E-ISSN: 2997-9439

American Journal of Education and Evaluation Studies

https://semantjournals.org/index.php/ AJEES

| Research Article

Check for updates

Problems of Digital Relations and their Conflict-of-Law Regulation in Private International Law

Azamat Ergashev Ergashevich

PhD in Law, Associate Professor of the Private international law department, Tashkent State University of Law, Uzbekistan

azamat.ergashev@interlex.uz

Abstract: This article provides an in-depth analysis of the emerging challenges in regulating digital relations within the framework of Private International Law. As global digital transactions become more complex, existing conflict-of-law rules are increasingly inadequate to address issues such as jurisdiction, applicable law, data protection, blockchain-based contracts, and artificial intelligence. The study explores current international frameworks, examines legislative gaps, and provides recommendations for modernizing conflict-of-law rules to accommodate the evolving digital legal environment, with a particular focus on Uzbekistan's experience.

Keywords: Private International Law, digital relations, conflict-of-law, jurisdiction, blockchain, artificial intelligence, cross-border data flows, Uzbekistan, electronic contracts.

Introduction. The rapid digitalization of global economic and legal relations has generated a wide range of new legal challenges. Private International Law, traditionally concerned with determining jurisdiction and applicable law in cross-border disputes, is now facing increased complexity due to the nature of digital relations. Transactions occurring entirely online, without a clear physical connection to any one jurisdiction, raise fundamental questions about territoriality, legal certainty, and fairness. This article seeks to provide a detailed analysis of these issues, offering insights into their practical implications and the reform efforts underway globally and in Uzbekistan.

The Legal Nature of Digital Relations. Digital relations encompass a broad spectrum of activities, from e-commerce and digital services to automated contracts and decentralized finance. These relations are often formed between parties in different jurisdictions, without physical presence or traditional documentation.

Electronic Contracts and Smart Contracts. Electronic contracts have gained widespread acceptance, particularly through instruments such as the UNCITRAL Model Law on Electronic Commerce.[1] However, recognition and enforcement still vary across jurisdictions. Smart

[1]UNCITRAL. (1996). *Model Law on Electronic Commerce*.

contracts, built on blockchain technologies, raise further complexities regarding automation, lack of human oversight, and jurisdictional accountability.[2]

Digital Assets and Intellectual Property. Digital assets such as cryptocurrencies and NFTs defy traditional property classifications. For instance, while some jurisdictions consider cryptocurrencies as property (UK Jurisdiction Taskforce, 2019), others lack legal definitions. This inconsistency hampers cross-border enforcement of ownership rights. Similarly, enforcing intellectual property rights on digital content across jurisdictions remains problematic due to varying interpretations and enforcement standards.[3]

Artificial Intelligence in Contract Formation. AI is now employed to draft and even negotiate contracts. However, under traditional contract law, agency requires intent and legal capacity. AI systems lack personhood, which raises questions about the validity of AI-generated contracts.[4]

Conflict-of-Law Challenges in the Digital Context. **Determining the Applicable Law** Traditional PIL rules such as lex loci contractus (law of the place of contract) and lex loci solutionis (law of the place of performance) become difficult to apply in a digital context where parties operate in different jurisdictions and transactions are executed electronically. Courts often fall back on connecting factors such as party autonomy or habitual residence, which are inadequate for decentralized systems like blockchain.[5]

Jurisdiction and Digital Presence. Digital presence complicates the concept of jurisdiction. In *Google Spain SL, Google Inc. v Agencia Española de Protección*[6] *de Datos*, the Court held that Google's operations in Spain constituted sufficient presence to establish jurisdiction. This ruling has influenced broader interpretations of territorial reach in digital cases, highlighting the inadequacy of traditional physical presence tests.

Cross-Border Data Flows and Privacy Regulations. Cross-border data transfers are regulated unevenly. The GDPR, for example, restricts data transfers to countries lacking 'adequate' protection (Article 45 GDPR). Uzbekistan's 2019 Law on Personal Data lacks an adequacy decision from the EU, complicating digital services that rely on data flows. This legal fragmentation exposes businesses to conflicting legal obligations.[7]

Platform Liability and Dispute Resolution. Digital platforms often incorporate terms of service with jurisdiction and arbitration clauses favoring their home country. However, in consumer cases, such clauses may violate protective PIL principles, especially under EU Regulation No. 1215/2012 (Brussels I bis Regulation), which prioritizes consumer domicile in jurisdictional questions.

International Frameworks and Soft Law Instruments. **The Hague Conference on PIL Instruments** The 2005 Hague Convention on Choice of Court Agreements and the 2019 Hague Judgments Convention provide key frameworks for jurisdiction and judgment recognition. Yet, these instruments do not account for unique features of digital contracts, such as smart contract enforcement or AI-generated obligations.[8]

UNCITRAL's Work on Electronic Commerce. The UNCITRAL Model Law on Electronic Commerce (1996) and the 2005 Convention on the Use of Electronic Communications in International Contracts recognize the legal validity of electronic messages. Nevertheless, adoption

[2] Bradshaw, S., Millard, C., & Walden, I. (2021). *Cloud computing law*. Oxford University Press.
[3] Bygrave, L. A. (2017). *Internet governance by contract: The rise of a new contractual order for regulating online behavior*. Oxford University Press.
[4] Koops, B.-J. (2020). The concept of Lex Digitalis. *Computer Law & Security Review, 36*, 105–117
[5] Kuner, C. (2020). *Transborder data flows and data privacy law*. Oxford University Press.
[6] European Court of Justice. (2014). Google Spain SL, Google Inc. v
[7] Kuner, C. (2020). *Transborder data flows and data privacy law*. Oxford University Press.
[8] Hague Conference on Private International Law. (2019). *Judgments Convention*.

remains patchy and many countries—including Uzbekistan—have yet to fully integrate these standards.[9]

Regional Approaches: *EU, US, Asia-Pacific.* The EU's General Data Protection Regulation, Digital Markets Act, and Digital Services Act represent an advanced framework for digital governance. In contrast, the United States lacks comprehensive federal regulation, relying on sectoral and state-level rules. Asia-Pacific frameworks like the ASEAN Data Management Framework are emerging but lack enforceability.[10] *Uzbekistan's Legal Framework in the Context of Digital Relations.* Uzbekistan has made initial efforts to regulate the digital sphere through several legislative acts. The Law on Electronic Commerce acknowledges the legal force of electronic transactions, a crucial step in integrating digital practices into national commercial law. However, the law lacks specificity regarding cross-border transactions, leaving a legal vacuum in areas such as foreign electronic signature recognition, international jurisdiction, and dispute settlement mechanisms. Without comprehensive provisions on transnational e-commerce, businesses and consumers remain exposed to legal uncertainty when engaging in international digital transactions.

Furthermore, the Law on Personal Data represents progress in addressing privacy and data governance. It includes provisions on data collection, processing, and user consent, yet mandates data localization—requiring that personal data of Uzbek citizens be stored within the country. This requirement, while aimed at sovereignty and control, poses compliance challenges for international companies operating across jurisdictions. The law also lacks clear rules governing the lawful transfer of data to countries with divergent legal standards, making it difficult for digital platforms to ensure regulatory alignment with frameworks such as the EU's GDPR.

Conflict-of-Law Rules in National PIL Legislation. Uzbekistan's Law on Private International Law sets out general conflict-of-law principles applicable to civil and commercial matters involving foreign elements. However, it does not specifically address the complexities introduced by digital relations. For instance, it does not provide rules on determining the applicable law for smart contracts, online service agreements, or AI-generated legal acts.

The law continues to rely on traditional connecting factors such as the place of contract formation, the habitual residence of the party, or the place of performance—criteria which are often inapplicable or ambiguous in the context of virtual transactions. As a result, Uzbek courts face difficulties in determining the governing law in digital disputes, leading to inconsistent jurisprudence and legal unpredictability. The absence of clear, adapted rules on digital conflict-of-laws risks hampering legal innovation and deterring foreign investment in Uzbekistan's digital economy.

Judicial Practice and Institutional Challenges. To date, Uzbekistan's judiciary has had minimal exposure to digital legal disputes involving international elements. There is a lack of established judicial practice on questions of applicable law, jurisdiction, and recognition of foreign judgments in digital contexts. This gap is partly due to insufficient technical training for judges and legal practitioners, many of whom are unfamiliar with blockchain technologies, AI applications, and digital signatures.

Institutional limitations further compound these challenges. Courts lack digital infrastructure such as e-filing systems, electronic evidence handling mechanisms, and digital case management tools. Additionally, there is no dedicated chamber or court specializing in IT or digital commerce, which

[9] UNCITRAL. (2005). *United Nations Convention on the Use of Electronic Communications in International Contracts*.

[10] Bygrave, L. A. (2017). *Internet governance by contract: The rise of a new contractual order for regulating online behavior*. Oxford University Press.

means that complex disputes involving new technologies are handled through general civil procedure, often without the necessary technical background.

To remedy this, Uzbekistan must invest in both capacity-building and institutional innovation. Judicial cooperation agreements with countries experienced in digital law, joint training programs with international organizations (UNCITRAL, UNIDROIT), and pilot courts for digital dispute resolution would enhance judicial readiness. Without such measures, Uzbekistan may struggle to keep pace with the rapid digitalization of international commercial relations.

Case Studies and Hypothetical Scenarios. Blockchain-Based Sales Contract between Uzbekistan and the EU. Consider a scenario in which an Uzbek buyer purchases a non-fungible token (NFT) from a French digital artist via a decentralized blockchain platform. The transaction is automated through a smart contract, which initiates the transfer of digital ownership once the buyer's cryptocurrency payment is received. However, due to a technical glitch, the artwork is not transferred correctly, and the buyer suffers financial loss.

The case raises critical PIL questions: What is the applicable law—the law of the seller's residence (France), the buyer's (Uzbekistan), or the blockchain jurisdiction (which may not even exist physically)? Which court has jurisdiction? The decentralized nature of the transaction makes it difficult to identify a governing legal framework. Under current Uzbek law, these questions remain unanswered, as there is no explicit provision for blockchain-based transactions or decentralized autonomous organizations. This legal uncertainty creates significant risk for Uzbek citizens participating in international digital commerce.

Cross-Border AI-Powered Contract Generation. Imagine an Uzbek entrepreneur using an AI-based legal tech platform located in Singapore to generate a service contract with a Dutch freelancer. The AI platform suggests contractual terms, fills in details, and finalizes the agreement with minimal human intervention. Later, a dispute arises regarding performance obligations and deliverables.

This hypothetical raises several unresolved PIL issues. First, was the contract legally formed if the AI, rather than a natural person, handled the negotiation? Second, can the AI be considered an agent under Uzbek or Dutch law? Third, what law governs the contract—Uzbek, Dutch, or Singaporean? Finally, which court has jurisdiction?

Uzbekistan's legal system provides no clear guidance on the use of AI in contract formation or on attributing legal responsibility to AI systems. As such technologies become mainstream, failing to modernize conflict-of-law rules will increase transactional risks and reduce Uzbekistan's competitiveness in the digital economy.

These scenarios highlight the urgent need for updated legislation that directly addresses the peculiarities of digital relations within the framework of private international law. The longer such reform is delayed, the greater the legal fragmentation and uncertainty for individuals and businesses operating across borders.7. Reform Proposals and Strategic Recommendations

Modernizing Conflict-of-Law Rules. Uzbekistan and similar jurisdictions should adopt conflict-of-law provisions tailored to digital relations. These should include:

1. Rules for determining the applicable law in smart contracts.
2. Mechanisms for addressing AI-generated legal acts.
3. Clear provisions on the legal status of decentralized platforms.

To address the increasing complexity of digital cross-border transactions, Uzbekistan should prioritize participation in international legal instruments that support the harmonization of conflict-of-law rules in the digital domain. Specifically, accession to the 2005 Hague Convention on Choice of Court Agreements and the 2019 Hague Judgments Convention would facilitate

mutual recognition and enforcement of foreign judgments—particularly relevant for digital disputes involving smart contracts, AI systems, and data transfers. These conventions also promote predictability and legal certainty in cross-border litigation. Furthermore, Uzbekistan should consider ratifying the UNCITRAL Convention on the Use of Electronic Communications in International Contracts (2005), which establishes a framework for the legal validity of electronic communications in international transactions.

In addition to joining existing instruments, Uzbekistan should advocate for the development of new multilateral agreements that reflect the technological advancements of the digital age. These may include treaties covering blockchain governance, cross-border AI liability, and international data flow regulation. Uzbekistan's active participation in UNCITRAL and The Hague Conference working groups can strengthen its voice in shaping global digital law and aligning domestic legislation with international standards. Ultimately, these steps would reinforce Uzbekistan's credibility as a secure and reliable jurisdiction for digital commerce and legal cooperation.

Strengthening Uzbekistan's Legal Infrastructure. Legal harmonization must be complemented by institutional and structural reforms at the national level. Uzbekistan should undertake a strategic overhaul of its legal infrastructure to prepare for the influx of digital legal disputes and to align with global legal standards. First, the establishment of specialized judicial chambers or courts with jurisdiction over digital and technology-related disputes is imperative. These bodies would be staffed with judges trained in private international law and digital technologies, enabling more informed and consistent decisions.

Second, legal education and professional development must integrate modules on digital law, international e-commerce, data protection, and legal informatics. Bar associations, judicial training centers, and universities should collaborate to develop certification programs and continuing legal education tailored to emerging legal technologies. Third, Uzbekistan must formulate a comprehensive national strategy on digital legal transformation. This strategy should include objectives such as:

4. Digitalization of court procedures and case management;
5. Creation of a centralized case law database for digital disputes;
6. Promotion of legal tech startups and legal research in digital governance.

By enhancing institutional capacity, Uzbekistan can effectively respond to the increasing volume and complexity of digital legal interactions and strengthen its role in the international legal order.

Adopting Lex Digitalis. The concept of Lex Digitalis, proposed by Koops (2020), envisions a transnational normative framework for regulating digital interactions across borders. Unlike traditional legal systems anchored in national sovereignty, Lex Digitalis is defined by technological environments, network architectures, and algorithmic governance. It offers a model for legal regulation in cyberspace that transcends state-centric approaches.

For Uzbekistan, embracing Lex Digitalis would require recognizing the need for a hybrid legal regime that incorporates both national and transnational norms. This could take the form of:

7. Adopting principles of interoperability between national digital laws and international standards;
8. Recognizing legal personality for digital agents such as smart contracts and autonomous AI systems under controlled conditions;
9. Enacting legislation that governs the use of distributed ledger technologies and ensures technological neutrality in digital dispute resolution.

Furthermore, Lex Digitalis promotes a risk-based regulatory framework where laws adapt dynamically to technological developments. Uzbekistan's legal system must become more agile and open to cross-border legal innovation. This transformation would position the country as a forward-thinking legal jurisdiction that not only regulates digital activity but also fosters its responsible growth.

Conclusion. Digital relations have irreversibly transformed the scope and substance of Private International Law. Traditional conflict-of-law rules, developed in an era of physical transactions and state-centric interactions, are now being tested by borderless, algorithmic, and decentralized legal realities. In this rapidly evolving landscape, legal certainty and coherence depend on the ability of states to modernize their legal frameworks and coordinate internationally.

For Uzbekistan, this means reimagining its Private International Law in light of digital transformations. Acceding to international conventions, modernizing domestic legal instruments, enhancing institutional capacities, and embracing innovative regulatory paradigms like Lex Digitalis are essential steps. Without such reform, Uzbekistan risks legal fragmentation, uncertainty in cross-border transactions, and diminished participation in the global digital economy.

The path forward lies in a synergistic approach—combining national innovation with international harmonization—to build a future-proof legal order that can effectively manage the complexities of digital relations under Private International Law.

REFERENCES

1. Bradshaw, S., Millard, C., & Walden, I. (2021). *Cloud computing law*. Oxford University Press.
2. Bygrave, L. A. (2017). *Internet governance by contract: The rise of a new contractual order for regulating online behavior*. Oxford University Press.
3. European Court of Justice. (2014). *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*. Case C-131/12.
4. Koops, B.-J. (2020). The concept of Lex Digitalis. *Computer Law & Security Review, 36*, 105–117.
5. Kuner, C. (2020). *Transborder data flows and data privacy law*. Oxford University Press.
6. UNCITRAL. (1996). *Model Law on Electronic Commerce*.
7. UNCITRAL. (2005). *United Nations Convention on the Use of Electronic Communications in International Contracts*.
8. Uzbekistan. (2004). Law on Electronic Commerce.
9. Uzbekistan. (2013). Law on Private International Law.
10. Uzbekistan. (2019). Law on Personal Data.
11. Hague Conference on Private International Law. (2005). *Convention on Choice of Court Agreements*.
12. Hague Conference on Private International Law. (2019). *Judgments Convention*.
13. UK Jurisdiction Taskforce. (2019). *Legal Statement on Cryptoassets and Smart Contracts*.