi*). Its legal qualification under Indonesian civil law depends primarily on the cause of the disruption, the extent of the affected party's control, the existence of fault or negligence, and the causal relationship between the disruption and the failure to perform. Articles 1244 and 1245 of the Indonesian Civil Code (KUHPerdata) provide the principal legal basis for determining the exemption from liability for damages arising from non-performance.

Technological disruption may be qualified as *force majeure* where it occurs beyond the affected party's reasonable control, could not reasonably have been anticipated or prevented, is not attributable to its fault or negligence, and directly prevents or materially impedes contractual performance. Conversely, where the disruption results from

inadequate maintenance, insufficient security measures, negligence, or other risks that could reasonably have been controlled or prevented, the failure to perform may constitute **wanprestasi**. The involvement of a third-party technology provider does not automatically establish force majeure; its effect must also be assessed based on the allocation of risk and the circumstances of the disruption.

Where technological disruption qualifies as force majeure, its primary legal consequence is the limitation or exemption from liability for damages, rather than the automatic termination of the agreement. Depending on whether the impediment is temporary or permanent, the parties may postpone or extend performance, or consider termination or contractual adjustment where performance is no longer possible.

Therefore, the distinction between force majeure and wanprestasi in electronic agreements ultimately depends on risk attribution and causation. Clear force majeure clauses addressing technological disruptions, notification, mitigation, and the consequences of interrupted performance are necessary to provide greater legal certainty and contractual balance in the digital era.

REFERENCES

- Abigail, A. D., Tyas, D. A., Setyawan, F., & Amrullah, M. A. (2025). Legal liability for *force majeure* in digital crypto asset contracts reviewed from the perspective of legal rationality in the digital age. *Academia Open*, 10(2). <https://doi.org/10.21070/acopen.10.2025.12855>
- Kamilah, A., Kusworo, F. R. A., May, N. S., & Lestari, R. D. (2025). Doktrin *force majeure* dalam hukum perikatan: Implikasi terhadap kontrak bisnis di era digital. *Indonesian Journal of Law and Justice*, 2(4), 1–11.
- Khairandy, R. (2005). Force majeure dalam hukum kontrak. *Jurnal Hukum*, 8(2).
- Khilmi, F. M., & Triana, N. (2025). *Force majeure* dalam sistem hukum Indonesia. *Iqtishaduna: Jurnal Ilmiah Mahasiswa Hukum Ekonomi Syariah*, 7(1), 403–414.
- Labibah, H. A., Damayanti, M., Lestari, A. A., Setiawan, G. N. R., & Ningsih, Y. P. (2026). Legal implications of internet service disruptions on late payment penalties in digital consumer transactions. *Journal of Development Research*, 10(1), 15–22. <https://doi.org/10.28926/jdr.v10i1.513>

- Marhaeni, I. A. V., & Priyanto, I. M. D. (2023). Penyelesaian sengketa wanprestasi apabila para pihak tidak mencantumkan klausul *force majeure* dalam perjanjian. *Kertha Negara: Journal Ilmu Hukum*, 11(2), 127–137.
- Putri, A. N. B., Karamoy, A. A., Dian, Y., Zibran, M., & Siswajanthi, F. (2026). Wanprestasi pada era digital: Tanggung jawab hukum dalam perjanjian berbasis elektronik. *RIGGS: Journal of Artificial Intelligence and Digital Business*, 5(2), 186–193. <https://doi.org/10.31004/riggs.v5i2.8346>
- Sepriadi, O., Zulfikar, P., Al Ghifari, S., Budi, U., & Ridwan. (2026). Hubungan hukum kontrak elektronik dengan keamanan transaksi digital. *Berajah Journal*, 6(3), 867–873. <https://doi.org/10.47353/bj.v6i3.534>
- Sidauruk, A. D., Purba, B., Karo-Karo, J. K., Siregar, S. A., & Yani, T. (2024). Analisis hukum atas perjanjian bisnis dalam era digital. *INNOVATIVE: Journal of Social Science Research*, 4(3), 16608–16616.
- Sinaga, I. P. A. S., Mahat, C. S., & Simarmata, G. M. (2023). Dinamika perjanjian kontrak elektronik dalam bisnis digital: Analisis komparatif dan implikasi hukum. *Ekasakti Jurnal Penelitian dan Pengabdian*, 4(1), 148–156.
- Tai, E. T. T. (2018). Force majeure and excuses in smart contracts. *European Review of Private Law*, 26(6), 787–804. <https://doi.org/10.54648/ERPL2018055>
- Tampoli, I. A. (2021). Tinjauan yuridis pembebasan ganti rugi dengan alasan keadaan memaksa (*force majeure*) ditinjau dari KUHPerdota. *Lex Privatum*, 9(12).
- Tori, Q. H. M., & Tedjomurti, K. (2021). Pemberlakuan *force majeure* akibat pandemi Covid-19 dalam kontrak kerja konstruksi. *Jurnal Privat Law*.
- Widiyaningsih, D., Sanusi, Pratama, E. A., & Mahardika, D. (2025). Dampak yuridis implementasi *smart contract* terhadap prinsip-prinsip hukum perjanjian dalam perspektif hukum perdata Indonesia. *Private Law Journal*, 3(2).
- Peraturan Perundang-undangan
Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.