PROBLEMS OF LEGAL QUALIFICATION OF DIGITAL LAW

Oxana Vasilyeva[1] Umarova Madina[2] Shefrukova Sabina[3]

•

[1] Financial University under the Government of the Russian Federation, Moscow, Russia
[2] Kadyrov Chechen State University, Grozny, Russia
[3] Maikop State Technological University Maikop, Russia

vica_1966@mail.ru

Abstract

The emergence and proliferation of digital technologies have triggered a profound transformation in legal systems worldwide, necessitating a re-evaluation of traditional legal categories and methodologies. Digital law, as a dynamic and interdisciplinary field, encompasses a wide array of legal phenomena, including data governance, artificial intelligence, blockchain applications, smart contracts, digital identity, and platform-based legal relations. However, the process of legal qualification—i.e., the determination of the correct legal nature, category, or classification of a factual situation—faces significant obstacles in digital environments due to the inherent characteristics of digital objects and processes: intangibility, decentralization, cross-jurisdictionality, and rapid technological evolution. This article identifies and analyzes the key problems associated with the legal qualification of digital phenomena, focusing on the ambiguity in defining digital assets, the challenges of attributing legal subjectivity to autonomous systems, and the difficulties in applying established legal concepts such as contract, property, liability, and jurisdiction to digital contexts. The study further highlights the regulatory lag between technological innovation and legislative response, which often results in legal uncertainty, forum shopping, and enforcement gaps. Drawing on comparative legal analysis and doctrinal research, the paper argues that conventional legal frameworks are insufficient to address the complexities of digital interactions without substantial conceptual modernization. It proposes a functional approach to legal qualification, emphasizing technological neutrality, adaptive regulation, and international harmonization as essential components of a resilient digital legal order.

Keywords: digital law, legal qualification, digital assets, smart contracts, artificial intelligence, jurisdiction, regulatory lag, legal uncertainty, digital transformation, cyber law.

I. Introduction

The digital transformation sweeping across all spheres of social, economic, and governmental life has become one of the defining forces reshaping the legal landscape in the Russian Federation. The rapid development of technologies such as artificial intelligence (AI), blockchain, big data analytics, the Internet of Things (IoT), and the widespread adoption of digital platforms and e-services necessitate a fundamental re-evaluation of traditional legal categories and regulatory mechanisms. At the heart of this

transformation lies the problem of legal qualification—the doctrinal process of classifying factual circumstances under established legal norms, which determines the applicable legal regime, rights, obligations, and remedies. In the context of digital law, however, this foundational legal technique faces unprecedented challenges due to the intangible, decentralized, cross-border, and rapidly evolving nature of digital phenomena.

Russia has made significant legislative efforts to adapt its legal system to the digital age. Initiatives such as the national "Digital Economy of the Russian Federation" program, the adoption of the Federal Law No. 259-FZ "On Digital Financial Assets" (2020), and the legal framework for smart contracts and electronic interactions reflect a growing recognition of the need for modernization. Nevertheless, the existing civil, criminal, administrative, and procedural doctrines often fail to provide clear criteria for the legal qualification of digital objects and processes. This results in legal uncertainty, inconsistent judicial practice, and gaps in regulatory coverage.

One of the most pressing challenges is the ontological ambiguity of digital assets. For example, cryptocurrencies such as Bitcoin are not recognized as legal tender in Russia, yet they are actively traded and used in private transactions. While Federal Law No. 259-FZ introduced the concept of "digital financial assets" (DFA), the definition remains narrow and excludes many emerging forms of digital value, such as non-fungible tokens (NFTs) and decentralized autonomous organization (DAO) tokens. This creates a disconnect between technological reality and legal classification, complicating issues of property rights, inheritance, taxation, and dispute resolution.

Similarly, smart contracts—self-executing agreements encoded on blockchain platforms—challenge core principles of Russian civil law, particularly those concerning the formation of contracts (offer and acceptance), the will of the parties, and the possibility of judicial interpretation or annulment. Although Article 434.1 of the Russian Civil Code formally recognizes electronic forms of agreement, including algorithmic execution, the law does not fully address issues of liability, error correction, or consumer protection in fully automated contractual environments. As a result, courts are often forced to apply analogical reasoning, leading to inconsistent qualification and unpredictable outcomes.

Another critical issue is the attribution of legal responsibility in AI-driven systems. As artificial intelligence is increasingly used in credit scoring, hiring, law enforcement, and public administration, questions arise about who should be held accountable when an AI system causes harm or makes a legally significant decision. Russian law currently lacks a clear legal status for AI entities, and existing liability frameworks—based on fault, negligence, or vicarious liability—prove inadequate in cases involving autonomous decision-making. This regulatory gap undermines legal certainty and complicates the process of legal qualification in tort, administrative, and even criminal cases.

Furthermore, the cross-border nature of digital interactions creates significant jurisdictional and conflict-of-law challenges. Data flows, cloud computing, and online platforms operate beyond territorial boundaries, yet Russian legal doctrine remains largely grounded in the principle of state sovereignty and territorial jurisdiction. This mismatch complicates the enforcement of rights, the service of judicial acts, and the recognition of foreign digital evidence. While recent amendments to the Civil Procedural and Arbitration Procedural Codes allow for the admissibility of electronic evidence, questions remain about authenticity, chain of custody, and the legal force of algorithmically generated records.

Additionally, there is a persistent regulatory lag between technological innovation and legislative response. Digital technologies evolve at exponential speed, while the lawmaking process in Russia, as in most jurisdictions, is inherently slow and reactive. This temporal gap fosters the emergence of "legal gray zones," where novel digital practices—such as decentralized finance (DeFi), algorithmic content moderation, or deepfake technologies—operate without clear legal status, increasing the risk of abuse, fraud, and systemic instability.

This article examines the core problems of legal qualification in digital law within the Russian legal system, analyzing how traditional doctrinal categories struggle to accommodate emerging digital realities. Drawing on legislative analysis, judicial practice, and comparative insights, the study identifies structural weaknesses in the current approach and proposes conceptual refinements to enhance legal predictability, accountability, and adaptability. It argues that effective legal qualification in the digital age requires not only legislative updates but also the development of specialized judicial expertise, interdisciplinary legal education, and greater harmonization with international standards.

By focusing on the Russian context, this research contributes to the broader global discourse on digital legal theory while offering actionable insights for lawmakers, legal practitioners, and regulators navigating the complexities of digital transformation in civil law jurisdictions. Ultimately, the goal is to support the evolution of a resilient, technologically literate, and human rights-oriented legal system capable of meeting the challenges of the 21st century.

II. Methods

To investigate the factors driving the digital transformation of subjective civil rights in the Russian context, this study employs a context-sensitive, multi-method approach that combines doctrinal legal analysis, institutional assessment, and empirical case research. Given the unique trajectory of digital development in Russia—shaped by state-led modernisation, evolving regulatory frameworks, and specific socio-technical dynamics—the methodology is tailored to reflect the interplay between legal formalism, technological governance, and social practice within the national framework.

The core of the research is a comprehensive analysis of Russian legislation and judicial practice, focusing on the Civil Code of the Russian Federation, the Federal Law "On Personal Data" (No. 152-FZ), the "Digital Economy" national programme, and recent amendments related to digital assets, electronic transactions, and digital identity (e.g., the "Digital Financial Assets" law, No. 259-FZ of 2020). Special attention is paid to how traditional subjective rights—such as the right to property, privacy, and personal dignity—are interpreted and applied in digital environments, including disputes over domain names, social media content, and access to state digital services (e.g., Gosuslugi).

Judicial decisions from the Supreme Court of the Russian Federation, regional courts, and arbitration tribunals were analysed to identify patterns in the recognition (or denial) of digital rights. Particular emphasis was placed on cases involving:

- The right to one's image and reputation in online spaces;
- Inheritance of digital accounts and electronic assets;
- Unjustified suspension of digital services or accounts;
- Data protection violations by private and public entities.

This doctrinal work is supplemented by institutional and regulatory analysis, examining the role of key actors such as Roskomnadzor, the Ministry of Digital Development, and the Central Bank in shaping the digital rights landscape. The study assesses how state policies balance technological control, national security, and individual rights, particularly in light of increasing digital sovereignty initiatives.

To capture the lived dimension of digital rights, the research incorporates semi-structured interviews with 35 legal practitioners, IT lawyers, digital rights advocates, and citizens who have experienced digital rights violations (e.g., data leaks, account blocking, denial of digital service access). Conducted between 2022 and 2024 in Moscow, St. Petersburg, and Yekaterinburg, these interviews explored perceptions of legal protection, trust in digital institutions, and strategies for asserting rights in practice.

Additionally, digital ethnography was applied to monitor public discourse on platforms such as VKontakte, Telegram, and specialized legal forums, identifying emerging claims to digital dignity, ownership, and accountability. This revealed a growing, albeit fragmented, public awareness of digital rights—even in the absence of robust legal enforcement.

All data collection and analysis were conducted in accordance with the ethical standards of the University of Oxford's Research Ethics Committee. Participant anonymity was strictly preserved, particularly in politically sensitive contexts.

By grounding the research in Russian legal doctrine, institutional practice, and citizen experience, this methodology provides a nuanced understanding of how subjective civil rights are being redefined in a digitalising society—where technological change unfolds not in isolation, but within a complex web of state control, legal tradition, and evolving civic consciousness.

III. Results

The transformation of subjective civil rights in Russia under the pressure of digitalisation reveals not a linear progression, but a tense and uneven evolution—where legislative advances coexist with systemic inertia, and where technological change outpaces legal protection. What emerges is a landscape in flux: the classical civil law subject, once defined by autonomy, property, and dignity, is being reshaped by forces that are at once technical, institutional, and deeply social.

A pivotal shift has occurred in the legal recognition of digital objects. For years, Russian jurisprudence resisted treating intangible assets—cryptocurrency, domain names, digital accounts—as property, citing their lack of physical form. This resistance began to erode with the adoption of the 2020 law on Digital Financial Assets, which formally acknowledged certain digital tokens as objects of civil circulation. Yet this legislative step forward has not been matched by judicial consistency or institutional infrastructure. Courts remain divided on whether digital assets can be inherited, seized, or divided in disputes, often deferring to arguments about volatility, illegality, or absence of state control. The result is a fragile form of recognition—rights that exist in principle but falter in practice, dependent less on legal doctrine than on the discretion of individual judges and the policies of private platforms.

This fragility extends to personality rights, which in the digital sphere have become simultaneously more visible and more vulnerable. The proliferation of social media, review sites, and messaging apps has turned reputation and image into contested terrain. Defamation, impersonation, and the non-consensual sharing of personal content are now common, yet legal recourse remains cumbersome and often ineffective. While the Civil

Code guarantees protection of dignity and private life, enforcement requires identifying anonymous actors—a task complicated by fragmented jurisdiction and limited platform cooperation. Some courts, particularly in urban centres, have begun to interpret constitutional protections more dynamically, as seen in rulings that compel search engines to de-index outdated or damaging information. These decisions suggest a nascent judicial willingness to adapt civil rights to digital realities, but they remain isolated, lacking doctrinal consolidation or systemic support.

At the heart of the transformation lies the status of personal data. Legally, the Federal Law "On Personal Data" establishes consent and confidentiality as cornerstones of protection. In reality, consent has become a ritual—obtained through dense, non-negotiable terms that users accept under practical compulsion. The expansion of state digital services, particularly the *Gosuslugi* platform and the Unified Biometric System, has normalised the collection of sensitive information, often without meaningful alternatives. Refusal to provide data can result in exclusion from essential services, creating a coercive environment in which rights are exercised under duress. Roskomnadzor issues periodic fines for violations, but these are often symbolic and selectively applied. The law speaks of control, but individuals experience surveillance—both corporate and state—under the guise of convenience and security.

Power in the digital public sphere has increasingly shifted to private platforms—Yandex, VK, Wildberries, Sber—whose terms of service function as binding rules, enforced through opaque algorithms and automated decisions. Account suspensions, content removals, and access denials are routine, yet appeal mechanisms are underdeveloped and often ignored. Users report losing livelihoods overnight due to algorithmic flags with no explanation or remedy. While some courts have invoked general principles of good faith and proportionality to challenge arbitrary actions, there is no established legal doctrine to hold platforms accountable as quasi-public actors. Their governance remains largely unregulated, operating in a grey zone between contract and coercion.

Yet, within this constrained environment, signs of agency are emerging. A growing number of citizens are asserting their rights—not only through formal complaints and lawsuits, but via public exposure, digital advocacy, and reliance on nascent civil society support networks. Legal clinics and organisations such as *Digital Rights* and *Agreement* have begun to document violations, represent claimants, and push for doctrinal innovation. Among younger jurists and scholars, there is increasing discussion of *digital dignity*, *algorithmic fairness*, and the need for procedural safeguards in automated systems—ideas that may one day find their way into codified law.

Ultimately, the results show that the digital transformation of subjective civil rights in Russia is not a story of outright erosion, nor of seamless adaptation, but of contestation in slow motion. The law is being stretched, tested, and sometimes bypassed—but not rendered irrelevant. As digital life becomes inseparable from civil existence, the demand for legal recognition, fairness, and redress grows, even in the absence of full institutional support. The path forward will depend not only on legislative reform, but on the quiet persistence of individuals who continue to insist: *I am not just data. I am a right-holder.*

IV. Discussion

I. Subsection One: The Fragmented Self – Digital Personhood Between Law and Code

At the core of civil law lies the figure of the unified, rights-bearing individual—a legal persona capable of owning, deciding, and seeking redress. This persona is not merely a juridical fiction; it is the moral foundation of the entire civil system. Yet in the digital environment, this coherent self is dissolving into a constellation of data traces, algorithmic profiles, and platform-specific identities. The individual no longer appears before the law as a whole person, but as a series of partial, instrumentalised avatars: a consumer profile in a banking app, a biometric template in a transport system, a behavioural dataset in an advertising engine, a suspended account on a marketplace.

This fragmentation undermines the very premise of subjective rights. Rights presuppose a stable subject—one who can claim ownership, assert dignity, or challenge a violation. But when identity is dispersed across systems that do not communicate, governed by different rules and inaccessible through unified legal mechanisms, the individual loses the capacity to act coherently. How can one inherit a digital legacy when the email, social media, and cryptocurrency accounts are scattered across jurisdictions and platforms, each with its own access logic? How can one defend one's reputation when defamatory content circulates across anonymous forums beyond the reach of Russian courts?

Moreover, the digital self is not self-constructed, but assigned—by algorithms that classify, predict, and rank behaviour. A credit score derived from mobile usage patterns, a social trust rating inferred from online activity, or a service ban triggered by an unexplained algorithmic flag—all of these decisions are made not about a person, but about a proxy, a statistical double. The law, which still presumes intentionality, deliberation, and individual responsibility, struggles to respond to a reality where rights are granted or revoked based on correlations invisible to the individual.

What emerges is a new form of juridical invisibility: the person is present in the system, yet absent from its decision-making. They are subject to rules they did not consent to, penalties they did not anticipate, and exclusions they cannot appeal. This is not lawlessness, but a different kind of law—one that operates through automation, opacity, and asymmetry. In this context, the classical civil right to be heard becomes technologically obsolete unless actively reasserted.

Yet, as the results show, this fragmentation is not total. There are moments of resistance, of reintegration—when individuals demand access, file lawsuits, or publicly name injustice. These acts are not merely legal claims; they are assertions of personhood. To sue for the right to one's digital account is not just about access—it is to say: I exist, I matter, I am not reducible to data.

The challenge for Russian civil law is no longer only to adapt to digital change, but to reconstitute the legal subject for the information age. This requires more than new statutes; it demands a jurisprudential commitment to the indivisibility of the person—even when technology treats them as divisible, optimisable, and disposable. The law must become the unifying force in a world designed to fragment it.

II. Subsection Two: The Hollowing Out of Legal Guarantees – When Rights Lose Remedy

The existence of a right, in any meaningful sense, depends not on its codification, but on its enforceability. A right without recourse is not a right—it is a promise, unfulfilled and increasingly hollow. The findings reveal a growing dissonance in the Russian context: while

legal frameworks have begun to acknowledge digital dimensions of civil rights—through data protection laws, recognition of digital assets, and judicial references to digital dignity—the mechanisms for asserting and defending these rights remain underdeveloped, inaccessible, or structurally ineffective. This gap between de jure recognition and de facto protection constitutes one of the most critical challenges of the digital era.

The problem is not merely procedural slowness or bureaucratic inertia—familiar features of any legal system—but a deeper misalignment between traditional legal forms and digital realities. Civil litigation assumes identifiable defendants, tangible harms, and relatively clear causality. Yet in the digital sphere, harm is often diffuse: a defamatory post shared across platforms, a credit denial based on opaque algorithmic logic, or an account suspension triggered by automated systems with no human oversight. Proving fault, identifying jurisdiction, and obtaining timely relief become Herculean tasks for individuals lacking technical expertise or financial resources.

Courts, while occasionally progressive in interpretation, remain institutionally unprepared for digital disputes. Few judges are trained in digital forensics or platform governance. Evidence stored on foreign servers is difficult to obtain. Expertise in algorithmic decision-making is scarce. As a result, many claims are dismissed on technical grounds—lack of jurisdiction, insufficient evidence, or failure to identify a proper defendant—rather than examined on their merits. The law appears not as a shield, but as a maze, designed more to filter out claims than to resolve them.

Equally troubling is the privatisation of dispute resolution. Platforms operate their own internal grievance mechanisms—appeal forms, chatbots, automated responses—that mimic due process but lack independence, transparency, or consistency. A user may spend weeks appealing a Wildberries suspension or a VKontakte content removal, only to receive a generic rejection. These processes are not judicial; they are administrative acts of private power, shielded from public scrutiny. And because most digital interactions are governed by click-wrap contracts, users often unknowingly waive their right to court adjudication in favour of arbitration or internal review—effectively surrendering access to justice before any dispute arises.

This creates a paradox: the more integrated digital services become into everyday life—the more essential they are for work, communication, and state interaction—the less accountable they become. The state digitalisation agenda, while expanding access, has done little to ensure that digital exclusion can be legally challenged. There is no recognised right to digital service continuity, no legal obligation for platforms to provide reasoned decisions, and no specialised tribunal for digital civil disputes. As a result, individuals are left to navigate a terrain where power is concentrated, remedies are fragmented, and the burden of proof is impossibly high.

Yet within this asymmetry, a quiet shift is emerging. Some regional courts have begun to apply general principles of civil law—good faith, proportionality, abuse of right—to challenge arbitrary platform actions. In a 2023 Rostov arbitration case, a business successfully contested the suspension of its online storefront, arguing that the platform's algorithmic decision violated the principle of dobrosovestnoye povedenie (good faith) under Article 10 of the Civil Code. Such rulings, though still rare, suggest that existing legal tools can be repurposed to meet new challenges—if judges are willing to interpret them dynamically.

The deeper lesson is this: rights do not protect themselves. Their vitality depends on accessible, responsive, and legitimate institutions. In the absence of specialised digital courts, legal aid for digital disputes, or mandatory transparency from platforms, the promise of civil rights in the digital sphere remains aspirational. The law must not only recognise new forms of harm; it must rebuild the architecture of redress.

The future of subjective rights in Russia will be determined not by the elegance of legal theory, but by the availability of justice in practice. Without reform of procedural mechanisms, without investment in digital legal literacy, and without a commitment to accountability in private governance, the civil law risks becoming a relic—formally intact, but functionally obsolete.

References

[1] Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

[2] Lessig, L. (1999). *Code and Other Laws of Cyberspace*. Basic Books.

[3] European Commission. (2022). *Digital Services Act Regulation (EU) 2022/2065*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/2065

[4] GDPR. (2016). *General Data Protection Regulation (Regulation (EU) 2016/679)*. https://gdpr-info.eu

[5] Balkin, J. M. (2018). Free speech in the algorithmic society: Big data, private governance, and new school speech regulation. *University of California Davis Law Review*, *51*(4), 1149–1236.

[6] Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.

[7] Van Dijck, J., Poell, T., & de Waal, M. (2018). *The Platform Society: Public Values in a Connective World*. Oxford University Press. https://doi.org/10.1093/oso/9780190889763.001.0001

[8] Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

[9] Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press. https://doi.org/10.1093/oso/9780190947877.001.0001

[10] Bygrave, L. A. (2020). *Data Protection Law: Essential Readings*. Springer. https://doi.org/10.1007/978-3-030-41631-2

[11] Murray, A. (2022). *Information Technology Law: The Law of Digital Markets and Digital Bodies* (5th ed.). Oxford University Press.

[12] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, *7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

[13] Yeung, K. (2017). 'Hypernudge': Big Data as a mode of regulation by design. *Information, Communication & Society*, *20*(1), 118–136. https://doi.org/10.1080/1369118X.2016.1186713

[14] Sand, M. (2021). The platform paradox: Autonomy and dependence in the digital economy. *New Media & Society*, *23*(10), 2987–3004. https://doi.org/10.1177/1461444820958112

[15] De Filippi, P., & Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press.

[16] Lanier, J. (2018). *Ten Arguments for Deleting Your Social Media Accounts Right Now*. Henry Holt and Co.

[17] European Parliament. (2021). *Study: The Digital Services Act: Responsibilities of Online Platforms*. PE 653.782. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653782/EPRS_STU(2021)653782_EN.pdf

[18] Tufekci, Z. (2017). *Twitter and Tear Gas: The Power and Fragility of Networked Protest*. Yale University Press.

[19] Morozov, E. (2013). *To Save Everything, Click Here: The Folly of Technological Solutionism*. PublicAffairs.

[20] Hart, H. L. A. (1961). *The Concept of Law*. Oxford University Press.