

# International Conflict of Laws Governing Civil Liability Arising from Digital Commercial Transactions in Cyberspace

Taqi Faisal Alsayid Majali<sup>1</sup>, Osama Emad Jamil Jraie<sup>2</sup>, Taqwa Faris Mohammad Alsarayreh<sup>3</sup>, Mohammad Suheel Ali Hayajneh<sup>4</sup>, Ruba Mohammad Hmaidan<sup>5</sup>

<sup>1</sup> Independent Researcher. Email: tuqamajali91@gmail.com

<sup>2</sup> Independent Researcher. Email: osamaemad434@gmail.com

<sup>3</sup> Independent Researcher. Email: taqwasar631@gmail.com

<sup>4</sup> Independent Researcher. Email: hayajnehdrmmohammad@gmail.com

<sup>5</sup> Assistant Professor of Private Law, Faculty of Law, Applied Science Private University, Amman, Jordan. Email: r\_hmaidan@asu.edu.jo

## Corresponding Author:

Taqi Faisal Alsayid Majali<sup>1\*</sup> (tuqamajali91@gmail.com)

**Abstract:** This research looks at conflict of laws as it relates to civil liability in digital commercial transactions in cyberspace and the problems of jurisdiction, applicable law and enforcement across borders. The study examines the new challenges for traditional private international law, based on territorial principles, in borderless and decentralized digital environments. Commercial interactions over the internet are increasingly happening in more than one forum at the same time, resulting in legal uncertainty over forum selection, determination of applicable law and liability allocation.

The study uses doctrinal legal research method together with a comparative legal approach to explore and examine relevant international legal principles, judicial interpretations, and scholarly contributions. Analyses and challenges the reactions of courts and legal systems to cyber-related conflicts, such as Internet torts, platform liability, smart contracts, and cross-border consumer transactions. The research also examines recent developments like targeting tests, effects-based jurisdiction and digital platforms in the formation of private legal relations.

The research shows that existing laws are fragmented and inconsistent, resulting in complexity, enforcement issues and legal uncertainty in the realm of digital commerce. The study ends by calling for greater harmonization and technological sophistication of the conflict-of-laws rules, to better protect the realities of cyberspace. It suggests flexible jurisdictional rules and more cooperation between States to provide legal security and robust cross-border governance of digital commerce....

**Keywords:** Conflict of laws; Private international law; Cyberspace; Digital commercial transactions; Jurisdiction; Applicable law; Civil liability; Cross-border disputes; Internet torts; E-commerce; Platform liability; Smart contracts; Digital governance; Transnational regulation.

## INTRODUCTION

The world of digital commercial transactions has dramatically changed the nature of the classic private international law issues including jurisdiction and law applicable to the transaction. Cyberspace is a borderless and decentralized space, which presents a challenge to traditional systems that are based on the classical principles of territorial conflicts of laws. Legal relationships are not restricted to geographical areas anymore; they are formed in a transnational way in the digital sphere through multiple legal systems.

Lukings and Habibi Lashkari (2022) provide a broad overview on the topic of conflict of law in the wider area of cyber security law and data sovereignty. They argue that legal governance of digital space is becoming more important, and that sovereignty is no longer only territorial, but is now concerned with data flows and the digital infrastructure. This is an innovation that poses fresh issues as to jurisdiction and applicable law in trans-border e-disputes

Similarly, Svantesson (2021) is critical on the private international law and its limitations in the context of the internet and its 'physical presence' and 'territorial location' customary connecting factors. Svantesson asserts that the principles of jurisdictions in cyberspace need to be rethought, given the worldwide reach and real-time nature of Internet activity. This perspective emphasizes the need to establish a more flexible and effective mechanism of laws to resolve the conflict-of-laws problems in the digital arena.

Besides, Basedow (2024) places digital trade in the context of the private law aspect of global trade and investment governance. His work is focused on the private law organisation of international economic relations, particularly in the space of the digital economy, which is less studied. Basedow's analysis further strengthens the notion that the field of private international law is more than a technical one, but a core element of the architecture of global regulatory rules for transborder commerce.

The contributions together present a conceptual framework for grasping the impact that cyberspace has on traditional paradigms of jurisdiction and conflict of laws and for reevaluating existing legal structures in the context of civil liability in digital commercial transactions.

## Literature Review

The existing literature on private international law and cyberspace also shows the increasing amount of scholarly work that has been devoted to the legal issues and challenges brought about by digitalisation, including the question of jurisdiction, which law applies, and civil liability. Though there has been much progress, there is still lack of coordination, doctrinal confusion and fragmentation in the field.

In the settlement of conflicts in international commerce, the role and relevance of private international law is analyzed and discussed by Harahap (2025). The study reveals the applicability of the traditional principles, but also demonstrates that the strategies are increasingly being used on the noses of platforms and digital transactions without borders.

Razmetaeva et al. (2021) address the jurisdictional challenges in the digital era, such as the main structural issues, such as overlapping jurisdictional claims and the issues of localization of online harm. In this work they bring attention to the apparent contradiction between territorial sovereignty and the globalization of digital technologies and to the divergent judicial decisions.

Elijah (2025) brings a fresh viewpoint by examining how jurisdiction works in civil cases in the context of an increasingly digital world. The study emphasizes the need to develop doctrine to address cross-border digital disputes, particularly in the context of courts becoming more aware that they are called upon to adjust their current jurisdiction principles to digital environments.

Melnik (2022) examines the trends in the unification of jurisdictional approaches in Internet matters, and considers the development of a harmonized national and international internet dispute regime. But the study also points out that this unification is not complete, not uniform, across jurisdictions, which reduces the usefulness of this unification in practice.

Wojciech (2025) considers Internet jurisdiction in both the common law and EU regulatory systems and shows that there is considerable variation in the approaches of these legal systems to disputes on the Internet. This comparative analysis reveals the lack of uniformity of the international picture of jurisdiction in cyberspace.

Das (2024) discusses the evolution of liability in the digital sphere, and how the concept of cyber torts plays a role in the broader law. The study uncovers the weaknesses of the current principles of tort law in order to address the multifaceted character of cyber harms, particularly in regard to

causation and attribution. Table 1 below provides a comparative overview of important studies on private international law and cyberspace.

**Table 1: Comparative Overview of Key Studies on Private International Law and Cyberspace**

| Author                   | Focus Area                                           | Key Contribution                             | Identified Limitation                           |
|--------------------------|------------------------------------------------------|----------------------------------------------|-------------------------------------------------|
| Harahap (2025)           | PIL in global business transactions                  | Relevance of PIL in digital trade emphasized | Inadequate attention to platform-related issues |
| Razmetaeva et al. (2021) | Jurisdiction in digital age                          | Overlapping jurisdictional claims identified | No solutions for enforcement issues             |
| Elijah (2025)            | Jurisdiction for civil litigation in the digital era | Call for rethinking of jurisdiction doctrine | Theoretical foundations only                    |
| Melnik (2022)            | Harmonization of jurisdiction rules                  | Harmonization tendencies highlighted         | Incomplete global standardization               |
| Wojciech (2025)          | EU and common law jurisdiction                       | Analysis of comparative legal systems        | Lack of uniformity in regulation                |
| Das (2024)               | Cyber-tort liability                                 | Cyber torts examined                         | Application of tort law difficulties            |

This body of literature indicates that a lot of developments had taken place in the area of scholarly research in relation to legal issues in the context of cyberspace; however, a distinct absence of a comprehensive theoretical framework for dealing with issues of jurisdiction and liability is evident.

### 3. Research Methodology

This literature shows that there was much progress in academic research concerning legal issues in cyberspace, but there is a clear lack of a coherent and unified framework which could cover issues of jurisdiction, applicable law and civil liability for digital commercial transactions.

## Research Methodology

The methodology applied to this study is the doctrinal legal research methodology which is the main analytical approach supported by comparative legal approach to analyze the complexities of conflict of laws in civil liability in digital commercial transactions in cyberspace. The doctrinal method is best suited for this research type, since it involves the interpretation, analysis and synthesis of legal rules, principles and judicial reasoning, based on primary law sources, including treaties, laws and judgments. In this context, doctrinal analysis can help to critically explore how private international law deals with jurisdictional fragmentation and legal uncertainty in a cross-border digital context particularly in circumstances where territorial connecting factors have become less relevant.

The above-mentioned doctrinal aspect is supported by methodological observations made by Giacalone and Giacalone (2024), who assert that the private international law field in the era of digitization requires an interpretation model which can adapt to the new technologies in classical interpretation process.. They highlight the need for methodologically open-minded approaches for solving new legal challenges for the digital world, notably concerning the transfer of data across borders, contractual relations online, and ambiguity in the digital space. In this study, doctrinal reasoning is not only used as a descriptive tool, but also as a critical tool to assess the adequacy of the current conflict-of-laws rules to resolve digital commercial conflicts.

The study not only examines the doctrinal aspects of the question, but also uses a comparative legal framework to identify differences and similarities between several legal systems in the areas of

jurisdiction and applicable law in cyberspace-related disputes. The comparative approach is crucial for understanding the various conceptions of responsibility, territorial relations and means of enforcement in digital commerce across jurisdictions. This way, private international law can be assessed, across a structured framework, in terms of its legal pluralism, and the level of fragmentation in practice of the harmonisation efforts can be revealed.

The comparative perspective is taken on the basis of that comparative analysis, which Okoli and Yekini (2023) also stress in understanding the implied jurisdiction agreement and the overall contractual autonomy of the parties to an international commercial contract. Their contribution shows that the allocation of jurisdiction in e-transactions is increasingly taking place on the basis of private ordering processes, such as the clauses of choice of court and choice of law found in online platforms. The current study, thus, takes this view and investigates the comparative approach by looking at how party autonomy and consumer protection and regulatory sovereignty are achieved in the digital economy.

In addition, the analytical approach used in this research combines the interpretation of the doctrine and comparative evaluation to build a consistent concept about civil liability apportionment in cross-border e-transactions. The current state of play in the regulation of cyberspace is analysed using primary legal sources, such as international instruments, scholarly commentary and judicial interpretations, looking for gaps, inconsistencies and trends in the regulation of cyberspace. This joint methodological approach seeks to contribute to the ongoing debate on the modernisation of private international law in the digital era in a statistically significant manner, while at the same time providing a legally informed but analytically sound analysis of the conflict-of-laws issues that arise in the digital commercial sphere.

#### **4. Jurisdictional Challenges in Cyberspace**

The jurisdictional issues that arise in cyberspace are one of the most complicated aspects of the current private international law, largely because interactions in the cyber world are borderless and the application of territorial based doctrines to virtual conduct is complicated. Jurisdictional concepts and principles, based on physical presence, territorial nexus and predictable connecting factors, are being increasingly challenged when dealing with online commercial transactions, cross-border data transfers, and tortious conduct facilitated by digital means. Courts and legal systems, therefore, are constantly confronted with uncertainty as to which forum is applicable, which law, and whether the judgements are enforceable, in respect of internet-related disputes.

Terentyeva (2021) refers to the concept of jurisdiction in cyberspace which has evolved from territorial jurisdiction to a more elastic one, such as minimum contacts and minimum effects tests, in the U.S. legal system. The change shows the general conflict between the old laws of jurisdiction and the architecture of digital communications networks which have no borders and may have harmful effects in more than one jurisdiction at the same time, leading to overlapping claims of jurisdiction.

Similarly, Okoli (2022) investigates the conflict of laws principles with the backdrop of internet torts, noting that even beyond territoriality other factors such as policy and security have been influential in the application of the conflict of laws principles. This is an emerging judicial preference in favor of regulatory efficiency and injury avoidance in cases involving disputes in the online world, especially those involving commerce and multi-jurisdictional online platforms.

In *The Conceptualisation of Jurisdiction in Networked Societies* (2021), Kohl mirrors this conceptual underpinning of jurisdiction in networked societies, which she describes as a novel concept influenced by the decentralisation of technologies and regulatory power. The internet is a networked system where classical jurisdictional anchors have been undermined, which means new models of interpretation are needed to accommodate the nature of the internet as a networked system, rather than one that functions based on place, says Kohl.

With a more general approach, Ryngaert (2023) contextualizes jurisdictional conflicts in the broader framework of international law on extraterritoriality, and introduces the reader to the various means by which States have expanded their territorial control over activities and acts conducted in a globalized digital space. Alongside this expansion comes a number of tensions between sovereignty

and legal security, and between the overlapping regulation, particularly in the area of cross-border e-commerce and digital consumer protection.

Brachotte and Nuyts (2023) examine jurisdiction over cyber torts under the Brussels I bis Regulation in the European legal context, charting the current challenges of locating harmful events in an online context. Their analysis shows that while the regulation contains the rules that are structured by jurisdiction, the extent of its application in cyberspace is open to debate as digital harm is multi-location and diffuse in nature.

The aforementioned, Verma et al. (2024), also discuss the subject by analyzing the conflicts between jurisdictions in the era of artificial intelligence, which adds an additional layer of complexity to the typical allocation of jurisdictions. Lacking human oversight, the use of AI systems can lead to legal consequences in different jurisdictions, adding to the issue of jurisdiction and regulatory control. The uncertainty of jurisdiction and regulatory framework only intensifies when AI systems can create legal implications without human involvement. But when AI systems can draw out legal implications without human involvement, it adds to the uncertainty of jurisdiction and regulatory framework..

Finally, Knapp (2022) looks at jurisdictional issues in IP matters involving cross-border disputes, including online copyright infringement, and introduces the idea that such digital dissemination of protected IP content poses a threat to the traditional territorial rights enforcement approach. The ease with which infringement of material can be achieved throughout the world makes it difficult to identify one forum that would be suitable for action, and often multiple actions are taken and different results obtained.

**Table 2: Jurisdictional Problems in Cyberspace and Legal Responses**

| Jurisdictional Issue                           | Description                                                   | Legal Response / Approach                       | Key Limitation                  |
|------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------|---------------------------------|
| <b>Territoriality vs digital presence</b>      | Difficulty applying physical territorial rules to online acts | Effects doctrine / minimum contacts test        | Lack of uniform global standard |
| <b>Cross-border internet torts</b>             | Harm occurs in multiple jurisdictions simultaneously          | Forum selection and flexible jurisdiction tests | Risk of parallel litigation     |
| <b>Extraterritorial jurisdiction expansion</b> | States extending laws beyond borders                          | Regulatory extraterritorial frameworks          | Sovereignty conflicts           |
| <b>Cyber tort jurisdiction under EU law</b>    | Determining place of harmful event online                     | Brussels I bis Regulation framework             | Ambiguity in "place of damage"  |
| <b>AI-driven cross-border harm</b>             | Automated systems generating multi-jurisdictional effects     | Emerging AI governance proposals                | Regulatory fragmentation        |
| <b>Online IP infringement</b>                  | Global dissemination of copyrighted content                   | Injunctions and geo-blocking                    | Enforcement limitations         |

This integrated analysis shows that with the exception of some of the specific practical issues surrounding jurisdictional claims in cyberspace, it is essential to recognize that there is a larger shift in the structure of legal authority in the digital age.

## 5. Applicable Law in Digital Commercial Transactions

The issue of the applicable law within digital commercial transactions forms one of the main aspects of private international law, especially in cyberspace where the digital contractual relations and harmful events extend outside of territorial boundaries. Digital commerce is different to border crossing trade, in that it is conducted using a 'platform' that provides a means of instant communication between multiple jurisdictions and jurisdictions, making the determination of one jurisdiction's law to govern a transaction much more difficult.

This complexity has posed essential issues on the autonomy of the party, the protection of the consumer, the sovereignty of the regulators and predictability of the law in online transactions. The "targeting activity test" in internet-based consumer contracts is one of the crucial points in this debate that is addressed by Chen (2023). Because the applicable law is now becoming more and more a matter of intent, Chen makes the point that it is becoming essential to find out whether a commercial operator has intentionally targeted its activities at a particular jurisdiction. This will involve departing from a territorial focus on connecting factors to more functional and "conduct" based factors which will better fit the realities of digital markets. But, Chen notes, much of the lack of clarity rests with what counts as "targeting" - especially when it comes to passive websites, or algorithmic marketing.

In a different area, Kunda considers the choice-of-law and choice-of-court clauses included in digital consumer contracts, and highlights the importance of the standard terms drafted by platforms and their increasing influence on the choice of applicable law. Kunda illustrates how these clauses ensure legal certainty and efficiency in transactions, but at the same time have a detrimental effect on weaker parties, such as consumers, who have less access to favourable jurisdictions. The balance shows the general tension that exists between contract autonomy and the principles of consumer protection that are required in PIR. Coyle, Dodge and Simowitz (2022) offer an empirical and doctrinal analysis of the developments in choice of law in American courts and explain why the law is becoming more and more fractured when it comes to cross-border digital disputes. They find, however, that in many cases the two different approaches (the traditional territorial approach and the present interest-based/policy-approach) conflict and result in different outcomes. This can result in uncertainty in electronic commerce, and will contribute to the necessity of having more harmonised principles concerning conflict of laws.

Manne and Harper (2024) recommend a new method of resolving the choice of law question in data privacy and digital regulation in their policy paper to prevent this "fragmentation" of state laws. Their work highlighted inefficiencies in digital regulation and the need for a great deal of coordination in terms of how rules are set, how cross-border digital transactions are regulated, and how effective the regulations are. In addition, technological evolution makes it more difficult to determine the application of the law, especially in novel digital landscapes, like the metaverse. Meliala and Putra (2024) explore the extent to which tacit choice of law applies in interactions that take place in the metaverse, and find that virtual spaces introduce new connecting factors that pose doubt on the applicability of the old ones.

They contend that legal systems need to gain new interpretative powers to accommodate the new contexts of decentralization and immersion that are digital, and that are constituted through virtual identities, not physical ones. Asensio (2024) offers a thorough discussion of conflict of laws in internet-based transactions, focussing on the structures of the traditional private international law frameworks.

The plethora of linkages in cyberspace causes a lack of legal clarity, forum-shopping and divergent judicial thinking, asensio points out. It is for this reason, he says, that his vision is to create a more holistic and technologically-savvy conflict-of-laws system designed to deal with the evolving landscape of e-commerce. This analysis shows that the dominant territorial approach to applicable law in digital commercial transactions is no longer the only approach, but rather a hybrid and increasingly fractured approach that tries to balance the expectations of parties in a contract, regulatory interests and technological realities.

## 6. Civil Liability in Cross-Border Digital Commerce

Civil liability for cross-border digital commerce is a fundamental substantive aspect of private international law, which deals with the legal ramifications of harmful digital acts of cross-border nature. This is a complex area due to the interplay between the contractual obligations, tortious liability, platform-based intermediation and new digital technology like smart contracts and decentralised systems. In this highly complex landscape, the definition, extent and apportionment of civil responsibility can be difficult in the face of the many actors, and jurisdictions, at play. Hassanah and Aprilianti (2024) discuss the transformation of civil liability as the principle and doctrine of civil liability as it is known is adapting due to the new digital environment.

They believe the liability frameworks are evolving from bilateral contractual ones to those with more complex and multi-layered structures including those of intermediaries, service providers and end-users. It marks an overall change in the doctrine of digital platforms in assuming quasi-regulatory roles in the commercial value chain. Similarly, Al-Halfi (2024) focuses on civil liability for damages resulting from the damage to digital content, adding some of the comparative legal issues in the definition of digital harm under the existing legal framework of torts. The study highlights that in many cases there is no obvious physical damage resulting from digital content damage and that this makes the assessment of causation, quantification of the damage, and the definition of jurisdictions difficult.

Consequently, there are problems with the robustness of the civil liability mechanisms in different legal frameworks in terms of effectiveness and consistency of remedies. Seo (2025) reviews from a sectoral point of view the civil liability of the operators of electronic commerce platforms, focusing on platform-consumer (P2C) relationships. While platform operators are emerging as new intermediaries that have a great deal of control over the design of both the website and transaction, their liability is not clearly established in different jurisdictions, as Seo shows. This legal limbo leaves gaps in the enforcement, especially in cross-border transactions where there could be more than one legal system that has jurisdiction with respect to enforcement. Additionally, Tresnawati and Fatmawati (2021) discuss smart contract and the impact of smart contract in private international law via blockchain era.

Difficult to figure out who would be responsible if a smart contract doesn't meet expectations of the parties involved, they argue, since it is a self-executing contract that does not require human instruction. However, liability becomes a challenge in existing legal systems with a contractual execution process that is not based on the traditional approach of legal interpretation but on code.

An added layer of complexity is shown by Dabetić and Mirković (2024) who explore the concepts of digital property under the private international law rules. From their analysis, digital assets are not necessarily considered to be property, which makes the rules of liability not completely clear, especially in cross-border conflicts regarding the ownership, transfer and infringement of digital assets..

From a more general doctrinal standpoint, the issue of civil liability is enveloped within the context of private international law of the smart contract platforms in European legal order as discussed by Verstappen (2023). Verstappen points out that liability allocation is increasingly a matter of harmonisation of the regulations in digital environments, but is limited by the different approaches to national law on the fields of tort law, consumer protection and contract law.

**Table 3: Mapping Civil Liability in Digital Commerce to Applicable Legal Regimes**

| Type of Digital Activity                                             | Type of Civil Liability          | Legal Characterization           | Applicable Legal Regime              | Key Challenge                         |
|----------------------------------------------------------------------|----------------------------------|----------------------------------|--------------------------------------|---------------------------------------|
| <b>Platform-based e-commerce</b> (Seo, 2025)                         | Platform liability (P2C)         | Intermediary responsibility      | National + EU hybrid regimes         | Unclear scope of platform duty        |
| <b>Digital content damage</b> (Al-Halfi, 2024)                       | Tortious liability               | Intangible harm classification   | Comparative tort law systems         | Difficulty in proving causation       |
| <b>General digital business models</b> (Hassanah & Aprilianti, 2024) | Mixed contractual/tort liability | Multi-party responsibility       | Private international law frameworks | Fragmented liability allocation       |
| <b>Smart contracts</b> (Tresnawati & Fatmawati, 2021)                | Code-based contractual liability | Automated execution systems      | Blockchain governance + contract law | Absence of human fault element        |
| <b>Digital property disputes</b> (Dabetić & Mirković, 2024)          | Property-related liability       | Classification of digital assets | Emerging digital property law        | Legal uncertainty in asset definition |
| <b>EU smart contract frameworks</b> (Verstappen, 2023)               | Regulatory liability             | Harmonized private law approach  | EU private international law         | Divergence across member states       |

The analysis shows that the current situation of civil liability in cross-border digital commerce is fragmented and that traditional liability rules need to be constantly adapted to the digital world, because of the technologisation and the doctrinal uncertainties.

## 7. International Regulatory Frameworks and Harmonization

International bodies harmonizing different national legal frameworks in the context of digital commerce and cyberspace related conflicts are an emerging attempt to balance the different national legal frameworks with the non-border nature of digital transactions. In this context, the main goal of harmonization is to minimize the jurisdictional conflicts, improve legal certainty and facilitate the enforcement of rights and obligations in the digital space in international contexts.

However, in the meantime, a coherent international regulatory framework is hampered by conflicting regulatory philosophies, digital maturity of states and conflicting interests of sovereignty. Azam et al. (2026) provide an exploration of the existing status quo of trade governance and cross-border data flows and their tensions with other norms such as Shari'ah values. In the fields of data governance, digital trade and transnational commercial regulation, they uncover emerging competing normative orders that have an impact on harmonizing regulation. This plurality of sources of law is also the source of the difficulty in attaining a single global regulatory regime.

This multiplicity of laws sources and their complexity renders it arduous to achieve a single worldwide regime. Nainggolan et al. (2023) also provide a discussion on legal protection for cross-border e-transactions and its improvements with the increase of international cooperation for the protection of the parties to e-commerce transactions. Most of the problems that arise in the regulation are not always solved with the available regulatory tools, particularly in low institutional capacity countries and low digital infrastructure countries. This creates inequities in legal protection in various parts of the worldwide digital economy. In terms of dispute resolution, Rajah (2025) discusses how international arbitration and international commercial courts have grown in significance to settle cross-border digital disputes and explores the developments in the relationship between them. Rajah



suggests that these are options to litigation that takes place in state courts, and that they effectively mean harmonising. But he also says that fragmentation continues because of a lack of a "one-stop" procedure for commercial disputes involving digital content.

Overall, the literature suggests that although some strides have been made in the direction of regulatory convergence in the governance of cyberspace, it is still not a reality but rather a future goal. The fact that digital globalization exists in a structurally complex form is reflected in both the presence of multiple regulatory regimes and the need to refine the international legal frameworks of digital globalization, which continue to evolve and be adapted to technology.

## Critical Discussion

The new architecture of "conflict of laws" of civil liability in the cyberspace is characterised by the ongoing "tension" between the old and the new territorial principles and the borderless nature of digital communication. This is the new architecture of "conflict of laws" of civil liability in cyberspace, which keeps on displaying the ongoing tension between the old and the new territorial principles and the borderless nature of digital communication.

This tension is especially pronounced in the ongoing use of classic concepts of jurisdiction and liability, which were developed for traditional settings of legal relations with a geographic focus, but which have been extended to a digital scene of multi-jurisdictional, decentralised legal relations. This results in a number of doctrinal implications, especially regarding trans-border digital harm, algorithmic decision-making and platform liability. Alcici (2024), on the contrary, considers this structural mismatch from a critical angle and analyses the effect that the new technologies have had on the law of State Immunity and the territorial tort exception. The study highlights that the growth of digital activity raises questions about the concept of 'territoriality', especially as far as negative digital behaviour is concerned, as it can take place across several different jurisdictions in parallel, without a clearly identifiable location of origin or of the harm.

This challenges the territorial integrity of the traditional exception principle and questions fundamental whether the current territorial doctrines are sufficient to deal with transnational digital harm. This criticism is supported by the literature, which shows that as more and more of the legal frameworks that have governed cyberspace are challenged in the cyberspace conflicts, they fail to meet the requirement mandated by the Internet. Multiple actors, such as platforms, users and automated systems, sharing the responsibility make it difficult to determine who is responsible and to make the traditional enforcement tools effective.

As a consequence, there is a displacement of doctrinal approaches in the law, which are scattered and sometimes contradictory, and the generation of forum shopping and unpredictable law. Additionally, with the advent of AI and automated decision-making processes, these obstacles have intensified even further, bringing in non-human actors into the legal equation. This will challenge the traditional notions of intent, fault and causation, and necessitate reshaping the concept of civil liability and jurisdiction in digital space. In general, the critical analysis shows that the laws in place are reactive not adaptive and unable to keep track with the fast-paced changes in the digital technologies and trans-border trade activities.

## Recommendations and Future Legal Directions

The results of this research suggest the existing conflict-of-laws regime in the context of civil liability in cyberspace should be extensively modernized to be able to cope with the complexities of digital commercial transactions. One of the key recommendations is the progressive harmonisation of jurisdictional definitions which would be as flexible as possible and would not be based on territorial principles but on the "connecting factors" that will be increasingly technology-driven, including targeting, digital presence and economic impact. This would make things easier to predict in legal matters and ensure that it remains fair in cases of cross border disputes.

Another important path is increasing the effectiveness of international cooperation mechanisms, which may help to minimise the fragmentation of applicable law rules. With an increase of platform-based transactions and automated contractual systems, states should take into account the development of coordinated soft-law instruments or model rules to guide judicial reasoning in disputes involving cyberspace transactions. Instruments of this kind could have a valuable role to play in minimizing the legal inconsistencies between jurisdictions whilst maintaining national legal autonomy.

Furthermore, the digital technologies, like Artificial Intelligence, blockchain and smart contracts, are developing, which requires a rethinking of the liability concepts. The upcoming legal frameworks should take into consideration hybrid models of responsibility, which include the participation of intermediaries, automated systems and decentralized infrastructures. This would make it possible to allocate liability according to the true characteristics of the digital ecosystem—and not the contractual arrangements that are common in the past.

Lastly, ongoing academic and policy research is needed to ensure that technology and policy are connected. In a dynamic cyberspace, the adaptive models of governance are needed to adjust to the digital revolution, rather than to a doctrine interpretation.

## Conclusion

This study has focused on the conflict of laws issue of civil responsibility for digital commercial transactions in cyberspace, which faces major problems and issues of jurisdictional fragmentation, uncertainty of applicable law as well as the changing liability framework. However, traditional principles of private international law remain essential, but are becoming overloaded as digital commerce becomes 'borderless and decentralised'.

This picture of legal fragmentation and doctrinal incoherence repeats itself in a variety of settings of choice-of-law, jurisdictional, and civil liability rules. Although courts and scholars have come up with new solutions, including platform liability and effects-based jurisdiction and targeting tests, these solutions have proven to be ad hoc and not uniformly applied worldwide.

Finally, the report calls for a re-thinking of legal approaches to these issues—toward being more adaptive and technologically responsive, reflecting the realities of cyberspace. International cooperation, updating the concept of jurisdiction and changing the civil liability arrangements are important measures to reach a more coherent and effective system of private international law for the digital age.

## Reference

- Lukings, M., & Habibi Lashkari, A. (2022). Conflicts of Law. In *Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective* (pp. 85-115). Cham: Springer International Publishing.
- Elijah, J. (2025). Crossing Borders in Cyberspace: Rethinking Jurisdiction in Civil Litigation Amid the Rise of Digital Transactions. Available at SSRN 5505341.
- Okoli, P. N. (2022). Jurisdictional Rule "X" in the Conflict of Laws: Challenges of Policy and Security in Internet Torts with Business Implications. *Ga. J. Int'l & Comp. L.*, 51, 397.
- Terentyeva, L. V. (2021). Legal Jurisdiction concerning the Disputes in Cyberspace in the USA. *Law: J. Higher Sch. Econ.*, 236.
- Svantesson, D. J. B. (2021). Private international law and the internet.
- Giacalone, M., & Giacalone, P. (2024). When private international law meets technology. In *Research Methods in Private International Law* (pp. 222-244). Edward Elgar Publishing.
- Harahap, S. K. (2025). The Role of Private International Law in Resolving Disputes in Global Commerce. *Global International Journal of Innovative Research*, 2.
- Verstappen, J. (2023). Private International Law. In *Legal Agreements on Smart Contract Platforms in European Systems of Private Law* (pp. 321-389). Cham: Springer International Publishing.

## International Conflict of Laws Governing Civil Liability Arising from Digital Commercial Transactions in Cyberspace

- Chen, Z. (2023). Internet, consumer contracts and private international law: what constitutes targeting activity test?. *Information & Communications Technology Law*, 32(1), 23-44.
- Tresnawati, T., & Fatmawati, A. M. (2021). Blockchain-based smart contract: Advancing digital consumer protection and preventing private international law e-commerce cases. *Yustisia*, 10(3), 354-368.
- Dabetić, J. S., & Mirković, P. (2024). Digital property-specific issues in the application of private international law rules. *Pravo-teorija i praksa*, 41(4), 121-133.
- Nainggolan, B., Susanto, H., Yuniantin, H., & Suwarno, S. (2023). Guarantee of Legal Protection in Cross-Border Electronic Transactions= Garantia De Proteção Jurídica Nas Transações Eletrônicas Transfronteiriças. *Journal of Law and Sustainable Development*, 11(11), 1-15.
- Azam, M., Alwreikat, N. M., Alsyoud, B., Al Fandi, A. S. A. A., & Pharaon, R. A. K. M. (2026). Contemporary Trade Governance and Cross-Border Data Flows: A Comparative Study of Sharī'ah Principles and International Legal Frameworks. *MILRev: Metro Islamic Law Review*, 5(1), 686-721.
- Okoli, C. S. A., & Yekini, A. (2023). Implied jurisdiction agreements in international commercial contracts: a global comparative perspective. *Journal of Private International Law*, 19(3), 321-361.
- Melnik, V. D. (2022). On the question of some tendencies in the unification of national and international jurisdiction of Internet disputes. In *SHS Web of Conferences* (Vol. 134, p. 00085). EDP Sciences.
- Knapp, M. (2022). The Scope of Jurisdiction in Cross-Border Intellectual Property Disputes: Tackling Online Copyright Infringements. *Białostockie Studia Prawnicze*, 27(1), 159-171.
- Kohl, U. (2021). Jurisdiction in network society. In *Research handbook on international law and cyberspace* (pp. 69-96). Edward Elgar Publishing.
- Rajah, V. K. (2025). Courting Global Commerce: The Shifting Dynamics Between International Arbitration and International Commercial Courts. *Journal of International Arbitration*, 42(2).
- Ryngaert, C. (2023). International jurisdiction law. In *Research Handbook on Extraterritoriality in International Law* (pp. 13-30). Edward Elgar Publishing.
- Razmetaeva, Y., Ponomarova, H., & Bylya-Sabadash, I. (2021). Jurisdictional issues in the digital age. *Ius Humani, Revista de Derecho*, 10, 167.
- Hassanah, H., & Aprilianti, A. (2024, August). Law Transformation of Civil Liability in Digital Business. In *International Conference on Business, Economics, Social Sciences, and Humanities-Humanities and Social Sciences Track (ICOBEST-HSS 2024)* (pp. 145-153). Atlantis Press.
- Al-Halfi, K. H. Y. (2024, October). Civil Liability for Damage to Digital Content (Comparative Study). In *ZAC Conference Series: Social Sciences and Humanities* (Vol. 1, No. 1, pp. 312-336).
- Seo, H. (2025). Civil Liability of E-Commerce Platform Operators in Korea (Focusing on the P2C Relations). *Yuridika*, 40(2), 171.
- Kunda, I. Choice-of-court and choice-of-law clauses in digital consumer contracts: Current practices and compliance by online platforms. In *Consumer Protection and the Digital Economy* (pp. 238-259). Routledge.
- Wojciech, S. (2025). The issue of internet jurisdiction in common law and EU Regulations.
- Meliala, A. J., & Putra, A. K. (2024). Tacit Choice of Law in the Metaverse: What Law Applies?. *Uti Possidetis: Journal of International Law*, 5(1), 1-37.
- Coyle, J. F., Dodge, W. S., & Simowitz, A. D. (2022). Choice of law in the American courts in 2021: Thirty-Fifth annual survey. *The American Journal of Comparative Law*, 70(2), 318-363.
- Manne, G. A., & Harper, J. (2024). A Choice-of-Law Alternative to Federal Preemption of State Privacy Law. American Enterprise Institute.
- Das, D. (2024). Exploring The Legal Landscape of Cyber Torts. Available at SSRN 4746064.
- Brachotte, S., & Nuyts, A. (2023). Jurisdiction over cyber torts under the Brussels I Bis Regulation. In *Research Handbook on EU Internet Law* (pp. 215-230). Edward Elgar Publishing.
- Alcici, L. M. (2024). The impact of new technologies on the law of State immunity: time for a reassessment of the scope of the territorial tort exception. *Studia Prawnicze: rozprawy i materiały*, 35(2), 191-207.
- Verma, A., Lal, R., Venaik, S., & Srivastava, A. Cyber adjudication in the age of artificial intelligence—A conflict of

jurisdiction. In *Artificial Intelligence and New Age Technology* (pp. 161-171). Routledge.

Asensio, P. D. M. (2024). *Conflict of Laws and the Internet*. Edward Elgar Publishing.

Basedow, J. R. (2024). Alienated Twins—The Overlooked Private Law Dimension of Global Trade and Investment Governance. *World Trade Review*, 23(4), 507-518

..