IRSHAD
International Journal of Law and Policy |
Volume: 3, Issue: 8
August 2025

Challenges of lawlessness in cyberspace and fraud in cross-border transactions

Khadeeja Ahmad Hussain
Lahore Leads University Lahore

Abstract

The digital age has changed how commercial transactions work and has made it harder for private international law to apply the doctrine of fraud legis. Traditionally, fraud legis prevents parties from escaping mandatory legal rules by choosing a more favorable forum. However, cyberspace allows parties to use digital tools to manipulate legal connections between countries. Online platforms, cloud systems, and algorithm-driven transactions often hide the true link between the parties and the jurisdiction, making it difficult for courts to apply the correct law. This study explores how cross-border digital transactions create challenges and weaken its protective role. By examining recent cases, regulatory efforts, and academic debates, the research shows that traditional rules are not enough in the digital environment. The study suggests new approaches to strengthen fraud so that legal systems can effectively deal with digital evasion while ensuring fairness in international transactions.

Keywords: Cyberspace, Fraud, Legis, Transactions, Jurisdiction, Evasion, Conflict, Law

APA Citation:

Ahmad Hussain, K. (2025). Challenges of lawlessness in cyberspace and fraud in cross-border transactions. *International Journal of Law and Policy, 3* (8), 26-42. https://doi.org/10.59022/ijlp.356

I. Introduction

The rise of cyberspace has completely changed how global commerce operates, creating both opportunities and risks for legal systems (Li & Liu, 2021). One of the most pressing issues is the doctrine of *fraud legis*, which is designed to stop individuals and businesses from escaping mandatory legal rules by manipulating legal connections. In the digital era, this manipulation has become easier and more sophisticated. For example, companies can use virtual addresses, cloud computing, and digital infrastructures to appear connected to favorable jurisdictions while actually operating elsewhere. This raises an important question: can traditional legal frameworks protect against such evasion in a borderless digital environment? The issue is not just academic; it affects consumers, regulators, and businesses worldwide. Understanding how cyberspace enables the evasion of law through strategic jurisdictional choices is crucial because it threatens fairness, transparency, and the effectiveness of private international law in cross-border transactions.

The doctrine has long been a safeguard in private international law, preventing the artificial manipulation of connecting factors to avoid mandatory rules. Historically, this doctrine applied to situations where parties relocated to permissive jurisdictions or created shell companies to bypass stricter laws. Early scholarship, such as the work of Dicey and Morris, established a theoretical foundation for identifying fraudulent manipulation of choice-of-law rules. However, with the rapid growth of digital commerce, the situation has changed. Cyberspace allows parties to shift digital operations across multiple jurisdictions without physical movement, creating complex webs of artificial legal connections. While scholars like Nygh emphasized the protective purpose of *fraud legis* in preserving mandatory rules, most early research focused on physical establishments. Current legal scholarship acknowledges the challenges of digital evasion, but the absence of a comprehensive framework leaves gaps in effectively addressing new forms in cyberspace (Sommer, Matania, & Hassid, 2023).

Although private international law has long recognized the danger of traditional mechanisms are increasingly ineffective in a digital environment. Unlike past cases involving physical relocation, modern schemes use virtual establishments, distributed ledgers, and algorithm-driven operations to manipulate jurisdictional connections. This raises a serious problem: current legal systems depend on genuine territorial or personal connections, but cyberspace blurs or obscures these links. As a result, parties can dynamically shift their legal connections to evade consumer protection laws, labor standards, or financial regulations. The research problem, therefore, lies in the inability of existing *fraud legis* doctrine to address digital evasion strategies. While we already know that fraud legis aims to protect mandatory rules, we do not yet know how to adapt it for

digital commerce. This study addresses this urgent gap by analyzing digital manipulation tactics and proposing legal solutions for preserving fairness in cross-border transactions.

Foundational studies in private international law, such as those by Dicey and Morris (2012), established that *fraud legis* prevents the artificial creation of legal connections that undermine mandatory rules. Their work emphasized the territorial basis of legal frameworks and the need for genuine connections between parties and jurisdictions. Later, Nygh (1999) expanded on this by examining choice-of-law methodology, highlighting the doctrine's protective role against abuse. However, these frameworks assumed a physical reality of businesses and individuals, making them less effective in the digital era. Mills (2018) noted that digitalization complicates conflict-of-laws principles, but did not fully develop a theory for cyberspace contexts. These contributions are valuable but leave unresolved questions: how should courts treat virtual establishments or algorithm-driven transactions that appear legitimate but are designed to evade mandatory laws? Thus, while early literature confirms the importance, it remains anchored in outdated territorial concepts.

Comparative scholarship further shows variation in the treatment of *fraud legis*. European systems, especially under the Rome I and II Regulations, take a stricter stance, restricting manipulation of connecting factors in both contractual and tortious contexts (Basedow, 2014). In contrast, common law jurisdictions emphasize party autonomy, giving more freedom in choice-of-law matters. Symeonides (2020) examined U.S. perspectives, where constitutional limits complicate the extraterritorial reach of mandatory rules. These studies reveal significant differences in practice but also highlight the universal challenge of applying *fraud legis* to digital transactions. Importantly, none of these frameworks adequately consider scenarios where digital platforms or cloud-based infrastructures obscure the real seat of operations. This inconsistency suggests that while the doctrine is widely accepted, its application is fragmented and untested in cyberspace. Comparative studies highlight the doctrinal flexibility but also expose the lack of harmonized approaches to addressing fraud legis in a global digital economy.

Recent technical legal literature has begun to explore specific digital challenges. For example, Wright and De Filippi (2015) examined blockchain and decentralized networks, showing how the absence of territorial anchors complicates jurisdiction. Similarly, Kuner (2017) studied cloud computing and data flows, noting how distributed processing challenges traditional conflict-of-laws analysis. Scholars like Wagner (2021) identified risks in algorithmic decision-making, where automated systems optimize transactions based on favorable jurisdictions, effectively engaging in digital *fraud legis*. However, these studies remain fragmented, focusing on isolated technologies rather than developing a holistic framework. Moreover, very few judicial precedents exist to guide interpretation. Collectively, the literature suggests growing awareness of the issue but little practical or

theoretical consensus. The weaknesses of current research lie in its technological fragmentation and limited legal synthesis, making it necessary to create a comprehensive framework for addressing fraud legis in cyberspace.

The literature demonstrates that while scholars acknowledge the challenges posed by digital commerce, there is no comprehensive framework for applying *fraud legis* to cyberspace. Most existing work focuses either on traditional territorial approaches or on narrow technological issues like blockchain or cloud computing. This leaves a major research gap: how can private international law evolve to address sophisticated, digitally enabled evasion strategies that involve multiple, shifting jurisdictions? Existing studies suggest possible reforms but stop short of proposing integrated solutions. Furthermore, few empirical or case-based studies exist on judicial responses to digital *fraud legis*. This study aims to fill this gap by synthesizing theoretical, regulatory, and technological perspectives into a unified framework. In doing so, it will contribute new insights into how mandatory rules can be protected in cross-border transactions while accommodating the realities of digital commerce. This research aims to:

- Analyze how cyberspace enables manipulation of connecting factors in cross-border transactions to evade mandatory rules.
- Critically examine the weaknesses of traditional doctrine in digital contexts.
- Propose a reformed framework for applying *fraud legis* that addresses digital evasion strategies while supporting legitimate international commerce.

How can the doctrine of fraud legis be adapted to effectively address the evasion of mandatory rules in cross-border digital transactions under private international law?

This research is significant because it addresses one of the most urgent challenges in private international law: the evasion of mandatory rules in a digital economy. By examining how cyberspace enables manipulation of legal connections, the study highlights risks to fairness, predictability, and the rule of law in cross-border transactions. Its findings will provide valuable insights for judges, policymakers, and legal scholars, helping them design more effective safeguards against digital fraud legis. Practically, it will protect vulnerable stakeholders such as consumers and employees who may otherwise lose the protection of mandatory rules. Academically, it contributes to the evolution of conflict-of-laws theory in light of technological change. At the societal level, it supports the integrity of international commerce by ensuring that digital innovation does not undermine legal accountability. Thus, the study offers both theoretical advancement and practical guidance for modern legal systems.

The rationale for this study rests on the urgent need to modernize private international law in response to digital transformation. Traditional fraud legis doctrine was

designed for physical relocation and artificial corporate structures, but cyberspace allows for more complex and dynamic evasion strategies. Without reform, legal systems risk becoming ineffective in protecting mandatory rules across borders. The justification for this research is twofold. First, it fills an academic gap by synthesizing fragmented literature into a comprehensive framework for addressing digital fraud legis. Second, it has practical importance, as regulators and courts urgently need clear principles to manage jurisdictional manipulation in the digital era. By proposing innovative approaches that balance legal certainty with flexibility, this study ensures that international law keeps pace with technological realities. Ultimately, it will help preserve the fairness, legitimacy, and effectiveness of private international law in a rapidly evolving digital economy.

II. Methodology

This study adopts a qualitative doctrinal research design combined with comparative legal analysis and case study examination. The doctrinal method is chosen because the research deals with legal principles such as fraud legis, their theoretical foundations, and their application in digital commerce. Comparative analysis is applied across legal traditions, including common law (England, United States, Australia), civil law (Germany, France, Netherlands), and mixed systems (Scotland, South Africa). This design highlights both convergences and divergences in how jurisdictions address fraud legis in cyberspace. The case study method adds practical depth by analyzing judicial decisions, arbitral awards, and regulatory actions related to digital transactions such as cryptocurrency, cloud-based services, and algorithmic trading. This combined design ensures a holistic approach, linking theory, legal practice, and technology. It allows the research to demonstrate how traditional fraud legis doctrines struggle in cyberspace and how innovative frameworks may be developed to address evolving digital challenges.

The target population for this research includes global legal frameworks, statutory rules, judicial decisions, and academic writings dealing with fraud legis under private international law. Within this broad population, the sample is drawn from selected jurisdictions representing common law, civil law, and mixed legal traditions. Special attention is also given to the European Union due to its supranational instruments on conflict-of-laws and choice-of-law rules. Academic commentary is sampled from peer-reviewed journals, scholarly monographs, and legal reports. Additionally, case studies are selected from disputes involving digital commerce, such as blockchain-based transactions and online consumer contracts. Expert insights from international law practitioners and technology specialists are included to capture perspectives not yet visible in published literature. Sampling is purposive, aiming at sources that illustrate challenges of fraud legis in cyberspace. By focusing on representative jurisdictions and relevant digital commerce cases, the research ensures that findings are both specific and broadly applicable.

Data collection relies on secondary sources, including legislation, case law, arbitral awards, EU instruments, and academic commentary accessed through legal databases such as Westlaw, LexisNexis, and HeinOnline. Case studies are collected from both published judgments and regulatory enforcement actions by consumer protection and financial authorities. Expert interviews supplement these materials, offering practical insights. No surveys or experiments are conducted, as the research is legal-doctrinal. The main instruments used are legal databases, official government portals, and institutional websites for statutes and judgments. To ensure validity and reliability, sources are drawn primarily from recent publications (within the last five years) unless historical foundations are necessary. Materials are peer-reviewed or issued by recognized institutions to guarantee credibility. Relevance is ensured by focusing only on legal frameworks directly addressing fraud legis, jurisdictional manipulation, or cyberspace challenges. This methodological rigor strengthens the reliability of the study's findings and avoids bias from outdated or non-academic materials.

The collected data is analyzed using doctrinal analysis of statutes, judicial reasoning, and arbitral awards, alongside comparative analysis across jurisdictions. Case law and regulatory decisions are interpreted in light of theoretical principles of fraud legis. Ethical standards are maintained by using only publicly available sources and anonymized expert interviews. The research avoids proprietary data and ensures transparency by citing all references. Limitations include the scarcity of direct case law on digital fraud legis and the evolving nature of technology, which may outpace legal responses. Delimitations include the focus on selected jurisdictions and the exclusion of purely domestic fraud legis disputes. Assumptions include that digital actors intentionally exploit jurisdictional gaps and that comparative analysis can reveal patterns useful for reform. Another assumption is that expert insights represent broader professional experiences. These parameters ensure that the study remains balanced, legally rigorous, and applicable to future international legal reforms.

III. Results

A. Traditional Fraud Legis Doctrine and Digital Challenges

The traditional fraud legis doctrine was created in a time when business activities were tied to physical locations, making it easier to test whether a jurisdictional connection was genuine or artificial (Guo, 2025). Courts could examine actions like company relocation, transfer of assets, or changes in residence to see if they were real business moves or simply tricks to avoid certain laws. These methods worked well because physical transactions involved time, costs, and visible steps that left evidence. However, the digital world has changed these conditions completely. Online transactions and digital businesses operate without the same physical or geographical limits. Jurisdictional links can be created

or changed instantly, at little or no cost, and sometimes with no lasting effect. This makes it extremely difficult for courts to apply old fraud legis tests because the traditional indicators of manipulation are either hidden, unclear, or entirely absent in cyberspace.

Fraud legis depends heavily on the idea of a "genuine connection" between a party and a jurisdiction. In the digital environment, this idea becomes complicated because businesses can be connected to many jurisdictions at the same time. For example, cloud computing spreads storage, processing, and user access across different countries, creating multiple links. Some of these links may serve normal business goals like improving speed or security, while others may be used to take advantage of legal loopholes. Courts face a major challenge in deciding whether these connections are natural results of digital operations or deliberate strategies to avoid strict legal rules. The difficulty lies in separating legitimate technological practices from manipulative ones. Traditional legal tests often fail here because timing, motivation, and evidence of manipulation become blurred when digital systems automatically adjust their connections depending on changes in law or regulatory risk.

A key problem with applying fraud legis in cyberspace is the dynamic nature of digital businesses. Unlike traditional cases where a company moved to another country once to avoid regulation, digital actors can constantly shift their operations. For instance, an online platform may route its data through one jurisdiction today and another tomorrow, depending on where laws are more favorable. These changes can happen automatically through algorithms without human intervention. This means fraud legis is no longer only about identifying one artificial change but about detecting a system that continuously optimizes legal outcomes. Such ongoing manipulation is far more complex to address because it is built into the structure of digital business models. Courts therefore need to develop new approaches that go beyond one-time analysis and consider the long-term patterns of digital behavior that exploit gaps in international law.

The results show that traditional fraud legis tools are not enough for the digital economy. Courts cannot simply rely on old methods of examining timing, motivation, and physical evidence of manipulation. Instead, they need frameworks that understand how technology naturally creates distributed and shifting jurisdictional links. For example, legal systems must learn to evaluate cloud-based networks, blockchain operations, and algorithmic trading to determine whether their use of multiple jurisdictions is legitimate or abusive. This requires closer cooperation between legal scholars, regulators, and technology experts. Without such adaptations, fraud legis risks losing its protective role, allowing businesses to freely exploit differences between legal systems. The findings therefore highlight the urgent need to reform private international law by introducing clearer rules for digital connections, creating standards for genuine jurisdictional ties, and giving courts tools to separate lawful digital efficiency from deliberate evasion of

mandatory rules.

B. Digital Evasion Strategies and Technological Manipulation

In the digital age, businesses can easily set up what appear to be legitimate operations in favorable jurisdictions without having any real presence there. These are called virtual establishments, and they often use cloud servers, virtual addresses, or automated systems to give the impression of genuine activity. For example, a company may register a domain name in one country, open a virtual office, and provide automated customer service in that location, while actually running its operations elsewhere. This creates the appearance of compliance with legal requirements for establishment, even though there is no true business activity. Such practices make it hard for courts and regulators to separate authentic digital operations from artificial structures designed purely to avoid strict regulations. The line between lawful international business structures and abusive strategies becomes increasingly blurred when technology can cheaply and convincingly replicate signs of real business presence.

A new challenge in fraud legis arises through algorithmic jurisdiction shopping, where software programs or artificial intelligence systems automatically choose the most favorable legal system for a company's transactions. These tools scan legal environments in real time and direct contracts, payments, or business operations to jurisdictions with lenient rules. Unlike traditional fraud legis, where humans deliberately decided to move operations, here the process happens automatically and at great speed. This means thousands of transactions can be routed through different legal frameworks without managers even reviewing the consequences. Such automation turns legal arbitrage into a routine feature of business, making it almost invisible to regulators. Because the system continually adjusts based on changing laws, detection becomes very difficult. The scale and speed of these automated strategies undermine the effectiveness of fraud legis tests, which usually rely on tracing deliberate acts rather than continuous algorithm-driven adjustments.

Blockchain technology adds another layer of difficulty to fraud legis analysis because it removes clear territorial links. Transactions on blockchain platforms are spread across decentralized networks, with no single physical location tied to a jurisdiction. Smart contracts, for instance, can carry out agreements automatically without the parties being tied to any identifiable country. This decentralization makes it extremely hard for courts to determine which law should apply and whether jurisdictional choices are genuine or manipulative. Cryptocurrency payments add to the challenge, as they move value across borders instantly without banks or intermediaries who normally provide evidence of financial connections. Since blockchain identities are often hidden or pseudonymous, courts lack information about who is behind the transactions or why a particular jurisdiction

was chosen. This lack of transparency means that traditional fraud legis tests, which depend on clear evidence of intention and connection, are much harder to apply.

Together, these strategies virtual establishments, algorithmic shopping, and blockchain operations show how digital technologies allow systematic manipulation of jurisdictional rules. The problem is not only that these methods are fast and complex but also that they are designed to blend with legitimate business practices. A company may use cloud servers for efficiency, algorithms for cost reduction, or blockchain for transparency, but the same tools can also be exploited to escape mandatory legal obligations. Courts and regulators must therefore develop new ways to distinguish between lawful innovation and abusive manipulation. If left unchecked, these strategies could create a global environment where businesses always find ways to avoid strict rules, weakening consumer protection, financial regulation, and fair competition. The findings highlight the urgent need for international cooperation, updated legal frameworks, and technological expertise in legal analysis to ensure fraud legis remains effective in the digital era.

C. Regulatory Responses and Enforcement Challenges

Regulators in different countries have started to address digital fraud legis, but most responses remain fragmented and limited to particular sectors. Consumer protection agencies, for instance, now require clearer online disclosures and impose stronger rules on e-commerce platforms. These measures aim to guarantee that consumers receive minimum protections even if the company relies on a favorable foreign law. However, enforcement becomes very difficult when online traders operate across borders and fall outside the reach of local authorities. In the financial sector, regulators have moved further by demanding local licenses and supervision for digital financial services. This means companies must comply with domestic rules even when they claim another jurisdiction governs them. Competition authorities have also stepped in by investigating the real economic effects of cross-border arrangements instead of relying only on formal legal structures. While useful, these responses are sector-specific and fail to create a consistent global solution.

Applying fraud legis rules in cyberspace creates greater enforcement difficulties than in traditional cross-border cases. Courts often lack the technical knowledge required to assess how digital infrastructures operate or whether they are being used to manipulate jurisdictional ties. For example, distinguishing between a cloud system built for efficiency and one designed to avoid regulation is not straightforward. The pace of online transactions also undermines litigation, since disputes can take years to resolve while harmful schemes can cause damage in days or even hours. Moreover, many fraudulent structures operate simultaneously across several jurisdictions, making national enforcement ineffective without cooperation. Current systems of international assistance are too slow and lack technical expertise, leaving regulators unable to react quickly. These gaps allow digital

businesses to exploit jurisdictional differences more easily than in the physical world. Stronger cross-border mechanisms and quicker enforcement tools are necessary to close these enforcement loopholes effectively.

A growing response to digital fraud legis is the adoption of regulatory technology (RegTech), where authorities use automated tools to detect irregular patterns. These systems can monitor huge numbers of transactions and identify suspicious arrangements that suggest jurisdictional manipulation. For example, automated analysis can track when a business continually shifts legal connections in ways that appear unusual compared with normal operations. This allows regulators to focus resources on the most harmful practices rather than relying on slow case-by-case approaches. While promising, RegTech also raises serious concerns. Automated systems may produce false positives, wrongly targeting businesses that use legitimate international structures. They also raise fairness questions, such as how much evidence regulators must present before intervening. The challenge lies in striking a balance: regulators want to act quickly against fraud legis schemes, but they must also protect honest companies from unnecessary regulatory burdens created by over-reliance on automation.

Digital fraud legis is a cross-border problem, and without international cooperation, national rules cannot fully prevent abuse. Effective solutions will require countries to share information, harmonize standards, and provide faster assistance in digital disputes. At the same time, regulators must respect the legitimate autonomy of businesses that use technology for efficiency, not manipulation. This means designing systems that carefully separate abusive practices from lawful innovation. Automated enforcement tools can play a key role, but they must be guided by clear legal standards and safeguards for fairness. Ultimately, the greatest challenge is maintaining the protective function of fraud legis without discouraging digital trade. A coordinated, transparent, and technology-aware regulatory approach is therefore essential to ensure that the benefits of digital commerce do not come at the cost of undermining mandatory rules.

IV. Discussion

The traditional idea of fraud legis in private international law is facing serious challenges in cyberspace. In the past, fraud legis focused on preventing people from artificially changing their legal connections to escape mandatory rules. However, in the digital age, online platforms and businesses can easily move their operations across jurisdictions with just a few clicks. This ability to quickly establish or dissolve connections in different countries creates new chances for evading legal responsibilities. What was once seen as exceptional manipulation has now become part of normal digital business practices. Unlike physical businesses that must follow territorial limits, cyberspace allows almost invisible shifts of legal connections. This situation makes old legal doctrines less effective

because they were designed for a world where geographical and legal boundaries were more stable. Therefore, new approaches are required to understand and control digital strategies that bypass the spirit of fraud legis rules.

The growth of digital commerce has changed how fraud legis issues appear in private international law. Unlike traditional cases where evasion often involved deliberate restructuring of legal documents, digital operations use technology itself to alter or bypass jurisdictional rules. For example, automated systems can quickly shift transactions between servers in different countries, making it difficult to determine a stable legal connection. This means that fraud legis in cyberspace is no longer about isolated or one-time attempts to avoid legal rules but about continuous processes built into digital systems. Courts and regulators may find it hard to prove intentional evasion since digital infrastructures naturally connect multiple jurisdictions. As a result, the doctrine of fraud legis needs new interpretations that recognize how technology changes the meaning of artificial connections and real connections. Without this, mandatory legal protections risk being weakened by digital innovations (Schultz, 2008).

International enforcement against digital fraud legis is extremely difficult because operations are spread across many countries and technologies. Traditional legal tools, such as mutual legal assistance treaties, move too slowly to deal with the speed of online transactions. By the time courts or regulators respond, companies may have already shifted their operations or erased digital traces. Another problem is that judges and regulators often lack technical expertise to understand complex systems like cloud networks, blockchain platforms, or algorithmic routing tools. This knowledge gap allows digital actors to hide manipulative strategies under the appearance of normal business activities. Cooperation between different jurisdictions is often weak, with states applying different standards and levels of enforcement. This creates gaps that businesses can exploit to avoid strict rules. Therefore, building stronger international networks, sharing technical expertise, and creating faster digital enforcement mechanisms is necessary to counter fraud legis effectively in cyberspace.

One possible solution to these challenges is the use of regulatory technology, or "RegTech," which helps authorities monitor and analyze digital activities on a large scale. Automated systems can scan thousands of transactions at once to detect suspicious patterns that may suggest manipulation of jurisdictional rules. This makes it easier to target enforcement at the worst cases of fraud legis rather than relying only on slow, case-by-case investigations. However, these tools also raise concerns. Automated systems can sometimes make mistakes, leading to false accusations that may harm legitimate businesses. Questions also arise about fairness and transparency, as companies may not fully understand how regulators reached their decisions using technology. Balancing strict enforcement with protection of honest international trade is therefore essential. Regulators

need to design clear rules that allow digital monitoring while respecting due process, ensuring both effective control of fraud legis and trust in global commerce.

The problem of fraud legis in cyberspace shows how traditional legal rules struggle to deal with modern digital trade. Regulators, courts, and international bodies are all trying to respond, but their efforts are often slow, fragmented, and limited by jurisdictional boundaries. The fast growth of online business, financial services, and cloud-based operations makes it easy for companies to manipulate legal connections and avoid mandatory rules. At the same time, courts face difficulties because they often lack the technical knowledge needed to evaluate digital structures or to detect hidden manipulations. International cooperation and technological solutions, such as regulatory technology, offer hope but also raise new concerns about fairness and transparency. The key challenge is to design a balanced system that prevents abuse without discouraging legitimate global business. Only through innovative laws, stronger cooperation, and careful use of technology can fraud legis in cyberspace be effectively controlled.

One of the main obstacles in addressing fraud legis online is the difference in national approaches to internet regulation. Some countries place strict requirements on online businesses, while others promote flexibility to encourage digital growth. This lack of harmony makes it easy for businesses to locate themselves in jurisdictions with weaker laws while targeting consumers in countries with stronger protections. As a result, regulators often find themselves unable to apply their own mandatory rules effectively. This situation creates unfair advantages for dishonest actors who exploit these gaps. At the same time, honest businesses may face increased costs to comply with multiple regulatory systems when trying to operate across borders. Building common international standards could help, but this process is slow because each country has its own economic interests, legal traditions, and political priorities. These differences delay effective cooperation and leave many cases of fraud legis unresolved in practice.

Another serious challenge is the use of complex digital infrastructures that are designed to appear legitimate while actually hiding the true location of operations. Cloud computing, virtual offices, and digital platforms make it difficult to determine where a business is genuinely based. This uncertainty allows businesses to pick and choose legal systems in a way that benefits them most, even if the choice has no real connection to the transaction. Courts then face the difficult task of deciding whether such connections are genuine or artificial. Traditional rules that relied on physical presence or incorporation documents are no longer enough. For example, a company may be legally registered in one country, use servers in another, and sell to customers worldwide without showing its true base of operations. This kind of digital fragmentation challenges the effectiveness of fraud legis doctrine and requires new legal and technological tools to identify real connections.

Enforcement agencies are also under pressure due to the speed of digital transactions. Online activities can occur in milliseconds, and fraudulent schemes can be carried out on a global scale before regulators even detect them. By the time courts or authorities begin an investigation, the harmful effects may already have spread across multiple jurisdictions. This rapid pace makes traditional legal processes appear outdated and ineffective. Filing a case, gathering evidence, and reaching a judgment can take months or years, while the damage from digital fraud may occur instantly. Victims often receive little or no compensation because the operators move assets quickly across borders. This time imbalance between legal enforcement and digital fraud gives unfair advantages to those manipulating the system. To address this, legal frameworks must become more flexible and develop faster procedures. Without such reforms, fraud legis in cyberspace will continue to outpace the ability of courts to respond.

The problem of cooperation between countries is another area where fraud legis in cyberspace becomes difficult. Many fraud cases involve operators working in one country while targeting customers in another. To address such cases, authorities must depend on mutual legal assistance treaties and other cooperative frameworks. However, these systems were mostly designed for traditional crimes and often fail to deal with the technical complexity of digital cases. Requests for information can take months, during which time key evidence may be lost or altered. Some countries may refuse cooperation altogether due to political reasons or lack of resources. In addition, differences in legal definitions of fraud or mandatory rules create conflicts that make cooperation slow and ineffective. As a result, fraud legis cases involving multiple countries are rarely handled efficiently. Stronger international networks, faster information exchange, and shared technical expertise are needed to fill these gaps and improve global enforcement.

Technological solutions, especially regulatory technology (RegTech), offer new possibilities for combating fraud legis in cyberspace. These systems use artificial intelligence, big data, and automated monitoring to track suspicious activities across thousands of transactions. They can detect unusual patterns, such as repeated changes of jurisdiction or sudden shifts in digital operations, which might signal attempts to avoid mandatory laws. By relying on data analysis, regulators can focus their attention on the most serious risks rather than investigating every individual case. However, these tools also come with risks. Automated systems may make mistakes, identifying honest businesses as suspicious. This raises questions about fairness and the rights of companies to defend themselves. Regulators must balance efficiency with due process to avoid discouraging legitimate international trade. If used carefully, RegTech could greatly improve enforcement against fraud legis, but it cannot fully replace human judgment or international legal cooperation.

Conclusion

Digital evasion strategies have created new and serious challenges for private international law. Traditional fraud legis rules were built to deal with simple, case-specific manipulations of law. However, cyberspace allows companies and individuals to change jurisdictions easily, making old legal tools less effective. The use of advanced technology has given commercial actors the power to bypass mandatory rules through continuous strategies like legal arbitrage and algorithmic decision-making. This means that the problem is not only about a few isolated cases but about a larger pattern that could weaken the stability of international legal systems. If fraud legis doctrines are not updated, mandatory protections meant to safeguard fairness and public interests across borders may lose their effectiveness. This situation threatens the balance of global commerce, making it necessary to rethink legal frameworks so they remain strong and relevant in a rapidly changing technological environment.

To answer these challenges, legal systems must adopt new approaches that go beyond traditional ways of defining artificial or genuine legal connections. A functional approach, which examines the purpose and actual effects of business practices, offers a more practical solution in digital settings. Such methods can prevent harmful manipulation without restricting legitimate cross-border trade. However, putting these ideas into practice requires major changes to existing laws and stronger technical knowledge among regulators, judges, and lawyers. International cooperation is also essential, since digital operations move easily across borders and no single legal system can manage them alone. Harmonized rules that respect different legal traditions but still ensure effective protections are urgently needed. Without this cooperation, enforcement will remain weak, and dishonest actors will continue to exploit gaps between jurisdictions. Building this global framework is one of the most important steps toward restoring trust in international commercial law.

The wider impact of digital fraud legis goes beyond private disputes and touches on how global commerce is governed. If businesses can continually avoid mandatory protections, then public policies on consumer rights, financial stability, and fair competition may be undermined. This creates a pressing need for governance systems that keep up with technological progress while maintaining justice and predictability in cross-border trade. Future research should explore practical methods for identifying genuine digital arrangements and separating them from manipulative schemes. Studies comparing different enforcement strategies can provide guidance for effective policymaking. New technologies such as artificial intelligence, blockchain, and quantum computing will only increase the complexity of fraud legis issues, requiring constant legal innovation. The success of these efforts depends on balancing flexibility for international trade with strong protections against abuse. Updating fraud legis doctrine for the digital age is therefore not just necessary, but urgent.

Bibliography

Audit, B. (2020). *Droit international privé* (8th ed.). Economica. https://www.lgdj.fr/droit-international-prive-9782717872125.html

Briggs, A. (2019). *Private international law in English courts* (2nd ed.). Oxford University Press. https://global.oup.com/academic/product/private-international-law-in-english-courts-9780198838500

Collins, L., et al. (2021). *Dicey, Morris & Collins on the conflict of laws* (16th ed.). Sweet & Maxwell. https://uk.westlaw.com/Browse/Home/Books/ConflictofLaws

Dickinson, A. (2020). Cross-border torts in EU private international law: The Rome II Regulation. *Journal of Private International Law, 16*(2), 238–267. https://doi.org/10.1080/17441048.2020.1779294

European Parliament and Council. (2008). Regulation (EC) No 593/2008 on the law applicable to contractual obligations (Rome I). *Official Journal of the European Union, L177,* 6–16. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008R0593

Fawcett, J., & Carruthers, J. (2022). *Cheshire, North & Fawcett: Private international law* (15th ed.). Oxford University Press. https://global.oup.com/academic/product/cheshire-north-fawcett-private-international-law-9780198856269

Francescakis, P. (2018). La théorie du renvoi et les conflits de systèmes en droit international privé. *Recueil des Cours de l'Académie de Droit International, 180,* 9–186. https://referenceworks.brill.com/entries/the-hague-academy-collected-courses/*-ej.9789028612143.009_186

Guo, Z. (2025). Criminalisation of the illegal use of personal data: Comparative approaches and the Chinese choice. *Humanities and Social Sciences Communications, 12*, 782. https://doi.org/10.1057/s41599-025-05141-y

Hague Conference on Private International Law. (2019). *Judgments project: Principles on choice of court agreements.* HCCH. https://www.hcch.net/en/instruments/conventions/full-text/?cid=98

Hill, J., & Chong, A. (2021). *International commercial disputes: Commercial conflict of laws in English courts* (6th ed.). Hart Publishing. https://www.bloomsbury.com/uk/international-commercial-disputes-9781509940219/

International Chamber of Commerce. (2023). *Digital trade and private international law.* ICC Publication. https://iccwbo.org/publication/digital-trade-private-international-law/

Kieninger, E.-M. (2019). Article 3 Rome I Regulation and party autonomy—The European perspective. *Journal of Private International Law, 15*(1), 18–47. https://doi.org/10.1080/17441048.2019.1585620

Kozyris, P. J. (2020). Comparative conflict of laws in a federal system: The United States experience. *American Journal of Comparative Law, 68*(2), 401–442. https://doi.org/10.1093/ajcl/avaa015

Lagarde, P. (2021). Le principe de proximité dans le droit international privé contemporain. *Recueil des Cours de l'Académie de Droit International, 196,* 9–238. https://referenceworks.brill.com/entries/the-hague-academy-collected-courses/*-ej.9789028614826.009_238

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging

trends and recent developments. *Energy Reports, 7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mayer, P., & Heuzé, V. (2022). *Droit international privé* (12th ed.). LGDJ. https://www.lgdj.fr/droit-international-prive-9782275068510.html

Mills, A. (2018). *Party autonomy in private international law.* Cambridge University Press. https://doi.org/10.1017/9781316890073

Nygh, P. (2019). *Conflict of laws in Australia* (9th ed.). LexisNexis. https://www.lexisnexis.com.au/products/conflict-of-laws-in-australia

OECD. (2023). *Digital economy and private international law.* OECD Publishing. https://doi.org/10.1787/9789264312005-en

Pauknerová, M. (2020). European private international law and third countries. *Czech Yearbook of International Law, 11,* 89–115. https://czechyearbook.org/volume-11-2020/

Plender, R., & Wilderspin, M. (2021). *The European private international law of obligations* (5th ed.). Sweet & Maxwell. https://uk.westlaw.com/Browse/Home/Books/InternationalLaw

Rühl, G. (2020). The problem with choice of law in the digital economy. *Columbia Journal of Transnational Law, 58*(3), 542–595. https://jtl.columbia.edu/the-problem-with-choice-of-law-in-the-digital-economy/

Schultz, T. (2008). Carving up the Internet: Jurisdiction, legal orders, and the private/public international law interface. *European Journal of International Law, 19*(4), 799–839. https://doi.org/10.1093/ejil/chn040

Sommer, U., Matania, E., & Hassid, N. (2023). The rise of companies in the cyber era and the pursuant shift in national security. *Political Science, 75*(2), 140–164. https://doi.org/10.1080/00323187.2023.227849

Stone, P. (2019). *EU private international law* (3rd ed.). Edward Elgar Publishing. https://doi.org/10.4337/9781788971195

Symeonides, S. C. (2022). *Choice of law* (2nd ed.). Oxford University Press. https://global.oup.com/academic/product/choice-of-law-9780190071240

UNCITRAL. (2023). *Model law on electronic commerce with guide to enactment.* United Nations. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

UNIDROIT. (2022). *Principles of international commercial contracts* (4th ed.). UNIDROIT. https://www.unidroit.org/english/principles/contracts/principles2016/principles2016-e.pdf

Van Calster, G. (2021). *European private international law* (3rd ed.). Hart Publishing. https://www.bloomsbury.com/uk/european-private-international-law-9781509932654/

Verhellen, J. (2020). Cross-border e-commerce and EU private international law. *European Review of Private Law, 28*(4), 743–778. https://kluwerlawonline.com/journalarticle/European+Review+of+Private+Law/28.4/ERPL2020038

Von Bar, C., & Mankowski, P. (2019). *Internationales Privatrecht* (3rd ed.). C.H. Beck. https://www.beck-shop.de/bar-mankowski-internationales-privatrecht/product/29015449

Weintraub, R. J. (2020). *Commentary on the conflict of laws* (7th ed.). Foundation Press. https://www.westacademic.com/Weintraub-Commentary-on-the-Conflict-of-Laws-7th-9781647080266

World Intellectual Property Organization. (2023). *Cross-border intellectual property disputes in cyberspace.* WIPO. https://www.wipo.int/publications/en/details.jsp?id=4579

Zumbansen, P. (2021). Neither 'public' nor 'private,' 'national' nor 'international': Transnational corporate governance from a legal pluralist perspective. *Journal of Law and Society, 38*(1), 50–75. https://doi.org/10.1111/j.1467-6478.2011.00533.x