IRSHAD

INTERNATIONAL JOURNAL OF LAW AND POLICY

Modern form of Law Evasion in International Private Law under the Conditions of the Digital Economy and Mechanisms for Combating

[Sardor Berdibayev][1]

[1]*Tashkent State University of Law, Tashkent, Uzbekistan*

Keywords:

Law Evasion, Digital Economy, Cryptocurrency, Regulatory Arbitrage, Cross-Border Cooperation

ABSTRACT

The digital economy has fundamentally transformed traditional mechanisms of law evasion in international private law, creating unprecedented challenges for legal systems worldwide. This study examines modern forms of law evasion including regulatory arbitrage in cryptocurrency markets, forum shopping through virtual presence, and jurisdictional manipulation via smart contracts. Employing doctrinal legal analysis and comparative methodology, the research analyzes legislative frameworks across multiple jurisdictions. The findings reveal significant regulatory gaps enabling cross-border law evasion. The study proposes comprehensive mechanisms for combating these practices, including enhanced international cooperation and technological solutions.

How to Cite: Berdibayev, S. (2026). Modern form of Law Evasion in International Private Law under the Conditions of the Digital Economy and Mechanisms for Combating. *International Journal of Law and Policy, 4*(1), 55-79. https://doi.org/10.59022/ijlp.483

I. Introduction

The unprecedented expansion of the digital economy has fundamentally transformed the landscape of international private law, creating novel challenges that traditional legal frameworks were not designed to address. As technological innovations continue to reshape global commerce and communication, the mechanisms through which parties evade applicable laws have evolved correspondingly, exploiting the inherent tensions between territorial sovereignty and the borderless nature of digital technologies. The emergence of cryptocurrencies, smart contracts, decentralized finance platforms, and virtual business presence has created unprecedented opportunities for sophisticated forms of law evasion that transcend conventional regulatory boundaries. These developments necessitate comprehensive examination of how traditional legal doctrines must adapt to maintain their protective functions in an increasingly digitalized world.

International private law, traditionally concerned with determining applicable law, jurisdiction, and recognition of foreign judgments, now faces the complex task of adapting centuries-old doctrines to a digital environment where physical location becomes increasingly irrelevant. The fundamental conflict-of-law principles that emerged from the territorial sovereignty of nation-states encounter significant difficulties when applied to transactions occurring simultaneously across multiple jurisdictions or within decentralized networks that resist geographical localization. The traditional connecting factors of domicile, nationality, place of contracting, and place of performance lose much of their determinative power when parties can establish presence in multiple jurisdictions with minimal effort, when contracts can be concluded through automated protocols without identifiable negotiation location, and when performance occurs through distributed networks spanning the globe.

This transformation necessitates a comprehensive examination of how traditional forms of law evasion have adapted to digital contexts and what new mechanisms have emerged specifically within the digital economy. The stakes of this examination extend beyond academic interest to practical consequences for businesses, consumers, investors, and regulators worldwide. Ineffective responses to digital law evasion undermine the rule of law, create unfair competitive advantages for bad actors, and erode public confidence in legal institutions. Conversely, overly restrictive responses may stifle legitimate innovation and impose disproportionate compliance burdens on legitimate businesses attempting to operate across borders.

The concept of law evasion, known in civil law traditions as fraus legis or fraude à la loi, refers to the manipulation of connecting factors to avoid the application of otherwise mandatory legal provisions. Distinguished from legitimate forum shopping, which involves selecting among genuinely available forums, law evasion implies deliberate artificiality in creating or modifying the circumstances that determine applicable law or jurisdiction. Classical examples include changing domicile solely to obtain a divorce not available under the law of the original domicile, or incorporating a subsidiary in a jurisdiction with favorable corporate

law to escape mandatory provisions of the jurisdiction where business activities actually occur. In the digital economy, this distinction between legitimate choice and improper evasion becomes increasingly blurred as parties can establish virtual presence, relocate digital assets, or structure transactions through multiple intermediaries with relative ease (Petsche, 2011).

The borderless nature of the internet creates particular challenges for law evasion analysis. When a website can be accessed from any jurisdiction, a cryptocurrency transaction can be initiated from any location with internet access, and smart contract code executes on globally distributed nodes, the traditional assumption that activities have identifiable territorial connections loses much of its force. Parties operating in this environment face genuine uncertainty about which law applies to their activities, creating both legitimate planning challenges and opportunities for those seeking to exploit jurisdictional ambiguities. Regulators face corresponding difficulties in determining when their rules should apply and how to enforce them against actors who can operate from anywhere in the world.

Scholarly attention to law evasion in international private law has traditionally focused on classic scenarios involving changes of domicile to obtain favorable divorce laws, corporate reincorporation to escape mandatory shareholder protections, and contractual choice of law to avoid consumer protection regulations. The seminal works of Lorenzen established the doctrinal foundations for understanding when party manipulation of connecting factors should be deemed fraudulent and therefore ineffective. These foundational analyses recognized that party autonomy in private international law must be subject to limits preventing abuse, while also acknowledging the difficulty of distinguishing legitimate from illegitimate exercises of choice. Subsequent scholarship refined these principles, developing doctrinal frameworks for evaluating evasion claims across different legal traditions.

However, the existing literature has been slow to address the unique challenges posed by digital technologies, with comprehensive analyses of digital law evasion remaining relatively scarce until recent years. This gap reflects both the novelty of the phenomena and the interdisciplinary expertise required to analyze them competently. Legal scholars approaching digital technologies must understand not only traditional private international law doctrine but also the technical characteristics of blockchain systems, the economics of digital markets, and the practical operations of online platforms. This combination of knowledge has developed only gradually as digital technologies have matured and their legal implications have become clearer.

Recent scholarship has begun examining specific aspects of digital-era law evasion with increasing sophistication. Casino et al. (2024) provided significant insights into cross-border e-crimes and the jurisdictional challenges they present, emphasizing the difficulties of applying traditional due process protections in digital contexts. Their analysis demonstrates how the speed and anonymity of digital transactions complicate both the detection of law evasion and the enforcement of remedial measures. The pseudonymous nature of many digital activities creates particular challenges for determining party characteristics that may be relevant to

choice-of-law analysis, such as consumer status or habitual residence. These characteristics, traditionally verifiable through documentary evidence, become difficult to establish when parties interact through digital interfaces that may deliberately obscure identifying information.

Similarly, regulatory bodies including the International Organization of Securities Commissions (IOSCO, 2023) and the Financial Stability Board (FSB, 2025) have produced extensive reports on regulatory arbitrage in cryptocurrency markets, documenting how market participants exploit jurisdictional differences to minimize compliance obligations while maintaining global customer access. These reports reveal systematic patterns of jurisdiction shopping, with cryptocurrency businesses establishing presence in jurisdictions offering favorable regulatory treatment while serving customers in more restrictive jurisdictions through technological means. The consistency of these patterns across different markets and time periods suggests deliberate strategic behavior rather than merely responding to legitimate business considerations.

The Hague Conference on Private International Law has undertaken preliminary work on the implications of digital technologies for private international law, including analyses of digital tokens, central bank digital currencies, and distributed ledger technology. These institutional efforts recognize that existing international instruments may be inadequate for addressing digital-specific challenges, though concrete solutions remain under development. The Conference's preliminary documents identify key questions requiring resolution, including how traditional connecting factors should be adapted for digital contexts, whether new connecting factors specific to digital transactions should be developed, and how enforcement mechanisms can be made effective against digitally-enabled evasion. These questions frame an ongoing agenda that may ultimately produce new international instruments addressing digital private international law.

Within the specific context of Central Asian legal development, researchers have analyzed the modernization of payment systems and digital commerce regulations in transitional economies. Khudoyberganov's (2024) examination of Uzbekistan's Law on Payments and Payment Systems provides valuable insights into how transitional economies are developing legal frameworks for digital financial services, though the intersection with international private law evasion concerns remains underexplored. The broader literature on post-Soviet legal reform offers contextual understanding of how civil law systems adapt to technological change, revealing patterns of selective borrowing from established systems combined with locally-specific adaptations reflecting domestic conditions and policy priorities.

Despite growing awareness of the challenges posed by digital technologies to international private law, existing scholarship exhibits several significant limitations that this research addresses. First, treatments of law evasion tend to remain anchored in traditional categories without adequately theorizing how digital technologies have transformed both the mechanics and the scale of evasive practices. The classic scenarios of domicile change and corporate reincorporation, while still relevant, fail to capture the distinctive features of digital

law evasion including the speed of transactions, the pseudonymity of actors, the global reach of digital platforms, and the absence of traditional intermediaries who historically served gatekeeping functions. A comprehensive analytical framework addressing these distinctive features remains underdeveloped.

Regulatory analyses of specific sectors such as cryptocurrency or e-commerce often proceed without reference to the broader framework of private international law, missing opportunities to leverage established doctrines for addressing novel challenges. Regulatory reports from bodies like IOSCO and FSB provide valuable empirical documentation of evasive practices but typically frame their analyses in terms of regulatory compliance rather than private international law concepts. This separation obscures connections between regulatory arbitrage and traditional law evasion doctrine that could inform more effective responses. Integrating these perspectives enables recognition that digital regulatory arbitrage represents a contemporary manifestation of long-recognized law evasion patterns, suggesting that traditional doctrinal tools may be adaptable rather than entirely obsolete.

Comparative analyses frequently neglect developing and transitional economies, creating blind spots regarding how law evasion manifests in different regulatory environments. The concentration of legal scholarship in developed Western jurisdictions means that experiences of countries like Uzbekistan in confronting digital law evasion remain largely undocumented in the international legal literature. Yet these jurisdictions face distinctive challenges arising from their position in the global regulatory landscape, often experiencing digital activities as recipients of services originating elsewhere rather than as originators themselves. Understanding these perspectives is essential for developing truly global responses to inherently global phenomena.

The primary aim of this research is to analyze modern forms of law evasion in international private law as they manifest within the digital economy and to propose effective mechanisms for combating such practices. This aim reflects recognition that digital technologies have created both new evasion opportunities and new tools for combating evasion, requiring comprehensive analysis of both dimensions. Effective response requires understanding not only the mechanisms of evasion but also the legitimate interests that overly broad responses might impair, including innovation, privacy, and efficient cross-border commerce.

To achieve this aim, the study pursues several specific objectives. First, it seeks to develop a comprehensive typology of digital-era law evasion forms, distinguishing between adaptations of traditional mechanisms and novel forms enabled by new technologies. This typology provides analytical framework for categorizing and understanding the diverse phenomena that fall under the general category of digital law evasion. Second, it analyzes the regulatory frameworks governing digital transactions in selected jurisdictions, identifying gaps and inconsistencies that create opportunities for law evasion. Understanding these gaps is prerequisite to developing effective responses. Third, it examines existing international

cooperation mechanisms and proposes enhancements tailored to digital challenges. Given the inherently cross-border nature of digital activities, cooperation mechanisms are essential to effective enforcement. Fourth, it evaluates technological solutions that may complement legal measures in detecting and preventing law evasion, recognizing that responses to digital challenges may themselves require digital tools.

This research addresses the following central questions that together constitute a comprehensive inquiry into digital law evasion: How have traditional forms of law evasion in international private law transformed within the digital economy? What novel mechanisms of law evasion have emerged specifically as a result of digital technologies such as cryptocurrencies, smart contracts, and decentralized platforms? What regulatory gaps and inconsistencies across jurisdictions create opportunities for digital law evasion? What mechanisms, both legal and technological, can effectively combat modern forms of law evasion while preserving legitimate commercial activities? How can international cooperation frameworks be enhanced to address the cross-border nature of digital law evasion? These questions guide the analysis through examination of phenomena, causes, and potential responses.

This research contributes to legal scholarship and practice in several important respects that justify the comprehensive treatment undertaken. Theoretically, it advances understanding of how fundamental private international law concepts require reconceptualization for digital contexts, offering a framework that bridges traditional doctrine with contemporary technological realities. The analysis demonstrates that core concepts of law evasion remain relevant in digital contexts but require adaptation to account for distinctive features of digital technologies. This theoretical contribution supports ongoing scholarly efforts to develop private international law doctrine adequate for digital commerce while maintaining continuity with established principles.

It provides guidance for regulators, practitioners, and policymakers engaged in developing responses to digital law evasion, identifying both best practices and approaches that have proven ineffective. Regulators can benefit from understanding how their frameworks compare with those of other jurisdictions and where gaps create arbitrage opportunities. Practitioners advising clients on cross-border digital transactions require understanding of how law evasion doctrines may apply to digital structures. Policymakers considering legislative reforms benefit from comparative analysis identifying effective approaches implemented elsewhere.

It contributes to understanding how jurisdictions at different developmental stages experience similar challenges, potentially informing legal reform efforts in transitional economies. The inclusion of Uzbekistan alongside established jurisdictions demonstrates that digital law evasion presents global challenges affecting all countries regardless of their developmental level. Countries undertaking digital legal modernization can learn from both the successes and failures of earlier adopters, while recognizing that local conditions may

require adaptation of borrowed approaches. The findings have particular relevance for ongoing international harmonization efforts, including the work of the Hague Conference and various regulatory standard-setting bodies attempting to develop coordinated global responses to inherently global challenges

II. Methodology

This study employs a qualitative research design combining doctrinal legal analysis with comparative methodology, an approach well-established in legal scholarship for examining complex regulatory phenomena across jurisdictions. The doctrinal approach involves systematic examination of legal texts, including primary sources such as legislation, regulations, and international instruments, as well as secondary sources including judicial decisions, scholarly commentary, and regulatory guidance. This methodology is particularly appropriate for analyzing the legal frameworks governing digital transactions and identifying how existing doctrines apply or fail to apply to novel situations created by digital technologies.

The doctrinal method proceeds through several analytical stages. Initial examination identifies the formal legal rules applicable to digital transactions in each jurisdiction examined. Subsequent analysis examines how these rules have been interpreted and applied in practice, drawing on case law where available and regulatory guidance where judicial decisions remain limited. Critical analysis evaluates the adequacy of existing rules for addressing identified challenges, considering both their formal scope and their practical enforceability. Normative analysis considers how rules should be reformed to address identified gaps while preserving legitimate interests.

The comparative legal methodology examines how different jurisdictions approach similar problems, enabling identification of patterns, best practices, and regulatory gaps. Functional comparison focuses on how different systems address the same underlying challenge of preventing law evasion, regardless of the formal categories employed. This functional approach recognizes that superficially different legal concepts may serve similar purposes, while apparently similar concepts may function quite differently in their respective legal systems. The functional perspective enables meaningful comparison across legal traditions that employ different doctrinal vocabularies.

This approach recognizes that legal rules operate within broader social, economic, and institutional contexts that affect their meaning and impact, requiring attention to implementation and enforcement realities beyond formal legal provisions. A rule that appears adequate on paper may prove ineffective in practice due to enforcement limitations, while a rule that appears limited may be rendered effective through creative interpretation and vigorous enforcement. Contextual analysis considers these practical dimensions alongside formal legal analysis.

Primary legal sources examined in this study include major international and regional instruments governing digital transactions and private international law. The European Union's Markets in Crypto-Assets Regulation (MiCA) provides comprehensive framework for cryptocurrency regulation that represents the most developed approach among the jurisdictions examined. The Budapest Convention on Cybercrime provides the primary international framework for cooperation regarding computer-related offenses, including provisions for mutual legal assistance and evidence preservation. The Rome I Regulation on applicable law and the Brussels I bis Regulation on jurisdiction provide the European framework for private international law that serves as reference point for comparative analysis.

National legislation examined includes Uzbekistan's Law on Payments and Payment Systems (Law No. LRU-578 of 2019), which established comprehensive framework for electronic payments and demonstrates how transitional economies approach digital finance regulation. The Civil Code provisions governing electronic transactions provide doctrinal foundation for private law analysis. Comparative materials include relevant legislation from the United States demonstrating fragmented regulatory approaches and the European Union demonstrating harmonized approaches. International instruments from organizations including the Hague Conference on Private International Law, UNCITRAL, IOSCO, and the Financial Action Task Force provide additional primary source material regarding international standards and cooperation mechanisms.

Secondary sources include peer-reviewed scholarship on international private law, digital asset regulation, and cybercrime, accessed through established academic databases including Scopus, Web of Science, and Google Scholar. Selection criteria prioritized scholarly works published in recognized journals, with preference for recent publications given the rapidly evolving nature of digital technology regulation while also including foundational doctrinal works providing theoretical grounding. Reports and guidance from regulatory bodies including the Financial Stability Board, IOSCO, and Eurojust provide important empirical context regarding implementation challenges and enforcement experiences that complement academic analysis.

The comparative analysis focuses on three distinct regulatory environments that together illustrate the range of approaches to digital law evasion and the challenges each presents. The European Union serves as supranational legal system with comprehensive digital regulation, offering the most developed harmonized framework through instruments such as MiCA, GDPR, and the Rome/Brussels Regulations. The EU approach demonstrates both the potential and limitations of harmonized regulatory responses to cross-border digital activities.

The United States serves as major common law jurisdiction with significant regulatory activity but fragmented approaches across federal and state levels. Multiple federal agencies assert overlapping jurisdiction, while states maintain varying regulatory requirements creating internal arbitrage opportunities. This fragmentation illustrates challenges of coordinating

regulatory response within federal systems and the arbitrage opportunities that inconsistency creates.

Uzbekistan serves as representative developing economy undertaking digital legal modernization, demonstrating how transitional economies balance innovation promotion with protection against abuse. The relatively recent adoption of comprehensive payment systems legislation provides opportunity to examine purposive regulatory design informed by international standards and experience of earlier adopters. This selection enables examination of how different types of legal systems at different developmental stages approach digital law evasion challenges.

The analysis proceeds through several stages designed to build comprehensive understanding of digital law evasion phenomena and potential responses. First, traditional forms of law evasion are examined to establish baseline understanding of doctrinal categories and their rationale. This historical foundation ensures that analysis of digital phenomena remains grounded in established private international law concepts while also identifying where traditional concepts may require modification.

Several limitations affect the scope and conclusions of this research that merit acknowledgment. The rapidly evolving nature of digital technology regulation means that legal frameworks continue to develop, potentially affecting the currency of specific provisions analyzed. New legislation, regulatory guidance, and judicial decisions may alter the landscape described here. Readers should verify current status of specific rules before relying on this analysis for practical purposes.

The comparative scope, while including diverse jurisdictions, cannot comprehensively cover all relevant legal systems, and findings may not fully generalize to jurisdictions with significantly different legal traditions or developmental contexts. The selection of jurisdictions reflects pragmatic considerations including availability of sources and language accessibility alongside substantive representativeness. Access to empirical data regarding actual law evasion practices is inherently limited given their illicit nature, requiring reliance on regulatory reports and documented cases that may not fully represent the phenomenon. These limitations are acknowledged as inherent to the subject matter and do not diminish the value of the analytical framework and recommendations developed.

III. Results

A. Traditional Forms of Law Evasion in Digital Contexts

Analysis of primary and secondary sources reveals that traditional forms of law evasion have adapted to digital environments in several distinct ways, exhibiting both continuity with historical patterns and significant transformation in their mechanics and scale. The foundational concept of fraus legis, involving artificial manipulation of connecting factors to evade mandatory rules, persists in digital contexts but operates through new mechanisms that

exploit the features of digital technologies. These adaptations demonstrate the resilience of evasive behavior, which tends to exploit whatever opportunities available technologies provide.

Traditional forum shopping involved selecting among genuinely available forums based on their favorable procedural rules, substantive law, or enforcement prospects. The practice is not inherently improper; parties legitimately may prefer forums offering efficient procedures, developed commercial law, or experienced judiciary. However, this legitimate choice becomes problematic when parties artificially create connections to forums they would not otherwise have access to, or when selection is motivated solely by desire to evade mandatory rules that would otherwise apply.

Digital technologies have transformed this practice by dramatically reducing the costs and practical difficulties of establishing presence in multiple jurisdictions simultaneously. Virtual offices, cloud-based operations, and remote employment enable businesses to establish plausible connections to favorable jurisdictions without significant physical presence, blurring the distinction between legitimate choice and artificial manipulation (Petsche, 2011). Where establishing foreign presence previously required significant investment in facilities, personnel, and local relationships, digital presence can be established through relatively minimal expenditure on domain registration, virtual office services, and remote contractors.

The research identified several patterns of digital forum shopping that recur across different markets and regulatory contexts. First, cryptocurrency exchanges frequently incorporate in jurisdictions with minimal regulatory requirements while serving customers globally through digital platforms. The operational presence in the favorable jurisdiction may be minimal, consisting of registered offices and necessary corporate filings, while actual business activities are conducted remotely by personnel located elsewhere. Customers access services through internet interfaces that obscure the jurisdictional structure underlying service provision.

Data processing operations are located based on favorable privacy regimes, with data routing technologies enabling choice of applicable law through technical configurations. The GDPR's broad territorial reach has prompted some businesses to structure operations to minimize EU nexus, routing data through non-EU servers and limiting processing activities within EU territory. Whether such arrangements constitute legitimate business planning or improper evasion depends on factors including the genuineness of non-EU operational presence and the degree to which arrangements appear designed primarily to avoid EU rules.

Dispute resolution clauses in online contracts increasingly specify arbitration in jurisdictions favorable to the drafting party, with the absence of physical negotiation making such clauses less visible to counterparties. Consumer contracts often contain arbitration clauses specifying proceedings in jurisdictions distant from consumers' residence, with governing law selected based on favorability to the drafting party. While arbitration clauses enjoy general enforceability under international conventions, their use to evade consumer

protection laws available in consumers' home jurisdictions raises policy concerns that courts have addressed inconsistently. Casino et al. (2024) documented how these practices create significant challenges for law enforcement and regulatory authorities attempting to apply territorial legal frameworks.

Choice of law clauses have long presented opportunities for evasion of mandatory rules, with doctrines such as Article 9 of the Rome I Regulation preserving overriding mandatory provisions of forum law regardless of party choice. These protective doctrines recognize that unlimited party autonomy would enable circumvention of rules reflecting important policy choices that states are unwilling to allow parties to avoid through contract. Consumer protection, employment law, and certain financial regulations exemplify such mandatory rules that cannot be displaced by contrary party agreement.

Digital contexts complicate application of these protective mechanisms in several ways that reduce their practical effectiveness. Online contracts typically present choice of law provisions as non-negotiable terms, often buried within lengthy terms of service that users accept without meaningful review. Empirical research consistently demonstrates that virtually no consumers read complete terms of service, meaning that choice of law provisions operates without genuine consent even though formally included in accepted terms. The global reach of digital platforms means that a single set of terms may govern transactions across dozens of legal systems, each with different mandatory rules that parties might legitimately seek to apply.

The analysis revealed particular concerns regarding consumer protection and employment law in digital contexts. Digital platforms routinely characterize service providers as independent contractors governed by commercially favorable law, avoiding employment protections that would apply under many national systems. The gig economy has generated extensive litigation regarding worker classification, with outcomes varying by jurisdiction and creating incentives for platforms to establish presence in jurisdictions with classifications favorable to contractor treatment. Similarly, consumer-facing platforms select governing law based on least restrictive consumer protection regimes while serving consumers in jurisdictions with more protective rules.

While traditional conflict-of-law analysis would preserve application of mandatory consumer and employment protections regardless of contractual choice, practical enforcement barriers often prevent effective remedy, particularly for low-value individual claims. The costs of litigating in foreign forums or compelling application of home-country law typically exceed the value of individual consumer transactions, leaving contractual choice effectively unremedied. Class action mechanisms that might aggregate individual claims face their own cross-border enforcement challenges, and platforms' arbitration clauses often preclude collective proceedings.

Traditional corporate law evasion involved reincorporation or use of subsidiary structures to access favorable legal regimes while conducting actual business activities elsewhere. The selection of Delaware as incorporation jurisdiction by companies with no

Delaware operations exemplifies this practice, which courts have generally accepted as legitimate despite its transparent regulatory motivation. The principle that corporations are governed by the law of their state of incorporation creates inherent potential for jurisdiction shopping that traditional doctrine has largely tolerated.

Digital businesses have refined these techniques through complex multi-jurisdictional structures that separate intellectual property holding, operational activities, and revenue recognition across multiple entities in different jurisdictions. The intangible nature of digital assets facilitates these arrangements, as software, data, and digital rights can be contractually allocated among related entities regardless of where economic activities actually occur. The locational indeterminacy of digital assets makes allocation among jurisdictions largely a matter of contractual designation rather than economic reality.

The research documented prevalent use of structures involving holding companies in low-tax or low-regulation jurisdictions, operating subsidiaries in jurisdictions with favorable employment and consumer law, and intellectual property vehicles in regimes offering advantageous treatment of intangibles. Large technology companies have attracted particular attention for structures that allocate profits to low-tax jurisdictions through intercompany arrangements involving intellectual property licensing and cost-sharing. While such structures may have legitimate business purposes, they also create opportunities for regulatory arbitrage by selecting the most favorable legal environment for each aspect of operations.

The determination of when such structures constitute improper evasion rather than legitimate planning remains contested, with different jurisdictions applying varying standards. General anti-avoidance doctrines exist in many jurisdictions but are applied with varying rigor and may be difficult to invoke regarding structures that follow formal legal requirements. The substance-over-form approach that might address purely artificial arrangements encounters difficulty when structures include some genuine economic activity in each jurisdiction, even if the allocation of activities appears motivated primarily by regulatory considerations.

B. Novel Forms of Digital Law Evasion

Beyond adaptation of traditional mechanisms, the digital economy has enabled entirely novel forms of law evasion that exploit unique features of digital technologies not present in earlier commercial environments. These novel forms present particular challenges because existing legal frameworks often lack applicable rules or enforcement mechanisms designed for the phenomena they address. The novelty of these mechanisms creates uncertainty regarding both their legal characterization and the appropriate regulatory response.

Cryptocurrency markets present among the most significant contemporary challenges for private international law, combining multiple features that complicate regulatory application. The pseudonymous nature of blockchain transactions obscures party identity while remaining publicly visible on the blockchain. The absence of traditional financial intermediaries removes gatekeepers who historically enforced regulatory compliance. The

global and continuous operation of cryptocurrency markets means that transactions occur without interruption across all time zones, making territorial boundaries largely irrelevant to market operation.

The Financial Stability Board's 2025 thematic review documented extensive regulatory arbitrage in cryptocurrency markets, with service providers exploiting inconsistent approaches across jurisdictions to minimize compliance obligations while maintaining global customer access. The review found that uneven implementation of international standards creates opportunities for regulatory arbitrage and complicates oversight of inherently global markets. Service providers establish formal presence in permissive jurisdictions while serving customers globally, with technological measures potentially circumventing geographic restrictions that regulators attempt to impose.

Specific patterns of cryptocurrency-related law evasion identified in this research include establishment of exchanges in jurisdictions lacking licensing requirements while serving customers in regulated markets through technological circumvention of geographic restrictions. Exchanges may claim not to serve customers in particular jurisdictions while taking minimal measures to verify customer location, knowing that determined users can easily circumvent geographic restrictions through VPNs and other tools. The practical difficulty of enforcing geographic restrictions creates tacit tolerance of non-compliance that undermines regulatory effectiveness.

Use of stablecoins to facilitate cross-border value transfer outside regulated banking channels enables evasion of anti-money laundering controls and currency regulations. Stablecoins purport to maintain stable value relative to fiat currencies, enabling their use as payment mechanism without the volatility that limits utility of other cryptocurrencies for ordinary transactions. Their use for cross-border transfers circumvents traditional correspondent banking relationships that historically provided points of regulatory control. Structuring of token offerings to avoid securities law by exploiting differences in how jurisdictions classify digital assets enables capital raising without compliance with investor protection requirements that would apply to conventional securities offerings.

The IOSCO (2023) policy recommendations acknowledged these challenges, calling for enhanced cross-border cooperation and consistent regulatory approaches. The recommendations emphasized that crypto-asset service providers should be subject to comprehensive regulation addressing investor protection, market integrity, and financial stability concerns regardless of the technological form of their activities. However, implementation of these recommendations remains uneven, with the FSB review documenting significant gaps and inconsistencies that persist across jurisdictions.

Smart contracts, self-executing code deployed on blockchain networks, present unique law evasion challenges arising from their automated execution and distributed nature. The term refers to computer code that automatically executes specified actions when predetermined conditions are satisfied, without human intervention in the execution process.

Unlike traditional contracts with identifiable parties, signing location, and place of performance, smart contracts may be deployed by pseudonymous parties whose real-world identities remain unknown. Execution occurs through nodes distributed globally, with no single location where the contract can be said to perform. These characteristics create jurisdictional ambiguity that complicates application of traditional conflict-of-law rules.

The research identified several specific mechanisms through which smart contracts facilitate law evasion. Automated execution prevents intervention that traditional contract law would permit when changed circumstances make performance unjust. Once deployed, smart contract code executes according to its programming regardless of changed circumstances that would justify modification or excuse under traditional contract doctrine. The impossibility, frustration, and unconscionability doctrines that protect parties in traditional contracts lack clear application to automated execution.

Immutability of deployed code prevents modification even when contracts prove to contain illegal provisions or terms that courts would strike down in traditional contracts. While some smart contracts include upgrade mechanisms, many are designed to be immutable once deployed, continuing to execute regardless of subsequent legal determinations regarding their validity. Pseudonymous deployment obscures the identity of parties, preventing application of rules that depend on party characteristics such as consumer status. The consumer protections available under many legal systems depend on ability to identify consumers, which pseudonymous systems deliberately frustrate.

The Harvard Law School Forum on Corporate Governance has analyzed how these features challenge traditional contract law assumptions, noting that existing legal frameworks provide limited guidance for determining which law governs smart contract disputes and how mandatory rules should be applied to automated execution. The autonomous character of smart contracts, combined with their distributed execution and pseudonymous participation, creates a genuinely novel phenomenon that traditional conflict-of-law doctrine was not designed to address.

Decentralized finance (DeFi) protocols represent a particularly challenging frontier for law evasion analysis, pushing the novel characteristics of digital technologies to their logical extremes. These protocols provide financial services including lending, borrowing, trading, and derivatives through smart contracts without traditional financial intermediaries. Users interact directly with protocol code rather than with identified service providers, accessing services through permissionless interfaces that do not require registration or identification.

The absence of identifiable service providers creates fundamental difficulties for regulatory frameworks premised on licensed intermediaries subject to territorial jurisdiction. Traditional financial regulation operates through licensed entities that serve as points of regulatory control, ensuring compliance with investor protection, prudential, and anti-money laundering requirements. DeFi protocols eliminate these intermediaries, leaving only protocol code and its users as potential regulatory subjects. Governance may be distributed among

token holders who are globally dispersed and pseudonymous, without any entity exercising control sufficient to make it a viable regulatory target.

The research documented how DeFi protocols enable evasion of securities regulation through token structures designed to avoid classification as securities. The characteristics that distinguish securities from other assets remain contested in the cryptocurrency context, with different jurisdictions reaching different conclusions and creating opportunities to structure offerings to minimize securities law exposure. Evasion of banking regulation through automated lending without licensed intermediaries removes prudential oversight designed to ensure financial system stability. Evasion of anti-money laundering requirements through permissionless protocols lacking customer identification eliminates controls designed to detect and prevent illicit financial flows.

Regulatory responses to DeFi remain nascent, with the EU's MiCA Regulation providing initial frameworks but significant gaps remaining, particularly regarding fully decentralized protocols without identifiable governance. The regulation focuses on crypto-asset service providers, a concept that may not apply to protocols that operate without any entity controlling their operation. This gap reflects the genuine difficulty of regulating autonomous systems that continue to operate without any identified controller, a challenge that existing regulatory paradigms are not designed to address.

The increasing feasibility of conducting business activities through purely virtual presence, combined with growing digital nomadism among workers, creates additional law evasion opportunities that exploit assumptions of fixed location embedded in traditional legal frameworks. Traditional connecting factors such as domicile, residence, and place of business assumed relatively fixed physical presence that could be verified and that created genuine connections to territorial legal systems. Virtual presence enables establishment of formal connections to favorable jurisdictions through virtual offices, registered agents, and digital incorporation services without meaningful economic activity in those jurisdictions.

Digital nomads who work remotely while traveling internationally present particular challenges for employment law and tax residence rules designed for sedentary populations. The research identified practices including claiming residence in no-tax or low-regulation jurisdictions while physically present elsewhere, structuring employment through entities in favorable jurisdictions regardless of where work is actually performed, and using virtual private networks and other technologies to obscure actual location from counterparties and authorities.

These practices exploit gaps in international coordination regarding digital presence and create enforcement challenges when actual physical location cannot be readily determined. Residence rules designed to identify a single primary location encounter difficulty with individuals who move frequently and may not establish stable presence anywhere. Employment law depending on identification of workplace faces challenge when work is performed remotely from varying locations. The traditional assumption that location can be

determined creates vulnerability when digital technologies make location indeterminate or manipulable.

C. Regulatory Framework Analysis

The European Union has developed the most comprehensive regulatory framework for digital assets and services among the jurisdictions examined, reflecting both its institutional capacity for harmonized regulation and its policy commitment to addressing digital technology challenges through comprehensive legal frameworks. The Markets in Crypto-Assets Regulation (MiCA), which entered into full application in December 2024, establishes licensing requirements for crypto-asset service providers, conduct of business rules, and investor protection measures designed to create a comprehensive framework for cryptocurrency activities within EU territory.

MiCA applies to crypto-asset service providers operating within the EU regardless of where they are established, with third-country providers required to establish EU branches or subsidiaries to serve EU customers. This approach asserts regulatory authority based on customer location rather than provider location, reflecting recognition that territorial regulation of providers is insufficient when providers can operate from anywhere to serve customers everywhere. The regulation covers a range of activities including custody, trading, exchange, and advisory services, with tailored requirements reflecting different risk profiles.

The research identified several strengths in the EU approach that other jurisdictions might consider emulating. Harmonized rules across member states reduce opportunities for intra-EU regulatory arbitrage that would otherwise arise from inconsistent national approaches. The single licensing framework enables providers authorized in one member state to operate throughout the EU, creating efficient single market while maintaining comprehensive regulation. Clear licensing requirements provide legal certainty for compliant operators while enabling enforcement against unlicensed activities. Conduct of business rules address specific risks of crypto-asset markets including custody, conflicts of interest, and market abuse.

However, limitations were also identified that qualify the EU approach as model for other jurisdictions. The regulation provides limited coverage of decentralized protocols without identifiable operators, reflecting the difficulty of regulating autonomous systems discussed above. Cross-border enforcement against non-EU entities remains challenging despite formal extraterritorial application, as service providers outside EU jurisdiction may continue operating with limited practical consequence. The pace of regulatory development continues to lag technological innovation, creating potential gaps regarding emerging technologies that the regulatory framework does not address.

The United States presents a fragmented regulatory landscape characterized by overlapping federal agencies and varying state-level approaches, creating both compliance challenges for legitimate businesses and opportunities for regulatory arbitrage by sophisticated

actors. Multiple federal agencies assert jurisdiction over aspects of digital asset markets, with the Securities and Exchange Commission regarding securities-like tokens, the Commodity Futures Trading Commission regarding derivatives and some spot markets, the Financial Crimes Enforcement Network regarding anti-money laundering, and the Office of the Comptroller of the Currency regarding bank custody of digital assets.

This fragmentation creates overlapping and potentially inconsistent requirements that complicate compliance for businesses operating across multiple asset types or service categories. A single enterprise may face regulatory requirements from multiple federal agencies applying different standards to different aspects of its operations. The boundaries between agency jurisdictions remain contested, with ongoing litigation regarding whether particular assets constitute securities subject to SEC oversight or commodities subject to CFTC oversight. This uncertainty creates compliance challenges while also enabling creative structuring designed to minimize regulatory burden.

State-level variation adds additional complexity to the US regulatory landscape. States including New York have imposed comprehensive licensing requirements through BitLicense and similar frameworks, while other states maintain minimal regulation of cryptocurrency activities. The research documented how this variation enables charter shopping, with digital asset businesses selecting state incorporation and licensing based on favorability of regulatory requirements. Businesses may establish presence in permissive states while serving customers nationally, exploiting the absence of federal preemption.

Recent federal legislative proposals including the Financial Innovation and Technology for the 21st Century Act represent efforts to provide clearer federal framework that would address fragmentation concerns. However, enactment remains uncertain and comprehensive reform has proven elusive, with persistent disagreement regarding appropriate regulatory approach and allocation of jurisdiction among federal agencies. The continuing uncertainty creates planning challenges for legitimate businesses while also perpetuating arbitrage opportunities that more coordinated regulation would eliminate.

Uzbekistan's approach to digital finance regulation reflects the challenges facing developing economies seeking to modernize legal frameworks while managing risks associated with digital technologies. As a transitional economy undertaking comprehensive legal reform, Uzbekistan has developed digital finance regulation informed by international standards while adapting to local conditions and developmental priorities. The regulatory approach balances goals of promoting innovation and financial inclusion with protection against risks including money laundering, fraud, and consumer harm.

The Law on Payments and Payment Systems (Law No. LRU-578 of 2019) established a comprehensive framework for electronic payments and payment service providers, with the Central Bank of Uzbekistan exercising supervisory authority over the payment system. Khudoyberganov (2024) analyzed how this framework addresses electronic money, payment operators, and payment agents, noting its alignment with international standards while

maintaining features adapted to local conditions. The framework establishes licensing requirements for payment service providers, conduct requirements addressing consumer protection and operational risk, and Central Bank supervisory authority to monitor compliance.

Significantly, the Law on Payments and Payment Systems explicitly excludes cryptocurrency transactions from its scope, reflecting deliberate policy choice to address crypto-assets through separate regulatory treatment. This exclusion acknowledges the distinct characteristics of cryptocurrencies that may require different regulatory approach than electronic fiat money, while deferring comprehensive cryptocurrency regulation to subsequent legislative development. Subsequent regulatory developments have established frameworks for cryptocurrency exchanges and related activities, though these remain less comprehensive than frameworks in jurisdictions such as the EU.

The 2023 launch of the National Payment System represented significant infrastructure development supporting digital payment modernization, creating integrated platform for processing digital payments throughout Uzbekistan. This infrastructure investment reflects recognition that regulatory frameworks require operational infrastructure to be effective, and that financial system modernization requires coordinated development of both. The research identified both opportunities and risks in Uzbekistan's approach: relatively permissive treatment of certain digital asset activities may attract legitimate innovation but also creates potential for arbitrage by actors seeking to evade stricter requirements in their home jurisdictions.

D. Cross-Border Cooperation Mechanisms

Effective response to digital law evasion requires robust international cooperation given the inherently cross-border nature of digital transactions that makes purely territorial regulation insufficient. No single jurisdiction can effectively regulate activities that occur across borders, involve actors in multiple countries, and exploit differences among national regulatory frameworks. The research examined existing cooperation mechanisms and identified both strengths and significant gaps that limit their effectiveness.

The Budapest Convention on Cybercrime provides the primary international framework for cooperation regarding computer-related offenses, with provisions for mutual legal assistance, extradition, and expedited preservation of digital evidence. The Convention has achieved broad ratification including by many non-Council of Europe states, creating widespread framework for cooperation. Eurojust (2020) documented the operational use of these mechanisms in cross-border cybercrime cases, noting both successful cooperation enabling prosecutions and persistent challenges limiting effectiveness.

Key limitations of existing cooperation mechanisms identified in the research include time delays inherent in mutual legal assistance processes that prove incompatible with the speed of digital transactions. Traditional mutual legal assistance procedures may require

months to execute, during which time digital assets can be transferred and evidence can be destroyed. Gaps in geographic coverage leave important jurisdictions outside international frameworks, creating potential safe havens for actors seeking to evade regulation. Limited cooperation regarding regulatory matters not rising to the level of criminal conduct leaves civil and administrative enforcement largely dependent on territorial jurisdiction.

Practical difficulties in executing requests across jurisdictions with different legal traditions and technical capabilities further limit effectiveness. Requesting authorities may lack understanding of legal requirements in executing jurisdictions, submitting requests that cannot be fulfilled. Executing authorities may lack technical capacity to gather digital evidence or may be unfamiliar with the technologies involved. The Financial Action Task Force guidance on virtual asset service providers addresses some cooperation needs regarding anti-money laundering, but broader regulatory cooperation regarding digital law evasion remains underdeveloped.

IV. Discussion

The findings of this research have significant implications for private international law theory that merit careful consideration by scholars and reformers. Traditional doctrines addressing law evasion developed within a framework assuming that connecting factors possessed objective, verifiable character and that manipulation required meaningful effort and commitment. A party changing domicile to obtain divorce law unavailable in the original domicile had to relocate physically, establishing new residence that created genuine connections to the new jurisdiction even if the relocation was motivated by desired legal consequences.

The territorial sovereignty of states provided the foundation for conflict-of-law rules that allocated regulatory authority based on geographic connections. States possessed authority to regulate persons and transactions within their territory, with private international law rules determining which state's authority applied when persons or transactions had connections to multiple states. This territorial foundation assumed that meaningful territorial connections could be identified and that activities could be located within state boundaries.

Digital technologies fundamentally challenge these assumptions by enabling easy, reversible, and potentially undetectable manipulation of factors that determine applicable law and jurisdiction. Virtual presence can be established and terminated with minimal cost and effort. Digital assets can be transferred across jurisdictions instantaneously. Automated systems can execute transactions without human intervention that might be localized. These characteristics undermine the assumption that connecting factors reflect genuine relationships between persons, transactions, and jurisdictions.

The concept of fraus legis requires reconceptualization for digital contexts that accounts for these changed conditions. The traditional requirement of artificial or fraudulent intent

becomes difficult to apply when digital structures can be established with minimal effort and may serve multiple legitimate purposes alongside evasive ones. A business establishing virtual presence in a favorable jurisdiction may genuinely conduct some activities there while also benefiting from favorable regulatory treatment. The mixed purposes complicate determination of whether the structure should be deemed fraudulent.

The research findings support scholarly arguments for effects-based approaches that determine applicable law and jurisdiction based on where transactions have impact rather than where parties or activities are formally located. Such approaches better reflect the realities of digital commerce where the same activity may simultaneously affect persons in multiple jurisdictions regardless of the formal location of the service provider. Effects-based approaches also align with policy goals of protecting those affected by activities regardless of the technological means through which activities are conducted.

However, effects-based approaches also raise concerns regarding legal certainty and the proliferation of potentially applicable laws, requiring careful calibration to avoid creating their own problems. If activities are subject to the law of every jurisdiction where they have effects, businesses may face compliance obligations under numerous legal systems with potentially conflicting requirements. The resulting uncertainty may chill legitimate activities alongside illegitimate ones, imposing costs that outweigh the benefits of enhanced protection against evasion.

The comparative regulatory analysis reveals important considerations for designing effective responses to digital law evasion that balance competing concerns. The EU's MiCA Regulation demonstrates the potential for comprehensive, harmonized frameworks that reduce opportunities for regulatory arbitrage within their geographic scope. The harmonized approach ensures that regulatory requirements apply consistently throughout the EU market, preventing races to the bottom among member states and ensuring that compliance in one member state enables operation throughout the EU.

However, the research also revealed limitations of even comprehensive frameworks when confronted with truly decentralized technologies and actors operating from outside regulated jurisdictions. MiCA's focus on crypto-asset service providers encounters difficulty when activities are conducted through autonomous protocols without identifiable service providers. Enforcement against non-EU actors remains challenging when they can continue operating without practical consequence. These limitations suggest that regulatory design must account for the practical limits of territorial regulation in digital contexts.

The principle of technological neutrality, while valuable for ensuring frameworks remain applicable as technologies evolve, must be balanced against the need for targeted rules addressing specific mechanisms of law evasion enabled by particular technologies. Generic rules that apply regardless of technological implementation may fail to address distinctive risks that particular technologies create. The research findings support hybrid approaches combining general principles applicable across technologies with specific provisions

addressing known evasion mechanisms in areas such as cryptocurrency, smart contracts, and decentralized platforms.

The contrast between the US fragmented approach and EU harmonization reveals tradeoffs between regulatory experimentation and arbitrage prevention that policymakers must navigate. Regulatory fragmentation may enable innovation by allowing different approaches to be tested, with successful approaches potentially spreading while unsuccessful ones are abandoned. However, fragmentation simultaneously creates opportunities for regulatory arbitrage that undermine the effectiveness of any jurisdiction's rules. For digital markets with inherently global reach, the costs of fragmentation appear to outweigh benefits, supporting international harmonization efforts.

Even well-designed regulatory frameworks prove ineffective without adequate enforcement mechanisms, making enforcement considerations central to any discussion of combating digital law evasion. The research identified several enforcement challenges specific to digital law evasion that existing enforcement mechanisms struggle to address. The speed of digital transactions exceeds the capacity of traditional enforcement processes, with assets potentially transferred or dissipated before authorities can act. Cryptocurrency transactions settle within minutes or hours, while traditional enforcement measures may require weeks or months to implement.

Pseudonymous technologies impede identification of violators and connection to territorial jurisdiction on which enforcement depends. Decentralized structures create uncertainty regarding proper enforcement targets when no single entity controls protocol operation. Cross-border enforcement requires cooperation from jurisdictions that may lack capacity, legal authority, or willingness to assist. These challenges are structural features of digital technologies that cannot be eliminated but must be accommodated in enforcement design.

Several enforcement mechanisms show promise for addressing these challenges. Blockchain analytics tools enable tracing of cryptocurrency transactions despite pseudonymity, supporting both investigation and asset recovery. These tools exploit the transparency of public blockchains, which record all transactions permanently even when participant identity is obscured. Regulatory technology solutions can automate compliance monitoring and anomaly detection, enabling more efficient allocation of enforcement resources. Cooperative arrangements among regulators enable information sharing and coordinated action against cross-border violators.

Casino et al. (2024) documented the development of these mechanisms while noting their continued limitations, particularly regarding fully privacy-preserving technologies. Privacy-enhancing technologies such as mixers and privacy coins can defeat blockchain analytics, while sophisticated actors may structure activities to avoid detection. Enforcement mechanisms must continue evolving to address technological countermeasures while respecting legitimate privacy interests.

The research findings support graduated enforcement approaches that combine industry engagement with credible deterrent measures. Compliance-oriented regulation that works with industry to develop practical implementation approaches may be more effective than purely punitive measures for legitimate businesses, while preserving deterrent effect for genuinely evasive actors. Clear regulatory expectations, reasonable compliance timelines, and accessible guidance support compliance by well-intentioned actors while preserving basis for strong enforcement against willful violators.

Addressing digital law evasion effectively requires enhanced international cooperation beyond current frameworks that were designed for different technological conditions. The research findings support several specific recommendations for enhancing cooperation mechanisms. Expansion of mutual legal assistance treaties to include expedited procedures for digital evidence preservation responsive to the speed of digital transactions would address the time-sensitivity problem that renders traditional procedures ineffective. Development of specialized information-sharing arrangements for regulatory matters not rising to the level of criminal conduct would enable cooperation regarding civil and administrative enforcement that currently depends on territorial jurisdiction.

Capacity building programs to enable developing jurisdictions to participate effectively in international enforcement cooperation would address the gap in capabilities that currently limits cooperation effectiveness. Jurisdictions lacking technical capacity or legal frameworks for gathering digital evidence cannot serve as effective cooperation partners, creating potential gaps in enforcement coverage that sophisticated actors can exploit.

The Hague Conference on Private International Law's ongoing work on digital economy implications for private international law represents an important venue for developing modernized frameworks. The research supports prioritization of projects addressing jurisdiction in digital contexts, recognition and enforcement of judgments involving digital assets, and applicable law rules for smart contracts and decentralized technologies. These projects should build on the Conference's successful track record of developing widely-adopted international instruments while adapting methodologies for faster-evolving technological contexts.

A recurring theme throughout this research concerns the tension between combating law evasion and preserving space for legitimate innovation and commerce that digital technologies enable. Digital technologies offer genuine benefits including financial inclusion for populations underserved by traditional finance, reduced transaction costs for cross-border commerce, enhanced privacy for legitimate activities, and new business models that create value for consumers and businesses alike. Overly restrictive responses to law evasion concerns risk stifling beneficial innovation while sophisticated evasive actors find alternative mechanisms to continue their activities.

Regulatory sandboxes offer one promising approach to managing this tension that has achieved adoption across multiple jurisdictions. By allowing innovative activities to proceed

under regulatory supervision with temporary relief from full compliance requirements, sandboxes enable both regulators and innovators to understand risks and develop appropriate frameworks. The research documented successful sandbox programs in several jurisdictions, though noting that sandboxes must be designed carefully to avoid becoming mere licensing advantages for well-connected firms.

Proportionality principles should guide enforcement approaches, with responses calibrated to the severity of evasive conduct and the harm caused. Minor technical violations by generally compliant actors warrant different treatment than systematic evasion by sophisticated bad actors. Risk-based approaches that focus supervisory attention on highest-risk activities and actors enable more efficient allocation of limited enforcement resources while maintaining deterrent effect against serious misconduct.

Conclusion

This research has comprehensively examined modern forms of law evasion in international private law as they manifest within the digital economy. The findings demonstrate that traditional mechanisms of law evasion including forum shopping, choice of law manipulation, and corporate structure abuse have adapted to digital contexts while novel mechanisms enabled by technologies including cryptocurrency, smart contracts, and decentralized platforms have created entirely new evasion opportunities. The borderless nature of digital technologies, combined with pseudonymous features and the absence of traditional intermediaries, fundamentally challenges regulatory frameworks premised on territorial sovereignty and identifiable actors.

The comparative regulatory analysis revealed significant variation in how jurisdictions approach digital law evasion, with the European Union's MiCA Regulation representing the most comprehensive framework while the United States maintains fragmented approaches that create arbitrage opportunities. Uzbekistan's developing framework demonstrates both the challenges facing transitional economies in addressing digital risks and the potential for regulatory environments that balance innovation encouragement with protection against abuse. Across all jurisdictions examined, enforcement remains challenging given the speed of digital transactions, the difficulty of identifying and locating violators, and the limitations of international cooperation mechanisms designed for a pre-digital world.

Based on these findings, several mechanisms for combating digital law evasion merit prioritization. International harmonization of regulatory frameworks should continue, building on models such as MiCA while learning from implementation experience and addressing gaps regarding decentralized technologies. Enhanced international cooperation mechanisms, including expedited mutual legal assistance procedures, specialized regulatory information sharing, and capacity building for developing jurisdictions, are essential given the inherently cross-border nature of digital transactions. Technological solutions including

blockchain analytics and regulatory technology should complement traditional enforcement, while preserving appropriate privacy protections. Effects-based approaches to jurisdiction and applicable law determination deserve further development as alternatives to traditional connecting factors rendered artificial by digital presence.

The research contributes to legal scholarship by providing a comprehensive typology of digital law evasion forms, integrating regulatory analyses with private international law doctrine, and incorporating perspectives from both developed and developing jurisdictions. For practitioners and policymakers, the findings provide practical guidance for identifying and responding to evasive conduct while preserving legitimate commercial activities. For international organizations engaged in harmonization efforts, the research supports prioritization of projects addressing digital-specific challenges while building on proven methodologies for international coordination.

Future research should address several areas where this study's scope was necessarily limited. Empirical research examining actual patterns of digital law evasion, to the extent data can be obtained, would provide valuable complement to the doctrinal analysis presented here. The implications of emerging technologies including central bank digital currencies, artificial intelligence, and evolving privacy technologies for law evasion merit continuing attention. The effectiveness of specific regulatory interventions should be evaluated as implementation proceeds, enabling evidence-based refinement of policy approaches.

The digital economy's transformation of law evasion in international private law represents one manifestation of broader challenges facing legal systems designed for a territorial world. The mechanisms proposed in this research for combating digital law evasion have broader applicability to the governance challenges of an increasingly digital global society. As technology continues to evolve, legal frameworks must demonstrate comparable adaptability while preserving core values of fairness, predictability, and protection against abuse that justify their continued relevance.

Bibliography

Allahrakha, N. (2024). Legal analysis of the law of the Republic of Uzbekistan "on payments and payment system". *TSUL Legal Report*, *5*, 38–55. https://doi.org/10.51788/tsul.lr.5.1./WAJR6426

Allahrakha, N. (2025). Cross-border e-crimes: Jurisdiction and due process challenges. *ADLIYA: Jurnal Hukum dan Kemanusiaan*, *18*, 153–170. https://doi.org/10.15575/adliya.v18i2.38633

Cámara Lapuente, S. (2021). Smart contracts: An introduction to the blockchain world. In A. Ferrante (Ed.), *Digital revolution and new society: Technology, artificial intelligence, and privacy* (pp. 87–112). Routledge.

Kunda, I., & Gonçalves, A. (2021). Private international law and the digital economy. In *Encyclopedia of private international law* (pp. 1423–1436). Edward Elgar Publishing.

Petsche, M. A. (2011). What's wrong with forum shopping: An attempt to identify and assess the real issues of a controversial practice. *International Lawyer*, *45*(4), 1005–1028.

Symeonides, S. C. (2016). *Codifying choice of law around the world: An international comparative analysis*. Oxford University Press.