International Journal of Innovative Technologies in Social Science

e-ISSN: 2544-9435

Operating Publisher
SciFormat Publishing Inc.
ISNI: 0000 0005 1449 8214

2734 17 Avenue SW,
Calgary, Alberta, T3E0A7,
Canada
+15878858911
editorial-office@sciformat.ca

ARTICLE TITLE	CHALLENGES OF CONFLICT OF LAWS IN CYBERSPACE
DOI	https://doi.org/10.31435/ijitss.1(49).2026.3346
RECEIVED	23 May 2025
ACCEPTED	25 December 2025
PUBLISHED	14 January 2026
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

CHALLENGES OF CONFLICT OF LAWS IN CYBERSPACE

Said Mabrouki
University of Oum El Bouaghi 04000 - Algeria. Legal and Political Studies Research Laboratory, Faculty of Law and Political Sciences, University of Oum El Bouaghi, Oum El Bouaghi 04000- Algeria.
ORCID ID: 0000-0002-7378-9159
Email: Said.mabrouki@univ-oeb.dz

Naima Akli
University of Bouira 10000 -Algeria. Globalization and National Law Research Laboratory, Faculty of Law and Political Sciences, University of Tizi Ouzou, Tizi Ouzou 15000-Algeria
Email: Naima.akli@univ-bouira.dz

ABSTRACT

The borderless nature of the internet poses significant challenges to jurisdiction and conflict of laws, as traditional territorial legal frameworks struggle to keep pace with the digital age. Although private international law has historically addressed cross border disputes, its rules have not evolved at the speed of technological change. In response, legal scholars advocate for a unified global framework often referred to as Lex Electronica enforced by digital judicial bodies. They argue that the internet's erosion of national boundaries necessitates new models of governance.
Nevertheless, private international law remains essential in practice, offering adaptable mechanisms such as tort liability principles for regulating online behavior. To effectively navigate the legal complexities of globalization, existing legal frameworks must be recalibrated, and national laws must evolve to reflect digital realities. At the same time, emerging actors like ICANN challenge traditional notions of sovereignty, exerting regulatory influence over cyberspace and raising critical questions about the capacity of legal systems to balance innovation with accountability.

KEYWORDS

Conflict of Laws, Private International Law, Digital Environment, Jurisdiction

CITATION

Said Mabrouki, Naima Akli (2026) Challenges of Conflict of Laws in Cyberspace. *International Journal of Innovative Technologies in Social Science*. 1(49). doi: 10.31435/ijitss.1(49).2026.3346

Introduction

The borderless nature of the internet, which transcends the territorial boundaries of states, raises countless problems concerning jurisdiction and conflict of laws. Although the rules of private international law have always provided solutions and proper legal frameworks, this is not the case when applied to the digital environment. It appears that these legal rules have not kept pace with the developments in information technology, as the scope they addressed in the past had defined territorial and legal limits. This leads us to question the extent to which these rules have adapted to ongoing changes.

In this regard, legal scholars argue that *"the evolution of the internet has caused borders to erode, paving the way for a new, free, and global space that legitimizes the idea of a unified global law for the internet (Lex Electronica), enforced by electronic judicial bodies"* (Fauvarque-Cosson, 2000). وعليه فان القوانين غير واضحة املعالم خاصة مع تشعب املنازعات وتداخل االختصاصات

Therefore, the laws are unclear, especially with the complexity of disputes and the overlapping of jurisdictions(mabrouki, 2023, p.227).

However, reality contradicts this. Rather than threatening the existence of private international law, the current developments necessitate it more than ever. It may provide a reference framework to rely on, as it often offers numerous legal solutions that may sometimes suffice. Supporting this view, some legal scholars researching this issue advocate for applying rules of tortious civil liability to regulate activities on the internet

(Vivant, 1996). Thus, the application of private international law remains essential. To confront the globalization of law, these rules must be profoundly recalibrated and renewed. The digital environment demands a reevaluation and adaptation of national legislations to meet new requirements (First Requirement). Finally, it will be demonstrated that these legal systems are under scrutiny due to the emergence of new powers, such as (ICANN), which seek to impose their sovereignty over the digital environment (Second Requirement)

First Section: Conflict of Laws in the Digital Environment

The transnational nature of computer networks grants an international dimension to activities that were previously tied to the legal system in which they operate. The global character of the internet will multiply disputes involving foreign elements. Until recently, private international law was viewed as merely peripheral, relevant primarily to multinational corporations (POST, 1995). Why, then, is this law not taken seriously in light of judicial precedents concerning domain names and whether resorting to it is effective or not? (Gautier, 1996) To assess the impact of the digital environment on jurisdictional issues within legal systems, we must first clarify how these matters are currently addressed. Jurisdiction, on one hand, refers to the authority of the legislative body over a specific issue (Subsection I), and on the other hand (Thevenoz & C., 2001), the authority of the court to adjudicate a case (Subsection II).

Subsection I: Determining the Applicable Law

When addressing conflicts of laws, the debate centers on proponents of the law of the country where the server is located (the "sending theory") and proponents of the law of the country receiving the message (the "receiving theory"). These solutions are unsatisfactory to all, as the first approach favors countries with servers whose laws are less restrictive than those of recipient states, while the second risks negatively impacting e-commerce due to the impracticality of complying with all recipient countries' laws (Vivant, 1996).

As for the applicable law governing tort liability, it is not subject to any international convention. Consequently, we resort to national law without delving into international legal matters. Thus, we transpose conflict-of-laws rules to the internet in accordance with existing legislation. The law of the state where the obligation-triggering act occurred is applied, as practiced in most legal systems. This is reflected in Article 20 of the Algerian Civil Code, which states: *"Non-contractual obligations are governed by the law of the country where the act giving rise to the obligation occurred. However, concerning obligations arising from tortious acts, the preceding paragraph does not apply to acts committed abroad that are lawful in Algeria, even if deemed unlawful in the country where they occurred."*

Similar to jurisdictional issues, the question of which state's law applies—the law of the state where the harmful act originated or the law of the state where the harm materialized—remains contested (Lucas, & Frayssinet, 2001). French jurisprudence has resolved this by adopting the *place where the damage occurred*. However, this choice has faced criticism due to the fluid nature of information exchanged online and its impracticality. Nonetheless, court rulings have clearly supported applying French law as the recipient country, particularly in areas like copyright, trademarks, domain names, and other fields.

While applying recipient-state laws to redress harm aligns with prevailing legal doctrine, this approach is unsatisfactory in practice. Implementing it in the digital environment would open the door to applying all global laws, complicating compensation for victims due to legal contradictions and challenges in enforcing foreign judgments. This necessitates exploring alternative mechanisms that offer more effective solutions and stronger safeguards for victims.

Legal systems under **Common Law** (e.g., the U.S. and Canada) advocate the *"Proper Law for the Tort"* principle, where judges evaluate each case to identify and apply the most suitable law. This method, termed the *"appropriate law approach"* (Gutman, 1999), is exemplified in a **New York court case** involving a traffic accident in Ontario, Canada. The court had to choose between U.S. law (which compensates victims) and Canadian law (which denies compensation). Judges ruled in favor of U.S. law, citing two reasons: (1) multiple factual ties to New York (e.g., the parties' residence), and (2) the greater fairness of U.S. law compared to Canada's restrictive approach, which risked collusion between victims and drivers against insurers. This reasoning frequently resurfaces in domain name disputes, where the *"Proper Law for the Tort"* has been applied by **WIPO** in domain name litigation (Gutman, 1999).

Thus, both civil and common law systems can complement each other, much like international conventions that blend private law predictability with common law flexibility. Notably, French courts in recent years have adopted the *"appropriate law"* principle, selecting the law of the state most closely connected to the harmful act.

Subsection II: Exercising Jurisdiction in the Digital Environment

- **The definition of digitization :**
- Digitization has numerous definitions that vary depending on the orientations, opinions, theoretical and intellectual premises, and ideology of each researcher and their scientific and academic specialization. We find definitions that can be presented as follows:

Some define it as the process of converting information sources:

"Digitization is the process of converting information sources from their traditional form (such as paper books) to a digital form (such as e-books) withthe aim of providing the greatest possible number of information sources to users with greater ease" (Zedira, 2025, p.8).

- Its one of the most significant transformations in the organizational environment is closely linked to modern information and communication technologies. This shift reflects a contemporary, modular model in which management transfers its inputs and outputs from traditional methods to a digital approach, relying on digital tools and technologies across various organizational processes (Boutarfa Rochdi, & Zedira Khammar, 2024, p. 3).

Jurisdictional issues have not been immune to the impact of technological advancements. Practically, the duties and obligations of parties in the digital environment do not differ from those in traditional settings (under conventional law). Therefore, the rules of private international law must be applied to determine the competent court for resolving disputes arising in cyberspace (I). The rapid evolution of the internet has undeniably increased the number of disputes with international dimensions, compelling private international law to adapt by envisioning a more comprehensive legal framework to accommodate such conflicts.

Before addressing jurisdictional competence over internet-related activities, it is crucial to outline the general principles courts may rely on for jurisdiction and the circumstances under which jurisdiction is deferred to another state. In France, this issue is governed by general law and international conventions, such as **European Council Regulation No. 44/2001** of December 22, 2000, on jurisdiction, recognition, and enforcement of judgments in civil and commercial matters (Conseil, 2001). This regulation supersedes the 1968 Brussels Convention and the 1999 Treaty of Amsterdam. It aims to respect the specificity of e-commerce for all EU member states, though it does not modify jurisdictional rules related to damages. Notably, Algerian legislators have largely adopted provisions similar to those of their French counterparts (**I**), while U.S. jurisdiction is defined by Supreme Court rulings from 1945 (**II**).

I. Jurisdiction in Algerian and French Law

When harmful information is disseminated online, disputes typically acquire an international character. To determine jurisdiction, jurisdictional rules must be expanded to encompass broader boundaries. Regarding liability for damages, **Article 37** and **Paragraph 2 of Article 39** of the Algerian Civil and Administrative Procedure Code allow plaintiffs to file claims either in the defendant's domicile or where the harmful act originated. French law parallels this but extends jurisdiction to include the *location where the victim suffered harm*, as stipulated in **Article 46** of the French Code of Civil Procedure. Thus, French jurisdictional scope is broader than Algeria's.

Both Algerian and French law grant plaintiffs the privilege of jurisdictional choice. Under **Article 20** of the Algerian Civil Code and **Article 41** of its Civil Procedure Code, plaintiffs may request trial in their own domicile, even summoning foreign defendants to national courts for contractual obligations formed there. French law mirrors this in **Article 14** of its Civil Code ( ). This principle, applied in French press law, acknowledges that publications may reach multiple jurisdictions, a rationale extended to internet disputes, including domain name cases under judicial precedent. Similar rulings under the 1968 Brussels Convention (replaced by EU regulations) permit victims to sue in the defendant's domicile, the origin of harm, or where damage occurred (Vivant, 1996).

II. Jurisdiction in U.S. Law

Studying U.S. law is essential for theoretical and practical reasons. U.S. courts were among the first to handle internet-related disputes, and the U.S. hosts vast numbers of internet users and e-commerce actors. Determining whether U.S. courts have jurisdiction over foreign parties is complex, particularly under the **14th Amendment's** protections for individual freedoms (Dearing, 1999). U.S. jurisdiction generally follows the defendant's domicile (*in personam* jurisdiction). However, jurisdiction over non-resident defendants may be asserted through two criteria: **general jurisdiction (a)** and **specific jurisdiction (b)**.

a. General Jurisdiction

General jurisdiction applies when the defendant has substantial, continuous ties to the jurisdiction. No additional links are needed; mere residence or corporate registration suffices. U.S. courts may thus adjudicate disputes involving non-residents if they operate within the jurisdiction (Muhammad, 2007).

b. Specific Jurisdiction

The U.S. Supreme Court established modern standards for specific jurisdiction. Courts must confirm:

1. **Minimum Contacts**: The defendant purposefully directed activities toward the jurisdiction, and the dispute arises from those activities.
2. **Fairness**: Exercising jurisdiction must not unduly burden the defendant and must align with "traditional notions of fair play and substantial justice".

Courts assess whether defendants could foresee being sued in the jurisdiction and whether jurisdiction aligns with state interests. These standards enable U.S. courts to assert jurisdiction over domestic and international disputes alike (Muhammad, 2007).

The distinction between general and specific jurisdiction holds theoretical importance, but courts often blend these criteria. Practically, jurisdiction hinges on sufficient connections between the defendant and the forum. In Canada, jurisdiction follows the **"Real and Substantial Connection"** test, akin to U.S. principles. These standards have been applied in domain name and trademark disputes, ensuring equitable resolution across borders.

Second Section: Proposed Solutions for Resolving Conflict of Laws in the Digital Environment

The digital environment and its associated issues necessitate a re-evaluation and development of states' jurisdictional rules. States must determine how to assert jurisdiction over activities arising in cyberspace, as the territorial scope of digital environments often remains ambiguous. Currently, there is difficulty in assessing the limited strategies adopted by states in this regard. The first proposed solution is granting parties the freedom to designate the court adjudicating their dispute—a practice already implemented in the dispute resolution procedures of **ICANN**. Adopting this approach could mitigate jurisdictional challenges (Gola, 2002).

The second proposal involves harmonizing national legislations to resolve jurisdictional conflicts in the digital environment. Harmonization here refers to aligning substantive and procedural standards with jurisdictional criteria. This issue lies at the heart of debates surrounding domain names and their protection, as the technical infrastructure of the internet often disregards safeguarding intellectual and industrial property rights online. These rights are treated indistinguishably from other data, exacerbating their vulnerability due to their intangible nature. As immaterial assets, they exist ubiquitously, transcending geographic boundaries and proliferating globally. However, the laws protecting these rights remain territorial, as they originate and operate within the confines of national jurisdictions that recognize them. This underscores the urgency of fortifying international protections through multilateral treaties. Despite such legislative harmonization—potentially offering solutions for online disputes—these measures remain insufficient (Subsection I).

In light of these challenges, a novel legal framework may emerge to overcome the limitations of traditional jurisdiction. When discussing domain names, it is imperative to examine the role of bodies managing registration systems, as these entities constitute a critical component of *digital governance*. Their decisions profoundly impact cyberspace, yet individuals remain subject to specific jurisdictional authorities. Traditional judicial bodies will inevitably retain relevance, as relinquishing their jurisdictional competence remains inconceivable (Subsection II).

Subsection I: Legislative Harmonization

Among the proposed models of shared governance for cyberspace is resolving challenges through the creation of a unified cyberspace law grounded in international treaties. The goal of harmonization is to ensure transparency and fairness, fostering better cooperation among judicial authorities. However, harmonization can be particularly challenging at the level of substantive standards, which reflect the values of citizens represented by their legislative bodies. A prime example is trademark law, where legal systems still clash over registrable marks—a conflict that equally applies to domain names (Gola, 2002).

Nevertheless, several international conventions in industrial property law (I) have emerged, implementing strategies to protect specific elements in cyberspace (II). This approach, applicable to other domains, raises challenges such as treaty conflicts and ratification complexities—processes that are inherently slow and intricate, contrasting sharply with the rapid, dynamic evolution of internet technology (III).

I. The Necessity of International Protection

The need for international protection in intellectual property has become urgent, exemplified by the **1883 Paris Convention for the Protection of Industrial Property**, which marked the first step toward globalizing this issue. This was followed by the **1891 Madrid Agreement**, later amended by the **1989 Protocol**. Culminating these efforts, the **1994 TRIPS Agreement** (Trade-Related Aspects of Intellectual Property Rights) sought to harmonize legislation and provide international protections. The TRIPS Agreement did not override prior international treaties but incorporated, expanded, and refined their provisions. It mandated that member states align their national laws, regulations, and intellectual property frameworks with its principles (El-Saghir, 2007).

The TRIPS Agreement obligated all WTO members to apply the provisions of referenced international treaties, regardless of their prior ratification. By consolidating fragmented intellectual property norms into a single document, TRIPS achieved coherence and obligated all WTO members to comply, irrespective of their participation in earlier treaties. Beyond referencing existing treaties, TRIPS introduced novel provisions to strengthen intellectual property rights globally, addressing gaps left by prior agreements. (El-Saghir, 2007)

In addressing conflicts between domain name holders and trademark owners, international protections for trademarks and domain names could serve as effective tools to combat abusive practices.

II. Limits of Legislative Harmonization

States cannot relinquish their role in regulating the digital environment under national laws; instead, they must adapt to its unique characteristics and resources. Legislative harmonization has become a widely adopted approach to resolving jurisdictional and territorial disputes arising from cyberspace.

International organizations like **UNCITRAL** (United Nations Commission on International Trade Law), **OECD** (Organisation for Economic Co-operation and Development), and **WIPO** (World Intellectual Property Organization) have significantly contributed to harmonizing legislation. Many states use the **UNCITRAL Model Law** as a foundation for modernizing commercial laws, incorporating rules on e-commerce to clarify the validity and evidentiary weight of electronic documents and signatures. Provisions on the rights and obligations of intermediaries in digital transactions derive from Canada's **Uniform Electronic Commerce Act** and **Uniform Electronic Evidence Act** (Gola, 2002).

While this unified legal framework appears suitable for regulating cyberspace, it allows states flexibility in achieving treaty-defined objectives. Legal scholars caution that treaties should not be the sole model, as they merely outline foundational principles for internet governance. The inherent complexity of centralizing legislation and the fragility of existing legislative processes render centralized systems inadequate for addressing vast, evolving challenges like internet regulation. Simple harmonization of dispute resolution mechanisms, however technically efficient, remains insufficient to resolve internet-related conflicts. (Burk, 1998)

Harmonization could also draw on other sources, such as judicial precedents establishing unified rules before legislative intervention. U.S. law exemplifies this, operating within a federal framework that fosters interstate litigation. American legal doctrine and jurisprudence have consistently advanced significant developments in such cases. For instance, U.S. law introduced the **"focus criterion"** for jurisdiction—later reflected in **Article 5 of the Hague Convention on Jurisdiction**—long before its international codification (M.Vivant, 1996). Judicial precedents may solidify customs that eventually inform legislative drafts, yet efforts to create a global treaty for cyberspace face obstacles, as states prioritize national interests over rapid technological evolution (Lucas, & Frayssinet, 2001).

III. Cyberspace as an Autonomous Realm?

Debate persists over recognizing cyberspace as an independent, parallel environment to the physical world. Legal scholars argue that *"isolating the internet from the real world is impractical, as the two are interdependent"* (Gola, 2002). For example, domain name disputes highlight this interplay: *"Online and offline activities cannot be equated, particularly in legal matters involving product/service identification or commercial reputation. A consumer encountering a trademark online evaluates it differently than offline, leading to confusion between digital and non-digital users"* (Gola, 2002) .

While more international treaties on cyberspace are anticipated, their scope remains limited to shared guiding principles. States must adopt common core values, especially regarding freedom of expression, as curbing cybercrimes demands international cooperation. Harmonization thus becomes integral to this policy framework. Yet, a critical question remains: Can an international organization establish and enforce rules to govern cyberspace?.

Subsection II: Establishing an International Organization to Regulate Cyberspace

The establishment of an international organization tasked with regulating cyberspace raises challenges related to competition among existing international bodies, making the creation of such a structure difficult. As previously noted, initiatives by the **European Union**, **UNCITRAL** (United Nations Commission on International Trade Law), **OECD** (Organisation for Economic Co-operation and Development), and **WIPO** (World Intellectual Property Organization) have evolved concurrently, leading to overlaps and contradictions. Introducing a new international organization risks further jurisdictional conflicts among these entities.

By the end of this chapter, it is evident that private international law must undergo reevaluation and modernization to address new challenges posed by the information society. Conflicts of laws and jurisdiction remain obstacles to establishing a cohesive legal framework for cyberspace.

While existing laws often provide solutions for domain name disputes, adapting positive legal provisions to accommodate the digital environment—and its novel legal elements such as domain names—remains essential.

Domain name litigation has also underscored the need for international legislative harmonization to adjust jurisdictional rules in non-contractual matters. This aligns with the **"focus criterion"**, which has proven more adaptable to the demands of cyberspace. Judicial precedents reveal excessive protections for trademark holders in cases of unfair competition and counterfeiting, while highlighting challenges tied to the internet's lack of territoriality and the difficulty of enforcing court decisions across foreign jurisdictions.

These legal frameworks could be adapted through new strategies tailored to cyberspace. A prominent example is the shift toward **online dispute resolution (ODR) mechanisms**, leveraging the efficiency and resources of digital networks.

The proliferation of domain name disputes prompted WIPO to develop extrajudicial **dispute resolution mechanisms**. This innovative approach resolves many domain name-related issues and may extend to broader internet governance, e-commerce, and other emerging cyber challenges."

Conclusion:

At the conclusion of this study, it becomes evident that private international law must undergo reassessment and development to address the new challenges posed by the digital environment. The issue of conflict of laws remains one of the greatest obstacles to establishing a dedicated legal framework for cyberspace. While existing laws in their current form often provide solutions for protecting certain rights, it has become imperative to adapt these laws to accommodate the evolving digital environment, which continually introduces novel legal elements.

Through a focused examination of conflict of laws in the digital realm, this study underscores the necessity of international legislative harmonization to revise jurisdictional rules, particularly those governing civil liability. This approach aims to operationalize the **"focus criterion"**, which has proven adaptable and effective in addressing the demands of the digital landscape.

To align legal frameworks with new strategies tailored to cyberspace, the adoption of **alternative dispute resolution mechanisms**—such as online, computer-mediated processes—is essential. Leveraging the internet's resources can enhance the efficiency of dispute resolution systems, as demonstrated by international precedents in this field.

This transformation requires embracing innovative solutions that harmonize legal predictability with the dynamic nature of digital interactions, ensuring equitable governance in an increasingly borderless world.

REFERENCES

1. Boutarfa Rochdi, & Zedira Khammar. (2024). DIGITIZATION AND ITS IMPACT ON THE QUALITY OF HIGHER EDUCATION IN ALGERIAN UNIVERSITIES. International Journal of Innovative Technologies in Social Science, (4(44). https://doi.org/10.31435/ijitss.4(44).2024.3018
2. Burk, D. L. (1998). Trademark doctrines for global electronic commerce. *South Carolina Law Review*.
3. Conseil, R. (2001). *L'OCE n° L 012, 22 décembre 2000*. Texte publié au *Journal Officiel des Communautés Européennes*.
4. Dearing, M. C. (1999). Personal jurisdiction and the internet: Can the traditional principles and landmark cases guide the legal system into the 21st century? *Journal of Technology Law and Policy*.
5. El-Saghir, H. E. (2007). *The international protection of industrial property rights: From the Paris Convention to the TRIPS Agreement*. Egypt: World Intellectual Property Organization.
6. Fauvarque-Cosson, B. (2000). *Le droit international privé classique à l'épreuve des réseaux*. Rapport présenté au colloque international sur l'Internet et le droit européen et comparé de l'Internet, Paris.
7. Gautier, P. Y. (1996). Du droit applicable dans le "village planétaire", à titre de l'usage immatériel des œuvres. *D chronique*.
8. Gola, R. (2002). *La régulation de l'internet: Noms de domaine et droit des marques*. Marseille: Université de Marseille.
9. Gutman, D. (1999). *Droit international privé*. Paris: Éditions Dalloz.
10. Lucas, A., Deveze, J., & Frayssinet, J. (2001). *Droit de l'informatique et de l'Internet*. Paris: Presses Universitaires de France (PUF).
11. Mabrouki, S. (2023). *The role of jurisdiction in the resolution of disputes of agricultural concession contracts. Journal of Legal and Economic Research, 6*(2), 215–229.
12. Muhammad, K. I. (2007). Conflict of laws in tort liability arising from car accidents (A comparative study). *Al-Rafidain Journal of Law*, 9(32), 139–140. College of Law, University of Mosul.
13. Post, D. (1995). Anarchy, state, and the Internet: An essay on law making in cyberspace.
14. Thévenoz, L., & Bovet, C. (2001). *Journée de droit bancaire et financier*. Berne: Éditions Staempfli.
15. Vivant, M. (1996). *Cybermonde: Droit et droits des réseaux*. Paris: Éditions G.É.P.
16. Zedira Khammar, Nour El Houda Kouachi, Zahia Boumedjane, Hichem Amejouj, & Said Mabrouki. (2025). THE IMPACT OF DIGITIZATION ON ADMINISTRATIVE CREATIVITY: A FIELD STUDY IN AN ALGERIAN PUBLIC INSTITUTION. International Journal of Innovative Technologies in Social Science, (2(46). https://doi.org/10.31435/ijitss.2(46).2025.3372