

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

BEYOND PANDEMICS: RETHINKING FORCE MAJEURE AND CONTRACTUAL LIABILITY IN THE FACE OF CYBERATTACKS AND AI-DRIVEN DISRUPTIONS

AUTHORED BY - JAIMOL THOMAS

Jaimol Thomas, Assistant Professor,
CSI College for Legal Studies, Kanakkary, Kottayam, Kerala.

CO-AUTHOR - RAMSI M

Ramsi M., LL.M Scholar
CSI College for Legal Studies, Kanakkary, Kottayam, Kerala.

ABSTRACT

Contracts are formed upon the underlying notion that parties entering into them will voluntarily assume reciprocal obligations in accordance with the terms and conditions agreed between them. Commercial transactions, however, remain susceptible to events occurring after the formation of a contract that may prevent, hinder, delay, or fundamentally alter anticipated contractual performance. Contract law consequently recognises mechanisms through which the consequences of extraordinary events may be apportioned between contracting parties. Force majeure represents one of the cardinal contractual mechanisms for confronting such circumstances. Traditionally associated with natural disasters, war, epidemics, governmental restrictions and other events beyond the control of contracting parties, its application has largely developed around physical and external disruptions.

The escalating digitalization of commercial activities, however, has put forth a new dimension to contractual disruption. Cyberattacks, ransomware, distributed denial-of-service attacks, cloud-service failures and data breaches may substantially interfere with contractual performance. Simultaneously, the growing assimilation of artificial intelligence into commercial operations creates further uncertainty where erroneous outputs, autonomous decisions or system failures result in contractual non-performance. These developments raise a pivotal question: Are conventional force majeure principles sufficiently equipped to allocate contractual risk arising from technologically induced disruptions? Neither cyberattacks nor AI-driven disruptions should automatically qualify as force majeure events; rather, their legal

consequences must be determined through the contractual allocation of risk, foreseeability, control, causation, reasonable preventive measures, and mitigation. A technologically informed approach therefore requires contractual provisions addressing cybersecurity obligations, technological dependencies, AI oversight, notification, business continuity, and mitigation. The future of force majeure consequently lies not in indiscriminately expanding the category of excusable events, but in developing a risk-based framework capable of allocating technological disruption with greater precision.

Keywords: Force Majeure; Contractual Liability; Cyberattacks; Artificial Intelligence; Cybersecurity; Risk Allocation; Commercial Contracts; Frustration; Technology Law.

I. INTRODUCTION

Contracts are formed upon the underlying notion that parties entering into them will voluntarily assume reciprocal obligations as per the terms and conditions agreed between them. Commercial transactions, on the other hand, are susceptible to events occurring after the formation of a contract which may prevent, hinder, delay, or fundamentally alter the anticipated performance of the contract itself. As an aftermath of such circumstances, contract law recognises mechanisms through which the consequences of extraordinary events may be apportioned between contracting parties.

The concept of force majeure derives from the French Civil Code. Under French law, it applies regardless of whether it is expressly stated in the contract. That is not the case under English law where it does not have a settled meaning and therefore it is a matter of contractual language.¹ An event of force majeure is an occurrence that happens outside the control of a party. The purpose of a force majeure clause is often to provide relief to one party if a force majeure event occurs and affects their performance of their contractual obligations. As otherwise, that party would have to rely on the common law doctrine of frustration that only applies in limited circumstances where performance is impossible which is a high threshold to meet. Force majeure represents one of the cardinal contractual mechanisms for confronting such a state of affairs. The expression generally connotes events beyond the control of the affected party that prevent or substantially interfere with contractual performance. Its vitality

¹ Elizabeth Burton & Alan Hunt, Digital, Commerce & Creative 101: Force Majeure, Lewis Silkin (Oct. 28, 2024), "<https://www.lewissilkin.com/insights/2024/10/28/digital-commerce-creative-101-force-majeure>" (<https://reference-url-citation.invalid/0>).

lies not merely in excusing non-performance, but in apportioning contractual risk before an unforeseen event actually occurs.

Historically, commercial disruption was predominantly conceived through physical events such as floods, earthquakes, wars, epidemics, governmental prohibitions and industrial disturbances. The COVID-19 pandemic provided a contemporary illustration of how an extraordinary event can affect contractual relationships across different industries and jurisdictions. Yet the commercial landscape that has emerged alongside and after the pandemic presents a further challenge as the possibility of contractual performance being disrupted without any corresponding physical destruction. Modern commerce increasingly operates through digital infrastructure. Nowadays banking, logistics, e-commerce, financial services, healthcare, manufacturing, communication and supply-chain management greatly depend upon interconnected technological systems. A ransomware attack may make critical data inaccessible; a distributed denial-of-service attack may render an online platform unavailable; and a failure of cloud infrastructure may prevent a service provider from fulfilling its contractual obligations.

Artificial intelligence augments an additional layer of complexity. Since AI systems are extensively used for inventory management, financial analysis, customer interaction, software development, fraud detection and automated decision-making, when such systems generate erroneous outputs or make unexpected decisions that contribute to contractual non-performance, the question of attribution becomes particularly difficult. The crucial issue, therefore, is not merely whether technology can cause contractual disruption. It is whether such disruption should transfer contractual risk from the party controlling or deploying the technology to the counterparty. This article argues that conventional force majeure principles remain capable of addressing technological disruptions, but only if they are interpreted and drafted through a more nuanced, risk-based approach.

II. FORCE MAJEURE IN THE DIGITAL COMMERCIAL ENVIRONMENT

Force majeure is traditionally rooted in civil law systems but now widely adopted across common law jurisdictions through express contractual terms. Unlike traditional contracts, technology agreements often involve ongoing service obligations, making the stakes of a force majeure event particularly high. As courts increasingly scrutinise force majeure claims in the

technology sector, parties must draft with precision, carefully defining excusable events, allocating risk, and setting clear notification and mitigation requirements.² For a force majeure event to excuse performance, the event must generally be unforeseeable, external to the parties, and make performance impossible, impracticable, or radically different from what was agreed.

Importantly, force majeure does not automatically discharge a party from its obligations; relief depends on the precise wording of the contract, the causal link between the event and the non-performance, and the party's compliance with any notice and mitigation requirements set out in the clause. In technology contracts, where continuity of service and reliability are paramount, force majeure provisions must be carefully drafted to balance commercial expectations with genuine risk allocation, ensuring that the clause offers protection without creating loopholes for avoidable failures.³ Its operation ordinarily depends upon the language agreed by the contracting parties. The occurrence of an extraordinary event, by itself, does not necessarily establish a right to contractual relief. Three considerations become particularly significant in technological disputes.

- I) First, whether the event falls within the contractual language must be examined. A clause expressly covering cyberattacks may produce a different result from a clause limited to conventional events such as natural disasters and war.
- II) Secondly, the affected party must ordinarily demonstrate a sufficient relationship between the event and the failure of performance. A cyberattack occurring within an organisation does not necessarily establish that every subsequent contractual default was caused by that attack.
- III) Thirdly, the affected party's own conduct becomes relevant. If reasonable measures could have substantially prevented or mitigated the consequences of the event, the argument that the resulting non-performance was entirely beyond its control becomes more difficult.

This is particularly paramount because nowadays technological risks are increasingly foreseeable. Cyberattacks are no longer purely hypothetical occurrences for digitally dependent businesses. Consequently, the legal analysis should not be reduced to the question of whether

² Princess Judith Allotey & Emmanuel Saah, Downtime and Disasters: Force Majeure Clauses in Technology Contracts, Mondaq (May 26, 2025), "<https://www.mondaq.com/contracts-and-commercial-law/1628758/downtime-and-disasters-force-majeure-clauses-in-technology-contracts>" (<https://reference-url-citation.invalid/0>).

³ Allotey & Saah, *supra* note [2]

the attack was caused by a third party. It should also consider whether the affected party reasonably managed the risk before the event occurred.

III. CYBERATTACKS: FORCE MAJEURE OR FORESEEABLE COMMERCIAL RISK?

Cyberattacks occupy an unusual position within force majeure analysis. On one hand, the attack is generally initiated by an external actor and is therefore not voluntarily caused by the affected party. On the other hand, the possibility of cyber intrusion is widely recognised as a commercial risk requiring preventive measures. Let us consider two situations. In the first, a company maintains updated security systems, appropriate access controls, regular backups and incident-response mechanisms. Despite these precautions, it becomes the victim of a sophisticated and previously unknown cyberattack that temporarily prevents it from accessing its essential systems. In the second case, another company continues using obsolete software despite known vulnerabilities, fails to implement basic security measures and subsequently suffers a ransomware attack that prevents it from performing its contractual obligations. Although both situations involve ransomware, their contractual implications need not be identical. The first presents a stronger basis for arguing that the disruption arose from an external event despite reasonable precautions. The second raises a more difficult question concerning whether the resulting non-performance was substantially connected to the affected party's own failure to exercise reasonable care. This distinction demonstrates why the occurrence of a cyberattack should not automatically determine the availability of force majeure protection.

This analysis may further be understood through the Hand Formula, articulated in *United States v. Carroll Towing Co.*,⁴ which evaluates the reasonableness of precautions by weighing their burden against the probability and gravity of potential harm. Although developed in the context of negligence, the formula offers a useful analytical perspective for assessing cybersecurity precautions and the allocation of technological risks in contractual relationships.

At the same time, sophisticated attacks, particularly those attributed to state actors, can be entirely outside a company's ability to predict or prevent. The scale of disruption caused by incidents like ransomware or critical infrastructure attacks can render contractual performance genuinely impossible. Some modern contracts are beginning to explicitly include cyberattacks

⁴ *United States v. Carroll Towing Co.*, 159 F.2d 169, 173 (2d Cir. 1947).

in their force majeure clauses, a growing acknowledgment of digital risk. On the other hand, cyber risk is now widely known and anticipated. Courts may hold that businesses are expected to have adequate cybersecurity measures in place. If the attack resulted from negligence or insufficient security protocols, a force majeure defence is unlikely to succeed. Many force majeure clauses do not explicitly list cyberattacks and courts are generally reluctant to expand the doctrine beyond what is contractually specified. Whether a cyberattack qualifies as force majeure often comes down to how the contract is written. Broadly worded clauses that cover "any event beyond reasonable control" may be interpreted to include digital disruptions. Narrowly defined clauses that list specific events without reference to technology or cyber incidents will likely leave a business without protection. Businesses that address cyber risk expressly within their contractual agreements are far better positioned to assert or defend against force majeure claims in the event of a digital disruption.

IV. THE PROBLEM OF AI-DRIVEN CONTRACTUAL DISRUPTION

Artificial intelligence creates a different form of contractual uncertainty because it may operate as an integral component of the performance process itself. Suppose a business uses an AI-powered inventory system to determine supply requirements and the system produces an erroneous prediction, causing the business to fail to deliver goods within the contractual period. Alternatively, an AI-powered financial system may generate an erroneous instruction resulting in a payment failure. Should such failures be regarded as force majeure? The answer should not depend merely upon the fact that an algorithm produced the immediate error. Unlike an earthquake or natural disaster, an AI system is ordinarily introduced into a commercial operation by a human or organisation. It is selected, configured, trained, monitored and maintained within a particular technological environment.

The integration of artificial intelligence into contractual operations presents a further doctrinal conundrum concerning the attribution of liability when technological errors or autonomous decisions result in non-performance. The uncertainty surrounding responsibility for such disruptions raises questions as to whether liability should rest with the party deploying the technology, its developer, or another entity involved in its operation. These difficulties further complicate the application of conventional contractual principles to AI-driven disruptions.⁵

⁵ Abanti Bose, The Doctrinal Issues Faced by AI Contracting, iPleaders (Aug. 13, 2021), <https://blog.ipleaders.in/doctrinal-issues-faced-ai-contracting/>.

Where a party voluntarily incorporates AI into its contractual performance, it is difficult to regard every unexpected output as an external force beyond its control. This does not mean that the party deploying AI must necessarily bear every resulting loss. AI systems may depend upon external cloud infrastructure, software providers, telecommunications networks and other technological dependencies. A failure originating from an external technological provider may therefore require a different assessment from an error caused by inadequate testing, defective configuration or absence of reasonable human oversight. The distinction may consequently be drawn between AI as an external technological dependency and AI as a voluntarily assumed component of contractual performance. This distinction provides a more appropriate basis for determining contractual responsibility than treating AI malfunction as an automatic force majeure event.

V. FORESEEABILITY, CONTROL AND MITIGATION

The concepts of foreseeability, control and mitigation acquire renewed importance and interpretation when contractual disruption is technologically induced. Because the existing interpretations are not at all adequate so as to address the changing need and complexities in the tech-driven commercial environment.

A. Foreseeability

Foreseeability should not be assessed in the abstract sense. The nature and extent of technological risk may vary according to the industry, nature of the information processed, technological dependence and sophistication of the contracting parties. A financial institution, cloud-service provider and small commercial enterprise may not reasonably face identical expectations concerning cybersecurity and technological resilience. Therefore, the relevant inquiry should be whether the particular disruption was reasonably foreseeable in the context of the contractual relationship and the technological environment in which the parties operated.

B. Control and Preventability

Foreseeability does not necessarily mean preventability. Cyberattacks may remain possible despite substantial security measures, and no technological system can guarantee absolute immunity from attack. The more appropriate inquiry is whether the affected party adopted reasonable and proportionate safeguards in view of the risk involved. Similarly, where AI is employed, consideration should be given to whether the deploying party exercised reasonable oversight, testing and monitoring before relying upon the system for contractual performance.

C. Mitigation

The invocation of force majeure should not operate as an unrestricted escape from contractual responsibility. The affected party should ordinarily take reasonable steps to minimise the consequences of the disruptive event. In cyber incidents, this may include activating backup systems, isolating compromised networks, restoring data, engaging incident-response professionals and notifying the contractual counterparty. In AI-related disruptions, mitigation may include human intervention, suspension of automated decision-making, alternative methods of performance and correction of erroneous outputs. Thus, the response to the technological event may be as significant as the event itself.

VI. THE INDIAN LEGAL POSITION

The Indian Contract Act, 1872 provides the principal statutory framework within which contractual performance and impossibility are examined. Section 32 concerns contingent contracts, while section 56 addresses agreements to do impossible acts and subsequent impossibility or unlawfulness. Where parties expressly incorporate a force majeure clause, the contractual language assumes particular importance. The Supreme Court has recognised the distinction between contractual force majeure and frustration under section 56. In *Energy Watchdog v. Central Electricity Regulatory Commission and Others*⁶, the Supreme Court examined the relationship between contractual force majeure and section 56, emphasising the importance of the contractual allocation of risk. Similarly, *Satyabrata Ghose v. Mugneeram Bangur & Co*⁷ remains an important authority concerning impossibility and frustration under Indian contract law. The pandemic-era decision in *M/s Halliburton Offshore Services Inc. v. Vedanta Ltd. & Anr*⁸ further illustrates the importance of examining the contractual provision, causal connection and conduct of the party invoking force majeure rather than treating an extraordinary event as automatically determinative. These principles can be extended cautiously to technological disruptions. A party invoking force majeure because of a cyberattack should establish not merely the existence of the attack but its connection with the inability to perform. Likewise, an AI-related failure should not automatically amount to impossibility where alternative means of performance remain reasonably available. The existing Indian framework can therefore accommodate technological disruption to an extent, although it does not presently provide a technology-specific contractual framework for

⁶ (2017) 14 SCC 80

⁷ AIR 1954 SC 44

⁸ 2020 DHC 1999

allocating such risks.

VII. TOWARDS A RISK-BASED FORCE MAJEURE FRAMEWORK

The central limitation of conventional force majeure clauses is that they are frequently event-oriented rather than risk-oriented. Traditional clauses may enumerate events such as war, natural disasters, epidemics, governmental action and other circumstances beyond reasonable control. Such drafting may be inadequate where performance depends upon complex digital systems and multiple technological service providers. A contemporary approach should instead ask a list of questions such as; Who controlled the relevant risk, whether the risk could reasonably have been mitigated, whether the event actually caused the non-performance, and how the parties allocated that risk through their contract? This approach allows a distinction between two technologically similar events that may have different contractual consequences. An external cyberattack against a business that maintained reasonable security measures may potentially justify contractual relief. Conversely, an attack substantially facilitated by the business's failure to address known vulnerabilities may warrant a different conclusion. Likewise, an AI failure resulting from the collapse of an independent cloud provider may differ materially from an erroneous output caused by inadequate testing or human oversight. The appropriate approach is therefore not to classify technology itself as force majeure but to evaluate the technological risk through the principles of contractual allocation, causation, control and mitigation.

VIII. RETHINKING CONTRACTUAL DRAFTING FOR THE DIGITAL AGE

The increasing technological dependence of commercial transactions requires greater specificity in contractual drafting. First, contracts should expressly address cybersecurity events, including ransomware, significant system intrusions, denial-of-service attacks and other incidents capable of materially affecting performance. Secondly, contracts should address third-party technological dependencies. Where performance depends upon cloud-service providers, payment processors, telecommunications providers or AI providers, the parties should clarify the circumstances in which their failure may constitute a force majeure event. Thirdly, contracts involving AI should address human oversight and responsibility. The parties should identify who bears responsibility for monitoring, intervention and alternative performance when an AI system produces an unexpected result. Fourthly, notification and

mitigation obligations should be expressly defined. Prompt communication can enable the unaffected party to take alternative commercial measures and may prevent an initially temporary disruption from developing into a more serious contractual dispute. Finally, contracts should incorporate appropriate business-continuity mechanisms, including alternative systems, backup arrangements and substitute methods of performance where commercially feasible. Such drafting would enable parties to anticipate technological disruption instead of attempting to fit emerging risks into contractual language designed primarily for physical events.

IX. CONCLUSION

Force majeure remains an important mechanism for allocating the consequences of extraordinary contractual disruption. However, the nature of extraordinary events has evolved. In a technologically dependent commercial environment, a business may remain physically intact while being rendered incapable of performance by ransomware, cloud-service failure, a data breach or an AI-related malfunction. The appropriate response is not to automatically expand the category of force majeure to encompass every cyberattack or AI failure. Such an approach would risk converting technological uncertainty into an unrestricted contractual escape. Instead, the analysis should focus upon contractual language, causation, control, foreseeability, reasonable preventive measures, attribution and mitigation. A cyberattack originating from an external actor despite reasonable cybersecurity measures may present a materially different contractual situation from an attack facilitated by the affected party's failure to maintain basic safeguards. Similarly, an AI failure resulting from an external technological dependency may differ from a failure arising from inadequate testing, configuration or human oversight. The future of force majeure should therefore move from an event-based approach towards a risk-based approach. Contracts must increasingly anticipate technological dependencies at the drafting stage and clearly allocate responsibility for cybersecurity, AI deployment, technological service interruptions, notification, mitigation and business continuity. Such an approach would allow force majeure to retain its traditional function while making it responsive to the realities of contemporary commerce. Ultimately, the question in a technologically disrupted contract should not simply be "Did an extraordinary technological event occur?" The more meaningful question is "Who was best positioned to anticipate, control, mitigate and bear the risk of that event under the contract?" That shift from identifying extraordinary events to allocating technological risk may provide the more sustainable foundation for contractual liability in the digital age.