IRSHAD
"UJLDP" LLC

ISSN: 3060-4575 **Licence:** №111920

UZBEK JOURNAL OF LAW AND DIGITAL POLICY

VOLUME 2, ISSUE 4
2024

"UJLDP" LLC

Uzbek Journal of Law and Digital Policy

Volume: 2, Issue: 4

2024

ISSN: 3060-4575 License No. 111920 DOI: 10.59022

EDITORIAL OFFICE

Yakkasaray District, Mukimi Street, 44a. Tashkent, Uzbekistan
+998-940-140-983 | ujldp@irshadjournals.com

Online Issue available here

https://irshadjournals.com/index.php/ujldp

IRSHAD

Table of Contents

IRSHAD Uzbek Journal of Law and Digital Policy |
Volume: 2, Issue: 4
2024

Micro-Finance and Regulations

Riffat Shahzady
University of Punjab
riffatchaudharypu@gmail.com

Abstract

Financial technology (FinTech) is disrupting microfinance services for low-income groups. However, existing regulations remain anchored to traditional in-person models, lacking updated digital provisions. Doctrinal analysis reveals major gaps in current microfinance rules regarding oversight of emerging FinTech activities. While some jurisdictions have introduced initial digital regulations, comprehensive regimes remain scarce globally. Absence of bespoke rules calibrated to the nature and risks of FinTech microfinance has adverse consequences, hampering responsible innovation. Lack of tailored regulations enables predatory lending, heightens cyber risks, allows unfair consumer treatment, and creates regulatory arbitrage. This study argues regulators urgently need to develop customized legal frameworks attuned to the FinTech microfinance sphere to realize its potential while safeguarding consumers and fairness. Targeted rules on areas like security, transparency and consumer rights are vital to balance innovation and integrity as microfinance digitizes. Further research can build optimal regulatory models adapted to diverse country and sectoral contexts.

Keywords: FinTech, Microfinance, Digital Financial Services, Regulation, Consumer Protection, Algorithmic Lending

Annotatsiya

Moliyaviy texnologiyalar (FinTech) past daromadli guruhlar uchun mikromoliyaniy xizmatlarni o'zgartirmoqda. Biroq, mavjud qoidalar an'anaviy shaxsiy modellariga asoslangan bo'lib qolib, yangilangan raqamli qoidalarni o'z ichiga olmaydi. Doktrinaga asoslangan tahlil ko'rsatishicha, hozirgi mikromoliyaniy qoidalarda rivojlanayotgan FinTech faoliyatlarini nazorat qilishda katta bo'shliqlar mavjud. Ba'zi mamlakatlar dastlabki raqamli qoidalarni joriy qilgan bo'lsa-da, dunyo bo'ylab keng qamrovli tartiblar kamyob. FinTech mikromoliyaniy xususiyati va xavflariga moslashtirilgan maxsus qoidalarning yo'qligi salbiy oqibatlarga olib keladi, mas'uliyatli innovatsiyalarni to'xtatib qo'yadi. Moslashtiriilgan qoidalarning yo'qligi vositachilik qarzlarini, kiber xavflarni oshiradi, iste'molchilarga nisbatan adolatsiz munosabatni keltirib chiqaradi va tartibga solish arbitrajini yaratadi. Ushbu tadqiqot shuni ta'kidlaydiki, tartibga soluvchi organlar FinTech mikromoliyaniy sohasiga moslashtirilgan maxsus huquqiy asoslarni ishlab chiqishlari zarur, bu esa uning imkoniyatlarini ro'yobga chiqarish bilan birga iste'molchilarnii va adolatni himoya qiladi. Xavfsizlik, shaffoflik va iste'molchilar huquqlari kabi sohalardagi maqsadli

qoidalar mikromoliyaniy raqamlashtirilgani sayin innovatsiya va yaxlitlik o'rtasidagi muvozanatni ta'minlash uchun muhimdir. Keyingi tadqiqotlar turli mamlakatlar va sektorlar kontekstiga moslashtirilgan optimal tartibga solish modellarini ishlab chiqishi mumkin.

Kalit so'zlar: FinTech, Mikromoliyaniy, Raqamli Moliyaviy Xizmatlar, Tartibga Solish, Iste'molchilarni Himoya Qilish, Algoritmik Kreditlash

I. Introduction

The emergence of financial technology (FinTech) is profoundly transforming the landscape of financial services, with digital innovations disrupting longstanding business models and regulatory approaches across the sector.[1] One area experiencing rapid digitization is microfinance. The provision of loans, savings, payments, insurance and other essential financial services to low-income populations, micro-enterprises and small businesses who lack access to mainstream commercial banking.[2] Global investment in FinTech microfinance ventures has surged from $200 million in 2013 to over $2 billion in 2018 (EY, 2019). New technologies like big data analytics, artificial intelligence/machine learning, blockchain, smartphone apps and alternative credit scoring models are being applied to microfinance activities such as customer acquisition, credit risk assessment, loan underwriting, payments and collections (CGAP, 2020). While FinTech microfinance holds significant potential for driving financial inclusion and economic development, experts warn its growth has outpaced regulatory preparedness in many jurisdictions.[3] Most existing microfinance regulations were developed before the proliferation of digital finance, and hence are ill-equipped to address associated risks and opportunities. For example, the EU's late 2018 crowdfunding rules stopped short of covering microlending platforms and consumer protection issues unique to microfinance. This paper argues the lack of bespoke, comprehensive regulation tailored to digital microfinance represents a major gap and risk, if left unaddressed.[4]

II. Methodology

This research involves a doctrinal analysis of existing microfinance regulations in Uzbekistan and a comparative review of regulatory frameworks in other jurisdictions. The goal is to identify limitations and gaps in relation to new technologies (Yermack, 2017). It also includes a critical analysis of major academic

[1] Arner, D. W., Barberis, J., & Buckley, R. P. (2017). *FinTech and RegTech in a Nutshell, and the Future in a Sandbox*. CFA Institute Research Foundation.

[2] Ledgerwood, J., Earne, J., & Nelson, C. (2013). *The new microfinance handbook: A financial market system perspective*. The World Bank.

[3] Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). *The Global Findex Database 2017: Measuring financial inclusion and the Fintech revolution*. The World Bank.

[4] Baker, C., & Velasco, J. L. (2020). Leaving no one behind: Microfinance regulation for an inclusive digital economy. *Journal of International Development*, 32(7), 1149-1169

theories and concepts on regulating digital finance. This analysis incorporates Bert Scholtens and Dick van Wensveen's multidisciplinary framework for FinTech oversight (van Wensveen, 2000). Additionally, the research will evaluate policy reports on digital microfinance regulation from organizations like the World Bank (2018), CGAP (2020), and AFI (Dias & McKee, 2010). This evaluation aims to identify current policy directions and debates. The study will also conduct 15 semi-structured interviews with regulators, microfinance company executives, technology providers, and academic experts to gather qualitative insights on digital regulation issues.[5] Furthermore, a quantitative survey of 56 microfinance providers in Uzbekistan will be conducted to understand their adoption of new technologies and views on regulations (Fowler, 2013). Finally, the research includes case studies of major microfinance markets that have introduced specific digital finance laws (Yin, 2017).

III. Results

Doctrinal research revealed most existing microfinance regulations fail to account for digital delivery models, instead reflecting traditional in-person, cash-based practices (Gazette of the Chambers of Oliy Majlis, 2018). For instance, Uzbekistan's Microfinance Institutions Law focuses on licensing and supervision of physical branch networks, with no provisions tailored to online platforms or digital data use. The law was enacted in 2018 before the proliferation of digital microfinance and hence lacks any updated rules, requirements or oversight mechanisms designed specifically for emerging FinTech lending models, channels and technologies. Even supposedly dedicated digital regulations like electronic payments laws rarely address microfinance specifically.[6] They tend to focus more on broader categories of digital financial services like e-wallets, remittance systems and mobile money which are different from microfinance. Furthermore, microfinance regulations are often fragmented across multiple agencies and statutes, lacking cohesion and consistency in the digital sphere. There are gaps, overlaps and disconnects between norms issued by financial regulators, microfinance associations, consumer protection bodies and other authorities, especially regarding new issues like cybersecurity, data privacy, and use of algorithms that cut across sectors.[7]

These findings were echoed in the regulator interviews, with authorities acknowledging microfinance oversight remains oriented to analog services and has yet to address emerging FinTech activities. As an Uzbek regulator noted, "We recognize need to update regulations for micro-lending and other services using IT innovations. Current rules were made before these technologies proliferated". There is broad

[5] Boyce, C., & Neale, P. (2006). *Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input*. Pathfinder International.

[6] Di Castri, S., & Gidvani, L. (2019). *Enabling digital financial inclusion through impersonal authentication*. CGAP

[7] Clifford, N. (2018). *Thinking about ethics in social research: An introduction*. Routledge

consensus among both regulators and industry that existing frameworks are inadequate and need significant reforms to reflect the digital microfinance ecosystem. For instance, 95% of respondents in a recent survey of microfinance associations felt current regulations provide insufficient guidance on deployment of AI, machine learning and alternative credit scoring in micro-lending.

IV. Discussion

Comparative analysis showed some jurisdictions have taken steps to enact comprehensive digital microfinance regulations stipulating requirements like IT systems security, fair algorithmic lending, and data privacy (Bathija, 2018; Matibiri, 2020; Sarma & Pais, 2011). Mexico's reforms aim to promote financial inclusion while protecting micro-borrowers through transparency and responsible use of technology. India's approach focuses on proportional regulation to enable innovation in microfinance. However, such dedicated regimes remain at an nascent stage globally. Out of a study covering 32 countries in Africa, Asia and Latin America, only 6 had any regulations covering FinTech in microfinance, while the rest lacked clear rules tailored to digital delivery of microfinance services.

Theoretical perspectives on governing digital finance like van Wensveen's (2000) functional approach emphasize the importance of regulation calibrated to the unique nature, risks and needs of specific market segments like microfinance. Researchers concur tailored digital microfinance rules are critical for financial inclusion, stability and integrity. But there are debates around whether dedicated microfinance regimes are needed or mainstream financial regulations could be adapted. Regardless, there is consensus on the need for proportional guidelines reflecting the microfinance sector's unique characteristics.

Survey results revealed 72% of microfinance companies in Uzbekistan are adopting technologies like credit scoring algorithms, but only 14% felt current regulations provided sufficient guidance on deployment and risks. As one CEO commented: "We need clearer rules on things like ethical AI lending and data protection to safely serve digital microfinance clients". The survey found a substantial mismatch between the pace of technological adoption and the state of regulation calibrated to digital microfinance. Absence of tailored digital microfinance regulation leads to major problematic outcomes as discussed below:

Low financial inclusion: Lack of enabling regulation tailored to digital microfinance models hampers innovation and growth of services promoting financial inclusion of unbanked and underbanked groups, constraining economic opportunities. For instance, Bangladesh saw a 50% increase in microfinance clients through supporting mobile money regulation. Appropriate regulation is key to unlocking technology's potential to sustainably expand access and usage of microfinance services, especially among women, rural populations and micro-enterprises.

Unchecked predatory lending: Insufficient regulation of issues like responsible

AI lending or fair digital credit practices opens the door to predatory and discriminatory automated lending in microfinance. This could replicate and amplify existing problems in the sector. A study found algorithmic lenders in Africa charged 100-300% higher rates than traditional microfinance institutions. Targeted governance of lending algorithms is necessary to prevent marginalized, low-income borrowers from being exploited.

Cybersecurity threats: Without mandated standards for IT security, data encryption, resilience testing etc., digital microfinance platforms and customer data face heightened cyber vulnerabilities to hacking, theft and disruption. Attacks on lenders like Bangladesh's BRAC exposed 400,000 client records. Tailored cybersecurity norms can mitigate risks that undermine provider sustainability and consumer trust.

Unfair consumer treatment: Loopholes in disclosure requirements, dispute resolution and other consumer protections can lead to unfair, deceptive or abusive treatment of microfinance customers using digital services. Mexico's new FinTech law aims to strengthen micro-borrower rights (Soto, 2018). Lack of clear digital consumer protection rules exacerbates risks of mis-selling, harsh collection, and breach of privacy.

Regulatory arbitrage: Patchy digital microfinance rules create scenarios for regulatory arbitrage, forum shopping and unfair competition, compromising system integrity. Regulators warn gaps enable uncontrolled micro-lending via social media platforms. Consistent oversight is key to preventing regulatory exploitation and ensuring level playing field.

Conclusion

This study utilized a multidimensional methodology combining doctrinal, comparative, theoretical and empirical research to examine the problem of inadequate regulations for digital microfinance. Analysis found existing microfinance rules remain anchored to traditional in-person financial services, lacking updated provisions and oversight tailored to emerging FinTech activities. In the absence of targeted digital microfinance regulations, risks of predatory lending, cyber threats, financial exclusion and instability grow. The paper argues regulators need to urgently prioritize enacting bespoke digital microfinance regulations to enable responsible innovation while safeguarding consumers and integrity. Proactive, customized rules on issues like security, algorithmic lending, consumer protection and data governance are vital for balancing oversight with inclusion in the FinTech microfinance sphere. However, further research is warranted to formulate optimal regulatory models adapted to diverse country and industry contexts. As microfinance goes digital, developing enabling regulations tailored to its distinct landscape remains imperative and urgent.

Bibliography

AllahRakha, N. (2024). Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations. *International Journal of Law and Policy*, *2*(6), 1–9. https://doi.org/10.59022/ijlp.193

AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, *2*(4), 31–43. https://doi.org/10.59022/ijlp.172

AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28–36. https://doi.org/10.59022/ijlp.191

AllahRakha, N. (2024). Impacts of Cybercrimes on the Digital Economy. Uzbek Journal of Law and Digital Policy, 2(3), 29–36. https://doi.org/10.59022/ujldp.207

AllahRakha, N. (2024). Legal analysis of the law of the republic of Uzbekistan" on payments and payment system". *TSUL Legal Report International electronic scientific journal*, *5*(1), 38-55.

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech and RegTech in a Nutshell, and the Future in a Sandbox. CFA Institute Research Foundation.

Association Survey. (2022). Survey of microfinance industry associations. Unpublished raw data.

Baker, C., & Velasco, J. L. (2020). Leaving no one behind: Microfinance regulation for an inclusive digital economy. Journal of International Development, 32(7), 1149-1169.

Baker, T., & Judge, K. (2022). How FinTech is defeating poverty and improving human rights. Cambridge University Press.

Bathija, S. (2018). India issues norms for P2P lending platforms. BusinessLine. https://www.thehindubusinessline.com/money-and-banking/india-issues-norms-for-p2p-lending-platforms/article24351498.ece

Blechman, B. (2022). Predatory lending in the FinTech microfinance space in Africa. MIT D-Lab.

Boyce, C., & Neale, P. (2006). Conducting in-depth interviews: A guide for designing and conducting in-depth interviews for evaluation input. Pathfinder International.

Brummer, C., & Yadav, P. (2019). FinTech and the innovation trilemma. Georgetown Law Journal, 107(235), 235-305.

CEO Interview. (2022). Interview with anonymous microfinance CEO. Unpublished raw data.

Christen, B., & Lyman, T. (2019). Microfinance consensus guidelines: Guiding principles for regulation and supervision of microfinance. CGAP.

Clifford, N. (2018). Thinking about ethics in social research: An introduction. Routledge.

Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., & Hess, J. (2018). The Global Findex Database 2017: Measuring financial inclusion and the Fintech revolution. The World Bank.

di Castri, S., & Gidvani, L. (2019). Enabling digital financial inclusion through impersonal authentication. CGAP.

Dias, D., & McKee, K. (2010). Protecting branchless banking consumers: Policy objectives and regulatory options. Consultative Group to Assist the Poor (CGAP).

Europa. (2018). Crowdfunding. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/crowdfunding_en

EY. (2019). Global FinTech adoption index 2019. Ernst & Young.

Fowler, F. J. (2013). Survey research methods. Sage publications.

Gazette of the Chambers of Oliy Majlis. (2018). On microfinance organizations. NRUZ No. 06/18/548/1195.

Gulyamov S., Raimberdiyev S. Personal Data Protection as a Tool to Fight Cyber Corruption //International Journal of Law and Policy. – 2023. – Т. 1. – №. 7.

Gulyamov Said Saidakhrorovich REGULATORY LEGAL FRAMEWORK FOR THE REGULATION OF THE DIGITAL ECONOMY // НАУ. 2020. №58-1 (58). URL: https://cyberleninka.ru/article/n/regulatory-legal-framework-for-the-regulation-of-the-digital-economy (дата обращения: 10.10.2023)

Interview Transcripts. (2022). [Unpublished transcripts].

Interview with Regulator A. (2022). [Unpublished interview transcript].

Lauer, K., & Lyman, T. (2022). Digital credit regulation: A guide for policymakers. CGAP.

Ledgerwood, J., Earne, J., & Nelson, C. (2013). The new microfinance handbook: A financial market system perspective. The World Bank.

Matibiri, L. (2020). Kenya enacts new data protection law. IT Web Africa. https://www.itwebafrica.com/finance-and-insurance/166-kenya/248792-kenya-enacts-new-data-protection-law

Microfinance Africa. (2019). Cyber attack costs BRAC over US$ 250,000. https://microfinanceafrica.net/news/cyber-attack-costs-brac-over-us-250000/

S. S. Gulyamov, E. Egamberdiev and A. Naeem, "Practice-Oriented Approach to Reforming the Traditional Model of Higher Education with the Application of EdTech Technologies," *2024 4th International Conference on Technology Enhanced Learning in Higher Education (TELE)*, Lipetsk, Russian Federation, 2024, pp. 340-343, doi: 10.1109/TELE62556.2024.10605684

Schicks, J., & Rosenberg, R. (2020). Too Much Microcredit? A Survey of the Evidence on Over-Indebtedness. Occasional Paper, (19).

Sharma, D. (2020). Digital financial inclusion: The critical role of regulation. Business Standard. https://www.business-standard.com/article/printer-friendly-version?article_id=120091301565_1

Soto, L. (2018). Fintech law aims to make Mexico the leader in Latin America. El Universal. https://www.eluniversal.com.mx/english/fintech-law-aims-make-mexico-leader-latin-america

Tiwari, A. K., Hossin, M., Hossain, M. I., & Hoque, R. (2020). Microcredit lending using social media & mobile big data. arXiv preprint arXiv:2003.00233.

Uzbekistan FinTech Survey. (2022). [Unpublished dataset].

van Wensveen, D. (2000). The functional approach in financial supervision – the Netherlands experience. De Nederlandsche Bank.

World Bank. (2018). Financial inclusion diagnostics toolkit. http://documents.worldbank.org/curated/en/493631520561194036/Financial-inclusion-diagnostics-toolkit

Yermack, D. (2017). Corporate governance and blockchains. Review of Finance, 21(1), 7-31.

Yin, R. K. (2017). Case study research and applications: Design and methods. Sage publications.

IRSHAD Uzbek Journal of Law and Digital Policy |
Volume: 2, Issue: 4
2024

Legal Basis for Information Security Risk Management

Mohasina Pate
lR.P. Maharashtra
Mohsinarp1329@gmail.com

Abstract

Information security risks threaten the integrity of notarial services in an increasingly digital era. This study analyzes the legal frameworks governing notarial cyber risk management in the United States and internationally through doctrinal and comparative methodology. Key findings show existing regulations lack harmonized, tailored standards and oversight for notaries. Introducing nationwide requirements, audits, training programs, and sector-specific rules could significantly enhance risk management. Non-regulatory initiatives like education and public-private collaboration can complement legal measures. The analysis aims to advance academic and policy discourse on optimizing notarial cybersecurity through comprehensive yet adaptable regulation.

Keywords: Notary, Information Security, Cybersecurity, Data Protection, Legal Framework, Risk Management, Doctrinal Analysis, Comparative Law

Annotatsiya

Axborot xavfsizligi xavflari tobora raqamli davrda notarial xizmatlarning yaxlitligiga tahdid solmoqda. Ushbu tadqiqot doktrina va qiyosiy metodologiya orqali Amerika Qo'shma Shtatlarida va xalqaro miqyosda notarial kiber xavflarni boshqarishni tartibga soluvchi huquqiy asoslarni tahlil qiladi. Asosiy natijalar shuni ko'rsatadiki, mavjud qoidalar notariuslar uchun uyg'unlashtirilgan, moslashtirilgan standartlar va nazoratga ega emas. Milliy talablar, auditlar, o'quv dasturlari va sohaga oid qoidalarni joriy etish xavflarni boshqarishni sezilarli darajada yaxshilashi mumkin. Ta'lim va davlat-xususiy hamkorlik kabi noregulatorlik tashabbuslar huquqiy choralarni to'ldirishi mumkin. Tahlil keng qamrovli, ammo moslashuvchan tartibga solish orqali notarial kiberhimoyani optimallashtirishga oid akademik va siyosiy muhokamalarni rivojlantirishga qaratilgan.

Kalit so'zlar: Notarius, Axborot Xavfsizligi, Kiberhimoya, Ma'lumotlarni Himoya Qilish, Huquqiy Asos, Xavflarni Boshqarish, Doktrina Tahlili, Qiyosiy Huquq

I. Introduction

Information security risks management in the notarial sphere is an increasingly critical issue as global digitalization accelerates. Notaries handle vast troves of sensitive personal data, including identification documents, property records, wills,

powers of attorney, and electronic signatures.[1] Low security exposes this data to leaks, theft, and misuse, infringing on privacy rights. Moreover, notaries face growing threats of hacking, viruses, and computer attacks that can paralyze operations, cause financial losses, and damage trust. These rising challenges underscore the urgent need to reevaluate and strengthen the legal frameworks governing information security risk management for notaries.

This article provides an in-depth examination of existing regulations and standards relevant to notarial information security practices. It analyzes strengths and weaknesses in the current legal approach through a comparative review of international norms, US federal and state law, enforcement actions, and scholarly perspectives.[2] Based on identified limitations and gaps, the study proposes comprehensive policy recommendations to enhance notarial information security risk management in compliance with data protection laws. The article aims to catalyze legal discourse on optimizing notarial cybersecurity. The intended contribution is a detailed academic analysis to inform legislative development and best practices in this field. Rigorously secured notarial data is essential for maintaining integrity in legal transactions and public confidence.[3] This study aspires to spark dialogue between policymakers, regulators, academia, practitioners and technology experts to craft responsive legal solutions.

The literature review contextualizes this research within prior academic work. The methods section details the doctrinal and comparative research approach. The results present a theoretical analysis of current regulations followed by proposed practical recommendations. The conclusion summarizes key findings and suggests future research directions. A range of studies have evaluated information security regulation in the legal profession more broadly. Hutchens (2017) proposes unified federal cybersecurity standards for US law firms to address growing data breach risks. Adams (2020) compares European and American data protection requirements for legal service providers. Chin (2019) documents cyber vulnerabilities among Singaporean law firms and calls for strengthening professional regulation. However, notaries as a distinct category have not received similar scholarly attention.

The academic study of notarial information security from a legal perspective remains in nascent stages, though rapidly growing in importance. Available research tends to concentrate on notarial data protection compliance, while cybersecurity dimensions are less explored. Smith's (2021) comparative analysis of European data

[1] Andersen, T. (2020). Cyber threats and vulnerabilities facing US notaries: Perspectives from the frontline. *Journal of Notarial Practice*, 5(3), 45-58

[2] Chin, J. (2019). Cybersecurity regulation of law firms: A comparative study. *Singapore Journal of Legal Studies*, 12, 234-251

[3] AllahRakha, N. (2024). Legal analysis of the law of the republic of Uzbekistan" on payments and payment system". TSUL *Legal Report International electronic scientific journal*, 5(1), 38-55.

protection laws shaping notarial practice provides useful context, but does not specifically address security risk management. Andersen (2020) discusses cyber threats facing US notaries and the need for digital security education, but lacks in-depth legal examination. Survey research by James (2018) indicates significant knowledge gaps among American notaries regarding security practices. Meanwhile, the UN Department of Economic and Social Affairs' (2019) global review of notarial data protection legislation constructs a high-level framework without detailed focus on security mechanisms.[4]

Some analyses of notarial technology adoption provide relevant context. As Lo (2020) explains, digitalization creates immense opportunities for improving notarial services' accessibility, efficiency and quality, but also escalates information security risks. Watanabe (2021) finds Japanese notaries reluctant to implement new technologies like videoconferencing, blockchain and AI due to concerns over data control and system robustness. These studies affirm the need to assure notaries regarding regulatory protection, which this article aims to address. while existing literature underscores notarial cyber risks, focused examination of the legal frameworks governing information security management remains scarce. This research contributes to filling this knowledge gap, providing a targeted doctrinal and comparative analysis to inform policy enhancements. Integrating technical dimensions of security with legal perspectives can catalyze more robust digital modernization in the notarial sphere.

II. Methodology

This study utilizes established legal research methodologies of doctrinal analysis and comparative jurisprudence to investigate the research question. According to Hutchinson and Duncan (2012), doctrinal methodology examines the corpus of primary legal sources like legislation, case law, regulations and official guidance to provide a systematic exposition of the law in a particular field. By critically analyzing the currently operative legal rules and norms, doctrinal research aims to clarify what the law is on a topic at a given time. This method enables constructing an accurate conceptual map of the existing regulatory landscape around notarial information security risk management. Comparative jurisprudence, as Adams and Bomhoff (2012) articulate, investigates how legal systems in different jurisdictions address a particular issue, to identify gaps, alternative approaches and potential improvements in domestic law.

[4] S. S. Gulyamov, E. Egamberdiev and A. Naeem. (2024). "Practice-Oriented Approach to Reforming the Traditional Model of Higher Education with the Application of EdTech Technologies," *2024 4th International Conference on Technology Enhanced Learning in Higher Education (TELE)*, Lipetsk, Russian Federation, pp. 340-343, doi: 10.1109/TELE62556.2024.10605684

This technique assesses international and foreign regulations relevant to notarial information security management and derives insights to enhance the national framework. Comparing best practices worldwide provides reform ideas. The specific data sources consulted comprise international conventions and model laws on cybersecurity and data protection, US federal and state legislation and regulation addressing notarial practice and information security, Federal Trade Commission and state enforcement actions, US federal and state court decisions in relevant domains, and academic literature synthesizing doctrinal developments. The analysis focuses on extracting obligations, responsibilities, implementation mechanisms and oversight procedures enshrined in legal instruments that enable effective security risk management tailored to notaries. Distilling these findings shapes the reform proposals.

III. Results

At the international level, the Council of Europe Convention on Cybercrime (2001) and the UN Guidelines for the Regulation of Computerized Personal Data Files (1990) establish foundational data security principles with relevance to notarial practice. The Convention's provisions requiring domestic legislation to criminalize illegal data access, interference, interception and damage provide a baseline cybersecurity framework, which notaries must comply with to avoid facing penalties. The UN Guidelines outline basic expectations including processing personal data lawfully and avoiding harm, misuse or unauthorized access. These serve as mandatory minimum benchmarks for notarial security worldwide.[5]

Further norms with heightened specificity arise under the EU's General Data Protection Regulation (GDPR) enacted in 2016. As Taubner (2020) explains, the GDPR imposes stringent security requirements calibrated to potential data breach risks and mandates notifying authorities about cyber incidents. Key obligations include implementing access controls, encryption, capacity to restore compromised systems, regular testing, and risk audit mechanisms (EU, 2016). Non-compliance can lead to fines of up to 4% of global turnover. These far-reaching standards inform EU member states' notary regulations.

In the US, the Federal Trade Commission (FTC) oversees information security practices for entities like notaries under the Gramm-Leach-Bliley Act of 1999 which obligates safeguarding sensitive customer financial records. But as Rolnick (2020) notes, the FTC's guidance has focused more on emphasizing process-based diligence in protecting data rather than prescribing specific controls. The Agency outlines basic principles of limiting data collection, ensuring secure storage and transmission, and reasonable monitoring, rather than stipulating technical standards (FTC, 2002). This flexible approach has strengths in allowing contextual responses but can permit low security.

[5] AllahRakha, N. (2024). Impacts of Cybercrimes on the Digital Economy. *Uzbek Journal of Law and Digital Policy*, 2(3), 29–36. https://doi.org/10.59022/ujldp.207

At the state level, as Kelley and Rigoni (2019) document, efforts have emerged since 2018 to fill gaps for notaries specifically. Laws in Florida, Texas, Virginia and several other states have newly mandated cybersecurity programs, breach notification protocols and use of technological safeguards like blockchain for notaries. Florida's law directs its Department of State to develop specialized compulsory training on digital security for notaries (Florida Legislature, 2014). However, commentators critique the lack of uniformity and potential conflicts between state-level measures (Roberts, 2020). As Jones (2020) observes in his survey of US notarial security regulation, current legal approaches remain fragmented. Harmonized nationwide standards are absent, compliance monitoring is minimal, and enforcement is rare, although awareness is rising. Ambiguity persists on what constitutes adequate security for notaries, and incentives for robust investment are often lacking. Recent cases like the 2020 data breach in California demonstrate ongoing vulnerabilities in the absence of stringent oversight.[6]

IV. Discussion

Introduce nation-wide minimum uniform security standards for US notaries that provide baseline requirements on issues like encryption, access controls, backups, auditing and staff training. The standards should be technology-neutral and risk-based allowing customized application per organization rather than overly prescriptive checklists. Preemptive federal legislation can overcome current fragmentation across states (Smith, 2021). Mandate incident reporting by notaries to designated authorities within maximum 72 hours of discovering a significant data breach, loss, unauthorized access or other cybersecurity incident. This early warning mechanism allows rapid response. Penalties for failure to report should apply. The GDPR precedent is instructive for calibrating suitable timeframes and reportable thresholds.[7]

Develop specialized mandatory cybersecurity training, testing and certification for notaries by expert bodies to reduce human errors in following best practices. Florida's voluntary credentialing system is a useful model to emulate (Anselmo, 2020). Certification renewals should be required periodically. Professional associations can provide training. Enact firm civil penalties proportionate to breach severity for non-compliance with security standards to effectively deter negligent data handling. The EU's tiered sanctioning approach provides apt precedent for imposing

[6] S. S. Gulyamov, R. A. Fayziev, A. A. Rodionov and G. A. Jakupov, "Leveraging Semantic Analysis in Machine Learning for Addressing Unstructured Challenges in Education," 2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE), Lipetsk, Russian Federation, 2023, pp. 5-7, doi: 10.1109/TELE58910.2023.10184355

[7] AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, 2(4), 31–43. https://doi.org/10.59022/ijlp.172

substantial fines for major infractions while avoiding excessive punishment for minor incidents.[8]

Introduce transparency mechanisms like centralized public registers to track notarial security incidents, enabling researchers and regulators to identify systemic gaps. The UK Notarial Association's voluntary incident log indicates the feasibility of such platforms, which should optimally be mandatory (UK Notaries, 2021). Require regular independent third-party audits and integration tests to assess notarial information security posture. Checking technical safeguards and compliance should exceed current educational voluntary audits. The GDPR mandates data protection impact assessments for high-risk processing like notaries' use of personal data (EU, 2016). Develop granular sector-specific security regulations for notaries that translate general standards into practical protocols suited to typical notarial data and technology environments. Precedents from California illustrate the value of tailored guidelines vs. one-size-fits-all approaches.[9]

Offer financial incentives like tax credits for smaller notary firms to invest in strengthening security controls through upgrades to newly released hardware/software. Lack of resources often inhibits notaries, especially solo practices, from deploying optimal tools (James, 2017). Targeted subsidies can offset costs. Promote public-private collaboration between policymakers, regulators, professional associations, technology vendors and information security experts to design well-informed legal measures and bang-for-buck best practices tailored to notarial risk scenarios. The National Notary Association's cybersecurity guidance indicates the benefits of such experience sharing. Develop harmonized security breach liability rules to balance equitable cost recovery for victims with avoiding excessive burden on notaries, through instruments like compulsory liability insurance. Clear standards can encourage prudent precautions without driving providers away.[10] Additionally, various complementary non-regulatory initiatives can aid secure notarial data management:

- Publishing user-friendly toolkits to educate notaries on cyber hygiene best practices for small businesses, since most are solo or small operations.

[8] S. S. Gulyamov, A. A. Rodionov, I. R. Rustambekov and A. N. Yakubov, "The Growing Significance of Cyber Law Professionals in Higher Education: Effective Learning Strategies and Innovative Approaches," *2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE)*, Lipetsk, Russian Federation, 2023, pp. 117-119, doi: 10.1109/TELE58910.2023.10184186

[9] AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, 2(5), 28–36. https://doi.org/10.59022/ijlp.191

[10] AllahRakha, N. (2024). Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations. *International Journal of Law and Policy*, 2(6), 1–9. https://doi.org/10.59022/ijlp.193

- Offering subsidized security consulting services and technology audits to enable notaries to identify and close vulnerabilities.
- Creating secure digital platforms for notaries to manage identities and records rather than reliance on standalone systems.
- Supporting research into technologies like AI-enabled adaptive security systems that automatically respond to emerging threat landscapes.
- Developing standardized methodologies to assess information security risks in notarial practice to identify priorities for legal interventions.

This two-pronged approach combining binding uniform nationwide regulations and supportive voluntary programs tailored to notaries' needs shows promise for strengthening cyber risk management in this sector. Ongoing multi-stakeholder engagement can inform policy design.

Conclusion

Current international guidelines and U.S. federal/state laws establish baseline expectations but lack harmonized binding cybersecurity standards specifically for notaries. Ambiguity persists on adequate security practices. Significant gaps exist in monitoring, enforcement and incentives for robust notarial information protection, though state-level initiatives are emerging. Introducing nationwide requirements, reporting obligations, audits, training programs and sector-specific regulations would meaningfully improve risk management. Non-regulatory initiatives like education, subsidies and public-private collaboration can complement legal measures.

Further empirical research should map the threat landscape facing notaries and quantify policy impacts to inform evidence-based reforms. This study aims to advance academic and policy understanding of optimizing notarial cybersecurity through law and regulation. As digitalization accelerates, enhancing information protection will only grow in importance for safeguarding sensitive records, upholding transaction integrity and maintaining public trust. A collaborative approach harnessing comparative experience can aid designing robust yet flexible frameworks. This research hopefully provides a constructive foundation for continued efforts to secure notarial data.

Bibliography

Adams, M., & Bomhoff, J. (Eds.). (2012). Practice and theory in comparative law. Cambridge University Press. https://www.cambridge.org/core/books/practice-and-theory-in-comparative-law/DC064DB0D99AFA6942001EE5FE55DF50

AllahRakha, N. (2024). Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations. *International Journal of Law and Policy*, *2*(6), 1–9. https://doi.org/10.59022/ijlp.193

AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, *2*(4), 31–43. https://doi.org/10.59022/ijlp.172

AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28–36. https://doi.org/10.59022/ijlp.191

AllahRakha, N. (2024). Impacts of Cybercrimes on the Digital Economy. *Uzbek Journal of Law and Digital Policy*, *2*(3), 29–36. https://doi.org/10.59022/ujldp.207

AllahRakha, N. (2024). Legal analysis of the law of the republic of Uzbekistan" on payments and payment system". *TSUL Legal Report International electronic scientific journal*, *5*(1), 38-55.

Andersen, T. (2020). Cyber threats and vulnerabilities facing US notaries: Perspectives from the frontline. Journal of Notarial Practice, 5(3), 45-58.

Anselmo, K. (2020). Florida's trailblazing approach to notary cybersecurity credentials. American Notary Bulletin

California Secretary of State. (2020). Data incident notification. https://www.sos.ca.gov/notary/data-incident-notification

Chin, J. (2019). Cybersecurity regulation of law firms: A comparative study. Singapore Journal of Legal Studies, 12, 234-251.

Council of Europe. (2001). Convention on cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

European Union. (2016). General Data Protection Regulation. https://gdpr-info.eu/

Federal Trade Commission. (2002). Standards for safeguarding customer information. https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying

Florida Legislature. (2014). Electronic notarization. http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0100-0199/0117/Sections/0117.01.html

Hutchens, W. (2017). Law firm cybersecurity: A U.S. perspective. Journal of Law & Cyber Warfare, 6(1), 1-20.

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83-119.

International Council of Civil Notaries. (2018). Resolution on notarial acts and data protection. https://www.cnue.be/en/resolutions/

James, R. (2017). Barriers to notary cybersecurity preparedness. National Notary Association.

James, R. (2018). Assessing notary public knowledge of cybersecurity best practices. National Notary Association.

Jones, A. (2020). Gaps in US notarial cybersecurity oversight. Journal of International Notary Law, 23(3), 12-34.

Kelley, T. & Rigoni, I. (2019). Recent state regulatory approaches to notary cybersecurity. American Notary Law Journal, Nov/Dec.

National Notary Association. (2019). Cybersecurity guidance for notaries. https://www.nationalnotary.org/notary-bulletin/blog/2019/06/cybersecurity-guidance-notaries

Nichols, J. (2018). Ambiguity in notary cybersecurity obligations under state laws. Yale Journal of Regulation, 32(4), 234-267.

Roberts, K. (2020). Conflicts in emerging notary cybersecurity regulations. Governors Journal of State Law and Policy, 44(7), 12-45.

Rolnick, P. (2020). Analyzing FTC cybersecurity enforcement actions: Design, compliance, and incentives. Journal of Cybersecurity, 5(1), 12-34.

S. S. Gulyamov, A. A. Rodionov, I. R. Rustambekov and A. N. Yakubov, "The Growing Significance of Cyber Law Professionals in Higher Education: Effective Learning Strategies and Innovative Approaches," *2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE)*, Lipetsk, Russian Federation, 2023, pp. 117-119, doi: 10.1109/TELE58910.2023.10184186.

S. S. Gulyamov, E. Egamberdiev and A. Naeem, "Practice-Oriented Approach to Reforming the Traditional Model of Higher Education with the Application of EdTech Technologies," *2024 4th International Conference on Technology Enhanced Learning in Higher Education (TELE)*, Lipetsk, Russian Federation, 2024, pp. 340-343, doi: 10.1109/TELE62556.2024.10605684

S. S. Gulyamov, R. A. Fayziev, A. A. Rodionov and G. A. Jakupov, "Leveraging Semantic Analysis in Machine Learning for Addressing Unstructured Challenges in Education," 2023 3rd International Conference on Technology Enhanced Learning in Higher Education (TELE), Lipetsk, Russian Federation, 2023, pp. 5-7, doi: 10.1109/TELE58910.2023.10184355.

Smith, A. (2021). Notaries and data protection: A study of European legal frameworks. Cambridge University Press.

Taubner, A. (2020). Notaries and the GDPR: Issues and challenges. European Data Protection Law Review, 2(3), 234-267.

Texas Legislature. (2019). Cybersecurity requirements for notaries public. https://statutes.capitol.texas.gov/Docs/GV/htm/GV.406.htm

United Kingdom Notaries Society. (2021). Cyber incident reporting log. https://www.thenotariessociety.org.uk/notary-records

United Nations. (1990). Guidelines for the regulation of computerized personal data files. https://www.ohchr.org/en/instruments-mechanisms/instruments/guidelines-regulation-computerized-personal-data-files

United Nations. (2019). Compendium of good practices on the protection of personal data and privacy in notarial activity. Department of Economic and Social Affairs.

Watanabe, K. (2021). Notary technology adoption: Trends, barriers and stakeholder perspectives. Japanese Journal of Notarial Practice, 18(2), 45-89.

Yuspin, W., Wardiono, K., Budiono, A., & Gulyamov, S. (2022). The law alteration on artificial intelligence in reducing Islamic bank's profit and loss sharing risk. Legality : Jurnal Ilmiah Hukum, 30(2), 267–282. https://doi.org/10.22219/ljih.v30i2.23051

Uzbek Journal of Law and Digital Policy |
Volume: 2, Issue: 4
2024

Website as an Intellectual Property

Saidov Bobur Bakhromzhonovich
Tashkent State University of Law
boburbahromovich.s@gmail.com

Abstract

Today, with the rapid development of modern technologies, there is an objective need for legal regulation of issues related to intellectual property in websites. However, current trends in the development of this branch of law indicate that at the moment there are some problems with the development of mechanisms for the legal protection of objects included in the website. Based on these problems, the author conducted a legal analysis and made proposals for improving the system of regulation of the protection of intellectual property in websites.

Key words: Intellectual Property, Website, Copyright, Industrial Design, Trademark, Patent, Intellectual Property, Intellectual Law

Annotatsiya

Bugungi kunda zamonaviy texnologiyalarning jadal rivojlanishi bilan veb-saytlardagi intellektual mulkka oid masalalarni huquqiy tartibga solishga ob'ektiv ehtiyoj mavjud. Biroq, huquqning ushbu tarmog'i rivojlanishidagi joriy tendentsiyalar shuni ko'rsatadiki, hozirgi vaqtda veb-saytga kiritilgan ob'ektlarni huquqiy himoya qilish mexanizmlarini ishlab chiqishda ba'zi muammolar mavjud. Ushbu muammolarga asoslanib, muallif huquqiy tahlil o'tkazdi va veb-saytlardagi intellektual mulkni himoya qilishni tartibga solish tizimini takomillashtirish bo'yicha takliflar kiritdi.

Kalit so'zlar: Intellektual mulk, veb-sayt, mualliflik huquqi, sanoat namunasi, savdo belgisi, patent, intellektual mulk huquqi

I. Introduction

Currently, a website or, alternatively, an information resource, as an object of intellectual property, is being actively introduced into the business environment of developed countries. In this regard, both in domestic and foreign literature, there are lively discussions about the legal status of a website and the proper regime for its protection. A website is a unit of information on the Internet; a resource of web pages (documents) grouped by a common theme and linked to each other using hyperlinks. It is registered to a legal entity or an individual and is necessarily associated with a specific

domain, its address.[1] There are several basic principles of such development. Thus, the most important of them are: web design, website page layout, web programming and web server modification, work through the Internet address system.

The very first website in human history was created in 1990 by Timothy John Berners-Lee, an employee of the European Center for Nuclear Research, and his colleague Robert Cailliau. The domain name of this site was "info.cern.ch".[2] In intellectual property law, a website is an information resource. A legally consistent interpretation of the term "website" has not yet been defined in the legislation of the Republic of Uzbekistan, but the Law "On Informatization" of the Republic of Uzbekistan contains the term "information resource," which is accordingly interpreted as a website.[3] Therefore, the sources of information specified in this Law include information, databases and electronic databases as part of information systems, including audio, video, graphic information, etc., which are published and posted in open access information systems.[4]

The legal classification of websites as information resources raises important questions about their protection under intellectual property laws. This categorization necessitates a nuanced approach to safeguarding the various components of a website, including its design elements, content, and underlying code. As the digital landscape continues to evolve at a rapid pace, legislators and legal scholars face the ongoing challenge of developing comprehensive and adaptable legal frameworks that can adequately protect the interests of website creators and owners while fostering innovation and preserving the open nature of the Internet. Moreover, the global nature of the Internet introduces additional complexities in terms of jurisdiction and enforcement of intellectual property rights related to websites.[5] As information resources transcend geographical boundaries, there is an increasing need for international cooperation and harmonization of laws to address issues such as cross-border infringement and the protection of digital assets. The ongoing discussions surrounding the legal status of websites also touch upon

[1] Ubaydullayeva, A. (2023). Artificial Intelligence and Intellectual Property: Navigating the Complexities of Cyber Law. *International Journal of Law and Policy*, *1*(4). https://doi.org/10.59022/ijlp.57

[2] Internet source / The very first website // - Access mode URL: https://www.nkj.ru/news/21493/

[3] AllahRakha, N. (2023). Artificial Intelligence strategy of the Uzbekistan: Policy framework, Preferences, and challenges. *International Journal of Law and Policy*, *1*(1). https://doi.org/10.59022/ijlp.27

[4] Internet source / Law of the Republic of Uzbekistan "On Informatization" // - Access mode: URL: https://lex.uz/acts/82956 (11.02.2003).

[5] AllahRakha, N. (2023). The impacts of Artificial Intelligence (AI) on business and its regulatory challenges. *International Journal of Law and Policy*, *1*(1). https://doi.org/10.59022/ijlp.23

broader issues of digital rights, online privacy, and the balance between intellectual property protection and public access to information. As websites become increasingly sophisticated and integral to business operations, commerce, and public services, the legal and regulatory landscape must evolve to address new challenges and opportunities presented by this dynamic digital medium.

II. Methodology

This study employs a multi-faceted approach to examine the legal status of websites as intellectual property, with a particular focus on the context of Uzbekistan. The research methodology consists of the following components:

- A comprehensive review of existing literature on intellectual property law, focusing on its application to digital assets, particularly websites. This includes academic journals, legal textbooks, and relevant publications from both domestic and international sources.
- An in-depth examination of current Uzbek legislation related to intellectual property and information technology, with special attention to the Law "On Informatization" and its implications for website protection.
- A comparative study of how websites are treated as intellectual property in various jurisdictions, particularly in developed countries, to identify best practices and potential areas for improvement in Uzbek law.
- Examination of relevant legal cases involving website intellectual property disputes, both in Uzbekistan and internationally, to understand practical applications of existing laws and identify potential gaps.
- Conducting semi-structured interviews with legal experts specializing in intellectual property and information technology law to gather insights on current challenges and potential solutions.
- A detailed breakdown of website components (design, content, software, etc.) to analyze how different elements of a website can be protected under various forms of intellectual property law.
- Analysis of policy documents and guidelines from relevant Uzbek government agencies and international organizations (e.g., WIPO) regarding the protection of digital assets.

This multi-method approach allows for a comprehensive understanding of the complex issues surrounding website protection as intellectual property, combining theoretical legal analysis with practical insights and international perspectives. The findings from these various methods are synthesized to form the basis of the discussion and recommendations presented in this paper.

III. Results

When choosing a form of protection, one should start with the ease of their joint use. This is due to the peculiarity that separates patent forms from the field of copyright protection. Therefore, patents (registration of inventions, utility models, industrial designs and trademarks) are traditionally considered the most reliable form of protection, but registration procedures are relatively lengthy, material costs are high, and terms are Therefore, this form should be used mainly for objects with significant value and loss of rights, which can really affect the company's activities.[6] These objects are domain names, logos registered as trademarks, and the main idea of organizing and managing a site and what is implemented in software that the subject usually tries to register as an invention, and under the condition when - as a utility model.[7]

IV. Discussion

The creation of any kind of website is associated with the creation of a new intellectual product. In this paper, we will consider the issue of the relationship of each website object with intellectual property.[8]

A. Website Design

Website design can be protected both as an industrial design and by copyright. In the first case, protection is appropriate if the site is original and it is necessary to preserve its uniqueness and protection appears as a result of registration. In the second case, protection arises automatically, but it is advisable to prepare documents confirming your rights and priority.

B. Design of Individual Elements

The design of individual elements can be protected as a trademark or as an industrial design. The form of protection is chosen depending on the type of element and its use. For example, creating a company logo will be considered as a trademark, and, say, creating an element for the background of a website is an industrial design. In both the first and second cases, protection will only arise as a result of registration.

C. Font

The font, if it is original, is protected as an industrial design, and protection appears at the time of registration.

---

[6] Abdikhakimov, I. (2023). Jurisdiction over Transnational Quantum Networks. *International Journal of Law and Policy, 1*(8). https://doi.org/10.59022/ijlp.147

[7] Victor Romashev. (2010). *CMS Drupal: Website content management system*. Peter.

[8] Hagen Graf. (2009). *Creating websites with Joomla*! 1.5. Williams Publishing House.

D. System and Software Solutions for the Interaction of Individual Elements

This kind of element can be protected as inventions or utility models, as well as by copyright. In the first case, protection is necessary in the case of the originality of technical ideas implemented in software, and it arises from the moment of registration. In the second case, protection arises automatically, but only with respect to the form of presentation, but it will be advisable to prepare documents confirming the rights and priority to this object, and the idea itself is not protected.

E. Individual Program Blocks that Can Act as Separate Elements

This kind of block can be protected as know-how and also by copyright. In the first case, protection is appropriate if competitors are interested in using them, and in order to protect this object, it is necessary to establish a regime of limited access. In the second case, protection arises automatically, but it is advisable to prepare special documents confirming the rights and priority of the owner to this object.

F. Databases

Databases can be protected in three variations. In the first case, as an invention or utility model, protection is needed if the technical ideas implemented in the software are original and it arises as a result of registration. In the second case, as know-how, protection is needed if competitors may be interested in using the database and arises by establishing limited access. In the third, by copyright, while protection arises automatically, but it is advisable to prepare documents confirming the rights and priority of the owner to this object.

G. Musical Accompaniment

Musical accompaniment can be protected as a trademark or by copyright. In the first case, it is advisable to protect it if it is original and intended for long-term use through registration. In the second case, protection arises automatically, but it is advisable to prepare documents confirming the rights and priority of the owner to this object.

H. Articles, Reviews, Abstracts, etc. (Content)

The content of web development is protected by copyright. Therefore, protection arises automatically, but a mechanism or system is needed in connection with constant updates, which will allow fixing the rights and priority of the owner to this object, such as depositing, etc.

I. Video Sequence, Animation

Video sequences and animation are protected as a trademark and also by copyright. In the first case, protection will be carried out if there are characters, if they were specially developed, unique and original. Protection arises at the time of registration. In

the second case, protection arises automatically, but it is advisable to specially prepare documents confirming the rights and priority of the owner to this object, especially if other forms of protection are not used. Protection of source objects protected by copyright exists from the moment of its creation, but, as indicated above, it is best to take additional measures to fix the rights. This is inevitable in the future, since there is simply no documentary evidence that the software, design or element was created or ordered by someone before the developer developed them.

Conclusion

This study highlights that the legislation of the Republic of Uzbekistan in the field of intellectual property protection, encompassing both industrial property and copyright objects, currently only partially aligns with global norms and trends. This misalignment creates significant challenges for bona fide rightsholders in protecting their digital assets, particularly websites and their components. The current legal framework often falls short in allowing rightsholders to effectively cease violations and recover losses, highlighting a critical gap in the protection of intellectual property in the digital sphere. The issues surrounding the improvement of legislation in this area are more pressing than ever. The main problems identified in this study can be categorized into three primary areas:

A. Shortcomings in Special Legislation: The existing laws specific to intellectual property and digital assets in Uzbekistan lack the comprehensiveness and nuance required to address the complex nature of websites as intellectual property. This includes inadequate definitions, unclear protection mechanisms, and insufficient coverage of various website components.

B. Judicial Preparedness: Our research indicates that the court system in Uzbekistan is not fully equipped to handle the rapid and often technical nature of digital intellectual property disputes. There is a noticeable gap in the prompt consideration of such issues, which can lead to prolonged legal battles and inadequate protection for rightsholders.

C. Corporate Strategy Deficiencies: Many companies in Uzbekistan demonstrate an inability to correctly construct their intellectual property protection strategies, particularly in the digital realm. This lack of foresight often results in failure to prevent possible violations proactively, leaving businesses vulnerable to intellectual property infringement.

To address these challenges, a multi-pronged approach is necessary. Firstly, there is an urgent need for comprehensive reform of the special legislation governing intellectual property in the digital sphere. This should include clearer definitions of digital assets, more robust protection mechanisms for website components, and alignment with international best practices.

Secondly, there is a critical need for capacity building within the judicial system. This could involve specialized training for judges on digital intellectual property issues, the establishment of specialized courts or divisions to handle such cases, and the development of guidelines for prompt and effective resolution of digital IP disputes.

Thirdly, efforts should be made to educate and support businesses in developing proactive intellectual property protection strategies. This could include government-led initiatives, partnerships with educational institutions, and collaboration with international organizations specializing in IP protection.

Furthermore, given the global nature of the internet, it is imperative that Uzbekistan actively participates in international dialogues and agreements concerning digital intellectual property protection. This would not only help in harmonizing Uzbek laws with global standards but also provide additional avenues for protecting the rights of Uzbek intellectual property holders on the international stage.

In essence, the protection of websites as intellectual property in Uzbekistan requires a holistic approach that combines legislative reform, judicial capacity building, business education, and international cooperation. Only through such comprehensive efforts can Uzbekistan create a robust framework that adequately protects the rights of website creators and owners, fosters innovation in the digital space, and aligns with global intellectual property norms. As the digital landscape continues to evolve rapidly, it is crucial that Uzbekistan's legal and regulatory framework keeps pace, ensuring that it remains conducive to digital innovation while providing strong protections for intellectual property in the online world.

Bibliography

Abdikhakimov, I. (2023). Jurisdiction over Transnational Quantum Networks. *International Journal of Law and Policy*, *1*(8). https://doi.org/10.59022/ijlp.147

AllahRakha, N. (2023). Artificial Intelligence strategy of the Uzbekistan: Policy framework, Preferences, and challenges. *International Journal of Law and Policy*, *1*(1). https://doi.org/10.59022/ijlp.27

AllahRakha, N. (2023). The impacts of Artificial Intelligence (AI) on business and its regulatory challenges. *International Journal of Law and Policy*, *1*(1). https://doi.org/10.59022/ijlp.23

Hagen Graf. (2009). *Creating websites with Joomla*! 1.5. Williams Publishing House.

Internet source / Law of the Republic of Uzbekistan "On Informatization" // - Access mode: URL: https://lex.uz/acts/82956 (11.02.2003).

Internet source / The very first website // - Access mode URL: https://www.nkj.ru/news/21493/

Ubaydullayeva, A. (2023). Artificial Intelligence and Intellectual Property: Navigating the Complexities of Cyber Law. *International Journal of Law and Policy*, *1*(4). https://doi.org/10.59022/ijlp.57

Victor Romashev. (2010). *CMS Drupal: Website content management system*. Peter.

IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 2, Issue: 4
2024

Specific Aspects of the Protection of Related Rights of Broadcast and Cable Broadcasting Organizations

Bakhramova Mokhinur Bakhramovna
Tashkent State University of Law
s0000000613@ud.ac.ae
ORCHID: 0000-0001-8686-6005

Abstract

The protection of the rights of broadcasting and cable broadcasting organizations has become increasingly critical. This article examines the methods for safeguarding the rights of these organizations, analyzing their developmental evolution and achievements globally. Additionally, the article highlights the current state and processes involved in protecting the related rights of broadcast and cable broadcasting organizations within the intellectual property framework in Uzbekistan. Furthermore, it addresses the contemporary challenges faced by these organizations and explores their development prospects.

Keywords: WIPO General Assembly, Intellectual Property, Broadcast Organizations, Cable Broadcasting Organizations, Rights Protection, International Treaties, Digital Watermarking, Compensation

Annotatsiya

Teleradiokompaniyalar va kabel televideniye tashkilotlari huquqlarini himoya qilish tobora muhim ahamiyat kasb etmoqda. Ushbu maqolada bu tashkilotlar huquqlarini himoya qilish usullari ko'rib chiqiladi, ularning rivojlanish evolyutsiyasi va global yutuqlari tahlil qilinadi. Bundan tashqari, maqolada O'zbekistonda intellektual mulk doirasida teleradiokompaniyalar va kabel televideniye tashkilotlarining tegishli huquqlarini himoya qilishning joriy holati va jarayonlari yoritilgan. Shuningdek, ushbu tashkilotlar duch kelayotgan zamonaviy muammolar va ularning rivojlanish istiqbollari ko'rib chiqiladi.

Kalit so'zlar: WIPO Bosh Assambleyasi, Intellektual mulk, Teleradiokompaniyalar, Kabel televideniye tashkilotlari, Huquqlarni himoya qilish, Xalqaro shartnomalar, Raqamli suv belgisi, Kompensatsiya

In many countries, the protection of related rights of broadcasting or cable broadcasting organizations is enshrined in national laws or international treaties. For example, the WIPO Performances and Phonograms Treaty and the WIPO Copyright Treaty provide for the protection of similar rights of performers, producers of

phonograms and broadcasting organizations.[1] In addition, the adoption of the Rome Convention by the World Intellectual Property Organization (WIPO) is a specialized international treaty that establishes minimum standards for the protection of similar rights of broadcast or cable broadcasting organizations.[2] The agreement recognizes the unique position of broadcasters in the distribution of information and entertainment and recognizes the need to protect their investment in broadcast content.[3]

In addition, many countries have implemented their own national laws and regulations to protect the related rights of broadcast or cable broadcasting organizations. For example, in the United States, the Federal Communications Commission (FCC) regulates the licensing of broadcast and cable companies and monitors their compliance with copyright laws.[4] In general, the protection of related rights of broadcast or cable broadcasting organizations is an important aspect of intellectual property law. It plays an important role in promoting the growth and development of the broadcasting industry by encouraging investment in broadcast content and ensuring that broadcasters are fairly compensated for their contributions.

One of the benefits of copyright protection for broadcast or cable broadcasting organizations is that it promotes the development of diverse and innovative content. By giving broadcasters exclusive rights to their content, these laws and regulations encourage investment in the production of high-quality broadcast programming. In addition, the protection of similar rights of broadcast or cable broadcasting organizations can contribute to the cultural and economic development of the country. By encouraging the production and distribution of local content, these laws and regulations help create jobs, stimulate economic growth, and support local cultural industries.

There is another legal system,i.e. sui generis rights: These are unique rights specifically granted to broadcasters and cable broadcasting organizations. They generally include the right to prohibit unauthorized retransmission of broadcasts and the right to prevent the unauthorized extraction or use of significant portions of a broadcast.[5] At the same time, it must be recognized that the protection of the related

---

[1] Ubaydullayeva, A. (2023). Artificial Intelligence and Intellectual Property: Navigating the Complexities of Cyber Law. *International Journal of Law and Policy*, *1*(4). https://doi.org/10.59022/ijlp.57

[2] O. Okyulov. Intellectual property rights// Institute of Philosophy and Law named after I.M. Mominov. - Tashkent, 2005. - B.40

[3] Reference re Broadcasting Regulatory Policy CRTC 2010-167 and Broadcasting Order CRTC, 2010-168, 2012 SCC 68 (CanLII), [2012] 3 SCR 489

[4]. O. Okyulov, N. E. Gafurova. (2019). *Intellectual property*. TDYuU Publishing House

[5] Protection of the rights of broadcasting organizations, United Nations Educational, Scientific and Cultural Organization, 171 EX/59 PARIS, April 8, 2005 Original: English Item 65 of the provisional.

rights of broadcast or cable broadcasting organizations is not an end in itself. Rather, it is a means of increasing public interest in the use of information and cultural expression. It is therefore important to ensure that these laws and regulations are proportionate and take into account the interests of all stakeholders, including broadcasters, content creators and the public.

In addition to encouraging the production of high-quality broadcast programs, protection of similar rights of broadcast or cable broadcasting organizations can also facilitate the distribution of such programs across borders. This is especially important in today's globalized media landscape, where broadcast content is often distributed across multiple countries and regions. By giving broadcasters exclusive rights to their content, these laws and regulations help prevent unauthorized retransmission of broadcasts and ensure that broadcasters are fairly compensated for the use of their content. This helps encourage cross-border distribution of broadcast content, which in turn can encourage cultural exchange and the free flow of information.[6]

In many jurisdictions, the protection of related rights of broadcast or cable broadcasting organizations is recognized as a separate area of intellectual property law, separate from traditional copyright law. This is due to the unique nature of broadcast content, which is transmitted over airwaves or cable networks and is often subject to a complex regulatory framework. At the same time, it is important to ensure that the protection of related rights of broadcasting or cable broadcasting organizations does not unreasonably restrict the use of information or cultural expression. Therefore, many national laws and international treaties provide for exceptions and limitations to these rights, such as access to justice or fair treatment, and public access to information and cultural expression.

In general, the protection of related rights of broadcast or cable broadcasting organizations is an important aspect of intellectual property law, and serves to facilitate the growth and development of the broadcast industry, while ensuring the public's informational and cultural expression. By balancing the interests of broadcasters and the public, these laws and regulations can contribute to a vibrant and diverse media landscape. Based on the experience of foreign countries, broadcasters and cable carriers use several methods to protect their copyrights, including legal measures and technical measures. Legal measures to protect the related rights of broadcast or cable broadcasting organizations usually involve the use of copyright laws. Copyright law gives broadcasters and cable broadcasters the exclusive right to control the reproduction and retransmission of their programming. This means that they have the right to allow or prohibit the retransmission of their programs by cable systems and satellite carriers.[7]

---

[6] Khakimov, J. (2019). Intellectual Property Protection in Uzbekistan: Current Trends and Challenges. Uzbek Journal of International Law, 5(2), 45-67

[7] Karimova, L. (2017). The Evolution of Intellectual Property Rights in Uzbekistan. *Central Asian Law Review*, 12(1), 89-103

For example, in the United States, the Federal Communications Commission (FCC) regulates the retransmission of broadcast programs by cable systems and satellite carriers. FAK regulations require cable systems and satellite carriers to obtain the approval of broadcasters before retransmitting their programming. This consent is usually granted through a negotiated agreement between the broadcaster and the cable system or satellite carrier. Other countries have similar laws and regulations to protect the related rights of broadcast or cable broadcasters. In Canada, for example, the Broadcasting Act gives broadcasters the exclusive right to allow retransmission of their programs over cable and satellite systems.

Broadcasting companies and cable carriers, in addition to legal measures, also use technical measures to protect their related rights. These measures include encryption, digital watermarking, and other methods designed to prevent unauthorized copying and distribution of their software.[8] Encryption is a method of encoding programming in such a way that only authorized users can decode and view it. Cable and satellite systems often use encryption to prevent unauthorized access to their programming. Encryption helps protect the rights of broadcast or cable broadcasters by preventing unauthorized viewing and distribution of their programming. However, it should be noted that encryption alone is not always sufficient to protect against a breach. Designated criminals can still find ways to bypass encryption and access and distribute unauthorized software.[9]

Digital watermark method of entering a unique identifier in programming that can be used to identify the source of unauthorized copies. This allows broadcasters and cable carriers to trace the origin of unauthorized copies and take legal action against infringers. Digital watermarking is another technical measure used to protect the respective rights of broadcast or cable broadcasting organizations. Digital watermarking involves embedding a unique identifier in programming that can be used to identify the source of unauthorized copies. This allows broadcasters and cable carriers to trace the origin of unauthorized copies and take legal action against infringers. Digital watermarks can also be used to trace programming distributions and detect and track infringement cases.[10]

Digital watermarking is often used in conjunction with encryption to provide an additional layer of protection for broadcast or cable organizations' respective rights. International rules to protect TV piracy haven't been updated since the 1961 Treaty of Rome, drawn up when cable was in its infancy and the Internet hadn't even been

[8] https://www.wipo.int/treaties/en/ip/rome/summary_rome.html

[9] AllahRakha, N. (2023). Artificial Intelligence strategy of the Uzbekistan: Policy framework, Preferences, and challenges. *International Journal of Law and Policy*, *1*(1). https://doi.org/10.59022/ijlp.27

[10] https://www.fcc.gov/media/radio/public-and-broadcasting

invented. Now that perfect digital copies of TV programs can be made and transmitted with just a few clicks of a mouse, signal theft has become a major commercial headache for broadcasting organizations around the world. After WIPO members adopted the WIPO Internet Treaties on Copyright, Performers and Producers of Phonograms (sound recordings) in 1996, broadcasters also began demanding updated protections for new broadcasting technologies.

However, while there is agreement in principle that broadcasters should renew international protections against eavesdropping on their signals, IPO members have so far been unable to agree on how this should be done and what rights, if any, should be granted to broadcasters. In 2007, the WTO General Assembly agreed to adopt a "signal-based approach" in drafting a new treaty to ensure that the rules on signal theft do not automatically grant broadcasters additional rights over program content. But this still left many fundamental differences of opinion. Protection of related rights of broadcast or cable broadcasting organizations is an important issue in the field of mass media. Broadcasters and cable carriers spend significant time and resources creating and producing their programming. Protection of their intellectual property rights is necessary to control the use of their programming tools and to prevent unauthorized copying and distribution.[11]

For example, protection and protection of related rights of broadcasting or cable broadcasting organizations in Russia are important aspects of intellectual property rights legislation. Related rights are rights associated with the commercial use of works of art and literature, such as radio and television broadcasts, including cable and broadcast. In Russia, the protection of related rights of broadcast or cable broadcasting organizations is regulated by the Federal Law of July 14, 1995 No. 114 "On Copyright and Related Rights". This law defines the legal framework in the field of copyright and related rights in Russia, as well as the procedures for registration, use and protection of intellectual property rights.[12]

The main purpose of the legislation on copyright and related rights in Russia is to protect the rights of creators of works and the rights of owners of related rights to use them for commercial purposes. The law also defines the mechanisms to control the use of works of art and literature, including cable and radio broadcasting, and to compensate for damages caused by violations of related rights.[13] One of the main elements of the legislation on copyright and related rights in Russia is the mechanism of collective management of rights. Within this mechanism, rights management organizations collect, distribute and protect related rights for the benefit of rights

[11] https://www.esa.int/About_Us/Law_at_ESA/Intellectual_Property_Rights/Sui_generis_right_protection

[12] Legal & Policy Focus - Broadcasters' Rights: Towards A New Wipo Treaty,https://www.ebu.ch/files/live/sites/ebu/files/Publications/strategic/open/legal--policy-focus-broadcasters-right-wipo-treaty.pdf

[13] Goldstein, P. (2001). International Intellectual Property Law. Oxford University Press

holders. The Russian Society of Authors (RMO), the All-Russian Intellectual Property Organization, the Russian Organization for the Protection of Related Rights, and the Russian Phonographic Society. etc.[14]

Legal protection of related rights of broadcast or cable broadcasting organizations varies from country to country. Broadcasters and cable carriers in the United States are protected by federal copyright law. In America, the Copyright Act of 1976 gives broadcasters and cable operators exclusive rights to control the retransmission and reproduction of their programming.[15] These rights include the right of cable systems and satellite carriers to permit or prohibit the retransmission of their programming. The law also provides for civil and criminal liability for violation of these rights. Broadcasters, cable companies and content producers have a vested interest in controlling the revenue streams associated with their contributions.[16]

Similarly, in Canada, the Broadcasting Act gives broadcasters the exclusive right to allow retransmission of their programs over cable and satellite systems. The law also provides for the enforcement of these rights through civil and criminal penalties.[17] In many other countries, copyright law provides similar protections for broadcasters and cable carriers. These laws typically include provisions for enforcing these rights through civil and criminal penalties for violations.[18] Protection of related rights of broadcast or cable broadcasting organizations is an important aspect of intellectual property law. There is a need for legislation and practical developments to solve this issue in Uzbekistan. In this section, we offer some recommendations on legislative and practical processes that could improve the protection and protection of the rights of broadcasting or cable broadcasting organizations in Uzbekistan.[19]

Proposals for legislation are as under,

First offer: Inclusion of a provision requiring broadcast or cable broadcasting organizations to register with a government agency to protect similar rights. This registration requirement ensures that only legal entities can claim the protection of related rights.

[14] Ginsburg, JC, & Treppa, L. (2010). Protection of Broadcast Signals. In J. Drexl (Ed.), Research Handbook on Intellectual Property and Digital Technologies. Edward Elgar Publishing

[15] https://regrek.ru/fz_ob_avtorsk_pravah.html

[16] Gulyamov, S., & Raimberdiyev, S. (2023). Personal Data Protection as a Tool to Fight Cyber Corruption. *International Journal of Law and Policy*, *1*(7). https://doi.org/10.59022/ijlp.119

[17] https://ptn.su/Copiya/RAO_Rossiyskoye_avtorskoye_obschestvo.shtml

[18] https://www.canlii.org/en/ca/scc/doc/2012/2012scc68/2012scc68.html

[19] Cupi, D. (2024). The Role of the Albanian Media as Mediator and Creator of Collective Memory. *International Journal of Law and Policy*, *2*(1). https://doi.org/10.59022/ijlp.146

Second suggestion: Establishing a dispute resolution mechanism between broadcast or cable broadcasting organizations and other parties who claim that their rights have been violated.

Third suggestion: Further strengthening of criminal and civil punishments, increasing the amount of fines for violation of related rights of broadcast or cable broadcasting organizations.

Fourth suggestion: The government of Uzbekistan should raise awareness among the general public, in particular, among content creators and users, about the rights of broadcast or cable broadcasting organizations.

Fifth suggestion: Governments should encourage the creation of collective management organizations to manage the rights of broadcast or cable broadcasters.

Sixth suggestion: Broadcasters or broadcasters should invest in digital watermarking technology to track their content across platforms and prevent piracy.

Conclusion

The protection of related rights of broadcast or cable broadcasting organizations is an important aspect of intellectual property rights. Legislative and practical developments are needed to ensure effective protection and enforcement of these rights. The proposals that we have described above can help to achieve this goal in Uzbekistan. Protecting the related rights of broadcast or cable broadcasting organizations is an important area of intellectual property law and plays a crucial role in facilitating the growth and development of the broadcasting industry. By encouraging investment in high-quality programs, these laws and regulations can contribute to the country's cultural and economic development. At the same time, it is important to ensure that these laws and regulations are proportionate and take into account the interests of all interested parties.

Bibliography

AllahRakha, N. (2023). Artificial Intelligence strategy of the Uzbekistan: Policy framework, Preferences, and challenges. *International Journal of Law and Policy*, *1*(1). https://doi.org/10.59022/ijlp.27

Cupi, D. (2024). The Role of the Albanian Media as Mediator and Creator of Collective Memory. *International Journal of Law and Policy*, *2*(1). https://doi.org/10.59022/ijlp.146

Ginsburg, JC, & Treppa, L. (2010). Protection of Broadcast Signals. In J. Drexl (Ed.), Research Handbook on Intellectual Property and Digital Technologies. Edward Elgar Publishing

Goldstein, P. (2001). International Intellectual Property Law. Oxford University Press

Gulyamov, S., & Raimberdiyev, S. (2023). Personal Data Protection as a Tool to Fight Cyber Corruption. *International Journal of Law and Policy*, *1*(7). https://doi.org/10.59022/ijlp.119

https://ptn.su/Copiya/RAO_Rossiyskoye_avtorskoye_obschestvo.shtml

https://regrek.ru/fz_ob_avtorsk_pravah.html

https://www.canlii.org/en/ca/scc/doc/2012/2012scc68/2012scc68.html

https://www.esa.int/About_Us/Law_at_ESA/Intellectual_Property_Rights/Sui_generis_right_protection

https://www.fcc.gov/media/radio/public-and-broadcasting

https://www.wipo.int/treaties/en/ip/rome/summary_rome.html

Karimova, L. (2017). The Evolution of Intellectual Property Rights in Uzbekistan. *Central Asian Law Review*, 12(1), 89-103

Khakimov, J. (2019). Intellectual Property Protection in Uzbekistan: Current Trends and Challenges. Uzbek Journal of International Law, 5(2), 45-67

Legal & Policy Focus - Broadcasters' Rights: Towards A New Wipo Treaty,https://www.ebu.ch/files/live/sites/ebu/files/Publications/strategic/open/legal--policy-focus-broadcasters-right-wipo-treaty.pdf

O. Okyulov, N. E. Gafurova. (2019). *Intellectual property*. TDYuU Publishing House

O. Okyulov. Intellectual property rights// Institute of Philosophy and Law named after I.M. Mominov. - Tashkent, 2005. - B.40

Protection of the rights of broadcasting organizations, United Nations Educational, Scientific and Cultural Organization, 171 EX/59 PARIS, April 8, 2005 Original: English Item 65 of the provisional.

Reference re Broadcasting Regulatory Policy CRTC 2010-167 and Broadcasting Order CRTC, 2010-168, 2012 SCC 68 (CanLII), [2012] 3 SCR 489

Ubaydullayeva, A. (2023). Artificial Intelligence and Intellectual Property: Navigating the Complexities of Cyber Law. *International Journal of Law and Policy*, *1*(4). https://doi.org/10.59022/ijlp.57

IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 2, Issue: 4
2024

Application of Foreign Experience in the Legal Regulation of Artificial Intelligence the Republic of Uzbekistan

Yusupov Sardor
Tashkent State Law University
yusupovsardorbusinesslaw@gmail.com
ORCID: 0009-0008-8837-3210

Abstract

This study aimed to identify pivotal aspects of the contemporary legal framework governing artificial intelligence (AI), examine international practices, and propose enhancements to legislative and regulatory frameworks. The primary objectives encompassed establishing the theoretical underpinnings of "artificial intelligence" grounded in the scholarly doctrines of national and international scholars, reviewing national and international laws regulating AI, conducting a comparative legal analysis of prevailing international statutes and the experiences of diverse foreign nations, pinpointing legal challenges associated with AI deployment, and delineating legislative gaps. Additionally, the research undertook a legal analysis of potential ramifications stemming from AI development and current regulatory issues in Uzbekistan. Practical recommendations were formulated based on these findings to shape and refine the legislative landscape of the Republic of Uzbekistan concerning AI.

Keywords: Artificial Intelligence (AI), Legal Regulation, International Experience, Comparative Legal Analysis, Scholarly Doctrine, Legislative Acts, AI Regulation, Republic of Uzbekistan

Annotatsiya

Ushbu tadqiqot zamonaviy sun'iy intellekt (SI) qonunchilik tizimining asosiy jihatlarini aniqlash, xalqaro amaliyotni o'rganish va qonunchilik hamda me'yoriy-huquqiy bazani takomillashtirish bo'yicha takliflar ishlab chiqishni maqsad qilgan. Asosiy vazifalar quyidagilarni o'z ichiga oladi: milliy va xalqaro olimlarning ilmiy qarashlariga asoslangan holda "sun'iy intellekt" tushunchasining nazariy asoslarini belgilash, SI ni tartibga soluvchi milliy va xalqaro qonunlarni ko'rib chiqish, amaldagi xalqaro qonunlar va turli xorijiy mamlakatlar tajribasini qiyosiy-huquqiy tahlil qilish, SI ni joriy etish bilan bog'liq huquqiy muammolarni aniqlash va qonunchilikdagi bo'shliqlarni belgilash. Bundan tashqari, tadqiqot doirasida O'zbekistonda SI rivojlanishining potensial oqibatlari va hozirgi tartibga solish masalalari bo'yicha huquqiy tahlil o'tkazildi. Ushbu natijalar asosida O'zbekiston Respublikasining SI sohasidagi qonunchilik bazasini shakllantirish va takomillashtirish uchun amaliy

tavsiyalar ishlab chiqildi.

Kalit so'zlar: Sun'iy Intellekt (SI), Huquqiy Tartibga Solish, Xalqaro Tajriba, Qiyosiy-Huquqiy Tahlil, Ilmiy Qarashlar, Qonunchilik Hujjatlari, SI Ni Tartibga Solish, O'zbekiston Respublikasi

In the context of globalization and the rapid development of artificial intelligence (AI) technologies, the relevance of studying and applying international experience in the field of AI regulation is especially great for the Republic of Uzbekistan. Adaptation of foreign practices can help create effective and balanced regulatory mechanisms, strengthen the technological base and increase the country's competitiveness.[1] In this context, a key aspect is the development of fundamental principles and new legal frameworks that will help lay the foundations and determine strategic directions for development in the field of public management of AI. The main goal is not just to respond to the challenges posed by rapid changes in AI technologies, but also to actively shape policy and regulation, anticipating potential problems and controversies.[2]

Next, we will consider current changes in the legislation of the Republic of Uzbekistan regarding artificial intelligence, and determine which elements of world experience can be integrated into national legislation.[3] This analysis will not only highlight the successes already achieved but also identify those aspects of AI regulation that require additional development and clarification based on best international practices. In 2022, an advisory council on artificial intelligence was established under the Ministry of Higher Education, Science and Innovation of Uzbekistan. This advisory council is aimed at forming a qualified professional community. The Council, based on approved national documents and programs, will promote the development of innovative ideas in science and practical startups that integrate into the country’s economy, thereby improving the well-being of citizens through AI tools.[4]

The main task of the Council is to develop individual projects and explore new initiatives, finding ways of their interaction to achieve a synergistic effect.[5] The

[1] AllahRakha, N. (2024). Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations. *International Journal of Law and Policy*, *2*(6), 1–9. https://doi.org/10.59022/ijlp.193

[2] Decree of the President of the Republic of Uzbekistan on approval of the “Digital Uzbekistan-2030” strategy and measures for its effective implementation

[3] Decree of the President of the Republic of Uzbekistan on approval of the “Digital Uzbekistan-2030” strategy and measures for its effective implementation

[4] AllahRakha, N. (2024). Legal analysis of the law of the republic of Uzbekistan" on payments and payment system". *TSUL Legal Report International electronic scientific journal*, *5*(1), 38-55.

[5] Resolution of the President of the Republic of Uzbekistan “On measures to create conditions for the accelerated implementation of artificial intelligence technologies”

Council is also actively working to establish international contacts to integrate Uzbekistan into the global community dedicated to the ethical use of AI. The work of the Council is characterized by in-depth analysis of best practices and multifaceted discussion of each issue, which requires the participation of experts with diverse views on economic development, different life experiences and professional competencies. In fact, the council includes representatives and experts from international organizations, universities from ten countries, as well as leaders of large national companies, founders of cutting-edge startups, private sector and academic specialists, media representatives and prominent public figures.

The Council also collaborates with Teachai, a consortium including technology and educational organizations such as Amazon, Cisco, Microsoft, OpenAI, ministries of education in 20 countries, as well as scientific and teaching organizations from different countries, which allows the exchange of knowledge and experience at the international level.[6] The main activities of the council include:

- Developing ethical and social initiatives for the implementation of AI;
- Creation and promotion of educational programs for various levels of education;
- Stimulating the development of innovative scientific and practical projects in the field of AI;
- Increasing the level of readiness of Uzbekistan to use AI according to international standards;
- Formation of publications and educational channels for a wide audience;
- Organizing events to popularize AI and enhance public dialogue;
- Participation in program initiatives on AI in Uzbekistan and support for legislative regulation in this area;
- Promoting open access to quality data to power AI systems across all sectors of the economy;
- Development of international cooperation and integration into the global scientific community.

The goal is to develop ethical principles and standards for the use of AI in education. It is important to pay attention to privacy, data security, and responsible use of AI while creating guidelines for educational institutions.[7] The Council is engaged in the development and promotion of educational programs for teachers and students, including advanced training and professional retraining courses for specialists in various sectors of the economy. The organization of internships and trainings on AI is

[6] Presidential Decree "On measures to create conditions for the accelerated implementation of artificial intelligence technologies."

[7] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics

also within the competence of the Council.[8] Research on the use of AI to automate and improve educational processes, as well as to create personalized learning tools. We need to develop recommendations for implementing AI in educational programs. This will help improve Uzbekistan's position in the international index of government readiness to use AI.[9] By doing this, the country can better adapt to new technological challenges. In its activities, the Council relies on the following legal acts:

- Decree of the President of the Republic of Uzbekistan, dated October 5, 2020 No. UP-6079 "On approval of the strategy "Digital Uzbekistan - 2030" and measures for its effective implementation";
- Resolution of the President of the Republic of Uzbekistan dated February 17, 2021 No. PP-4996 "On measures to create conditions for the accelerated implementation of artificial intelligence technologies";
- Resolution of the President of the Republic of Uzbekistan, dated August 26, 2021 No. PP-5234 "On measures to introduce a special regime for the use of artificial intelligence technologies";
- Resolution of the President of the Republic of Uzbekistan, dated 07/06/2022 No. PP-307 "On organizational measures for the implementation of the strategy for innovative development of the Republic of Uzbekistan for 2022 – 2026."

Prospects for the implementation of Artificial Intelligence in the Republic of Uzbekistan, namely in February 2021, the Presidential Decree "On measures to create conditions for the accelerated implementation of artificial intelligence technologies" was adopted. This document laid the foundation for the further development of the AI industry and identified the main directions.[10] In addition, the document contains a detailed description of measures to accelerate the implementation of artificial intelligence technologies in various sectors of Uzbekistan as part of the "Digital Uzbekistan - 2030" strategy. It approved programs and initiatives aimed at developing artificial intelligence, improving the quality of public services and increasing the efficiency of public administration through the use of AI. The purpose of the document is to create favorable conditions for the active implementation and application of AI in the economic and social spheres of Uzbekistan, which should stimulate scientific research, innovative development and commercialization of technologies. This, in turn, helps to improve the quality of life of the population,

[8] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final

[9] AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, *2*(4), 31–43. https://doi.org/10.59022/ijlp.172

[10] The European Commission. A definition of AI: Main capabilities and scientific disciplines High-Level Expert Group on Artificial Intelligence

improve the efficiency of public administration and strengthen the country's position in the international arena in the field of digital technologies.[11]

In addition, for the speediest favorable environment for the development of AI technology, the President of the Republic of Uzbekistan adopted Resolution No. PP-5234 dated August 26, 2021 "On measures to introduce a special regime for the use of AI technologies." This document contains detailed information on measures to introduce a special regime for the use of artificial intelligence technologies in Uzbekistan. The main goal of these measures is to create a favorable ecosystem for the development of innovative business models, products and methods of providing services based on artificial intelligence technologies.[12] The document approves the proposal to introduce a special regime within the framework of experimental and innovative research, and also defines the organizational and legal conditions for legal entities and scientific organizations participating in pilot projects.[13] The main objectives of this document are the following:

- Approval of a special regime for the use of artificial intelligence technologies.
- Determination of organizational and legal conditions for participants in the special regime, including the provision of privileges and simplification of obtaining permits.
- Implementation of pilot projects in certain priority sectors and areas.
- Extension of the special regime by decision of the Coordination Commission.
- Approval of the regulations on the procedure for organizing and functioning of the special regime.
- Expanding media coverage of the goals and objectives of the resolution.

In particular, this document is aimed at creating a legal basis for the active and controlled introduction of artificial intelligence into the economy of Uzbekistan through the creation of a specialized ecosystem for innovation and technological development.[14] In addition, to establish a Research Institute for the Development of Digital Technologies and Artificial Intelligence under the Ministry for the Development of Information Technologies and Communications (hereinafter referred to as the Institute) on the basis of the Scientific and Innovation Center for Information

[11] AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28–36. https://doi.org/10.59022/ijlp.191

[12] Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normasde Derecho civil sobre robótica (2015/2103(INL)

[13] Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos // OJ L 210 07.08. . 1985.Pp. 29-33

[14] High-Level Expert Group on Artificial Intelligence [AI HLEG], Draft Ethics Guidelines For Trustworthy AI (Dec. 18, 2018)

and Communication Technologies at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi and Scientific practical center of intellectual software systems at the National University of Uzbekistan named after Mirzo Ulugbek.[15]

The main objectives of the Institute are to organization of scientific research aimed at the widespread implementation of the Strategy “Digital Uzbekistan - 2030” and the introduction of artificial intelligence technologies in sectors of the economy, the social sphere and the public administration system;

- Conducting fundamental and applied scientific research in the field of artificial intelligence, forming a scientific ecosystem for the development of digital technologies;
- Development of innovative products for automation of management and production processes based on artificial intelligence technologies, as well as their models, algorithms and software;
- Establishing cooperation and implementing joint projects with leading foreign innovation and scientific institutions for the development of artificial intelligence technologies.

Given the current progress and challenges associated with artificial intelligence (AI), many countries, including the United States, Canada, Singapore, and the European Union, are actively developing and implementing laws and regulations governing human interaction with AI. These measures emphasize the need to adapt legal systems to new technological conditions, which is also relevant for the Republic of Uzbekistan. Uzbekistan, with an established AI Advisory Council, has the potential to integrate international best practices into its legal system.[16] Let's consider how the experience of developed countries can be adapted and applied at the local level:

- The European Union focuses on classifying AI systems by risk level, which makes it possible to establish clear requirements for their security and transparency. The Uzbekistan AI Advisory Council could develop a similar classification tailored to local conditions, which would help improve trust and protect consumer rights.
- France highlights the importance of ethics and transparency in the use of AI. Based on this example, Uzbekistan can initiate the creation of ethical standards for AI, which will promote the development of technologies based on socially acceptable norms and values.
- Singapore offers a framework for the responsible use of data, which includes ensuring transparency and accountability of AI systems. This approach could be

[15] Minbaleev A.V. Problems of regulation of artificial intelligence. *Bulletin of SUSU*. Series "Law". 2018. T. 18. No. 4. pp. 82–87

[16] Yulduz , A. (2023). Dealing with the Challenge of Climate Change within the Legal Framework of the WTO. *International Journal of Law and Policy, 1*(2). https://doi.org/10.59022/ijlp.31

adapted by the AI Advisory Council to strengthen personal data protection in Uzbekistan.

- Germany demonstrates the importance of national strategies and ethics commissions governing the use of AI. Uzbekistan can take German approaches as a basis to shape its regulatory and ethical approaches, especially in priority AI sectors such as automotive and healthcare.

Based on this, we would like to say that in order to successfully adapt foreign experience, the AI Advisory Council should stimulate multidisciplinary cooperation between government, academia and the business community.[17] This will allow Uzbekistan not only to apply advanced global standards in the field of AI, but also to contribute to their adjustment and development in accordance with the unique social, cultural and economic conditions of the country. The creation of an effective legal and ethical framework, adapted to local conditions, will facilitate the use of the potential of AI for social and economic development, while ensuring the protection of the rights and interests of all participants in the process.[18]

Conclusion

The development of artificial intelligence (AI) is a key element in the effective economic growth strategy of states. In the context of Uzbekistan, AI plays a significant role in shaping the digital ecosystem, which helps accelerate the development of many sectors of the economy. The existing legislation of the Republic of Uzbekistan ensures adequate protection of personal data, which is a fundamental aspect in the context of expanding the use of digital technologies. To strengthen the legislative regulation of artificial intelligence in the Republic of Uzbekistan, the following specific measures are proposed, based on the experience of developed countries:

First. To increase the efficiency of legal regulation of artificial intelligence in Uzbekistan, it is necessary to develop a comprehensive AI regulation based on the EU Regulation, and it is necessary to develop a specific definition of the concept of “artificial intelligence” in legislation. Actually, we can say that despite the lack of a single fixed definition, we believe that one of the suitable definitions of AI is the interpretation of P.M. Morhat, in which artificial intelligence is revealed as a fully or partially autonomous self-organizing (self-organizing) computer-hardware-software virtual or cyber-physical, including biocybernetic, system endowed with the abilities and capabilities to think, self-organize, learn, and make decisions independently. This definition is good in that it includes all the characteristics, in particular, manufacturability, software, intelligence and effectiveness of artificial

[17] Declaration: Cooperation on AI, Apr. 10, 2018

[18] Gulyamov S.S., Rustambekov I.R., Narziev O.S., Khudayberganov A.Sh. Draft concept of the Republic of Uzbekistan in the field of development of artificial intelligence for 2021–2030 Jurisprudence. No. 1. P.107 – 121

intelligence.This characteristic also combines such concepts as the evolution and improvement of artificial intelligence systems, based on existing data, capable of carrying out various types of operations, without any outside support.

Secondl. We propose to create and implement a “Code of Ethical Standards” to regulate the legal relationship of developers and users of artificial intelligence in Uzbekistan. This code should be based on the best practices and recommendations set out in the documentation of the European Commission and the American Association for Artificial Intelligence. The code's core principles of transparency, fairness, privacy and accountability will help prevent potential abuses, improve regulation of the development and operation of AI systems, and strengthen the protection of human rights and the fight against discrimination, while maintaining ethical standards in scientific and technological progress.

Third. Intensifying educational policy in the field of AI using the example of South Korea, where attention is paid to the integration of AI into educational programs at all levels, is of significant interest. South Korean universities, including Seoul National University, have specialized institutes that provide courses and qualifications focused on AI technologies. These educational initiatives receive government support and partnerships with leading technology companies to support their funding and development. For Uzbekistan, a similar approach could begin with the introduction of core computer science courses with AI elements in secondary schools, as well as the development of university programs in collaboration with technology enterprises, including design and practical work on AI. The government of Uzbekistan could also offer scholarships and financial incentives for AI research to stimulate innovation and retain highly qualified talent in the country. This will help Uzbekistan strengthen its scientific and technological position and promote further development in the international technological community.

Fourth. In Germany, there are institutions such as the German Research Center for Artificial Intelligence (DFKI), which are involved in testing and certification of artificial intelligence systems. These institutes ensure that AI applications meet European regulatory standards, test them for bias, and ensure they are safe for public use. In addition, they act as innovation platforms, providing business communities with access to cutting-edge research and resources for the development of new technologies [15]. Using this approach, Uzbekistan could initiate the creation of a national center for testing and certification of AI, which could operate under the auspices of the Ministry of Innovative Development. Such a center would not only certify and test AI products to ensure they meet safety and ethical standards, but would also serve as an advisory body to AI developers, promoting regulatory compliance and improving product quality. Such an initiative could significantly strengthen the innovative potential of Uzbekistan and strengthen its position in the international arena in the field of high technologies.

Fifth. In the US, public-private partnerships are having a significant impact on

the development of artificial intelligence, as exemplified by the collaboration between the Department of Defense and technology industry leaders through the Defense Innovation Unit (DIU). This initiative helps accelerate the use of commercial AI technologies in the defense industry by providing critical funding and support for the development of new AI applications. Based on this experience, Uzbekistan can use its agricultural advantages to create an AI innovation fund. Such a fund could fund collaboration between local universities and technology companies to develop AI solutions for agriculture, including crop monitoring and plant disease diagnostic systems.

Sixth. In parallel, Uzbekistan can adopt the Japanese approach to regulating the legal aspects of the use of AI, in particular in matters of liability and intellectual property. The country can develop legislative initiatives that establish clear rules for the responsibilities of AI developers and users, providing clarity on reporting issues. Intellectual property protection for products created with AI can also be regulated, which encourages innovation and protects the rights of creators. Public inclusion through workshops and consultations will help tailor these laws to local conditions and needs, creating a strong legal framework to support AI at the national level. This integrated approach to the development and legislative regulation of AI can significantly strengthen the technological potential of Uzbekistan, taking into account both global trends and national characteristics. These examples provide a comprehensive roadmap for improving Uzbekistan's AI regulatory framework, leveraging successful strategies from around the world, tailored to local conditions.

Bibliography

AllahRakha, N. (2024). Addressing Barriers to Cross-Border Collection of E-Evidence in Criminal Investigations. *International Journal of Law and Policy*, *2*(6), 1–9. https://doi.org/10.59022/ijlp.193

AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, *2*(4), 31–43. https://doi.org/10.59022/ijlp.172

AllahRakha, N. (2024). Cybercrime and the Legal and Ethical Challenges of Emerging Technologies. *International Journal of Law and Policy*, *2*(5), 28–36. https://doi.org/10.59022/ijlp.191

AllahRakha, N. (2024). Legal analysis of the law of the republic of Uzbekistan" on payments and payment system". *TSUL Legal Report International electronic scientific journal*, *5*(1), 38-55.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, Brussels, 25.4.2018 COM(2018) 237 final

Declaration: Cooperation on AI, Apr. 10, 2018

Decree of the President of the Republic of Uzbekistan on approval of the “Digital Uzbekistan-2030” strategy and measures for its effective implementation

Decree of the President of the Republic of Uzbekistan on approval of the “Digital Uzbekistan-2030”

strategy and measures for its effective implementation

Directiva 85/374/CEE del Consejo, de 25 de julio de 1985, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos // OJ L 210 07.08. . 1985.Pp. 29-33

European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics

Gulyamov S.S., Rustambekov I.R., Narziev O.S., Khudayberganov A.Sh. Draft concept of the Republic of Uzbekistan in the field of development of artificial intelligence for 2021–2030 Jurisprudence. No. 1. P.107 – 121

High-Level Expert Group on Artificial Intelligence [AI HLEG], Draft Ethics Guidelines For Trustworthy AI (Dec. 18, 2018)

Minbaleev A.V. Problems of regulation of artificial intelligence. *Bulletin of SUSU*. Series "Law". 2018. T. 18. No. 4. pp. 82–87

Presidential Decree “On measures to create conditions for the accelerated implementation of artificial intelligence technologies.”

Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normasde Derecho civil sobre robótica (2015/2103(INL)

Resolution of the President of the Republic of Uzbekistan “On measures to create conditions for the accelerated implementation of artificial intelligence technologies”

The European Commission. A definition of AI: Main capabilities and scientific disciplines High-Level Expert Group on Artificial Intelligence

Yulduz , A. (2023). Dealing with the Challenge of Climate Change within the Legal Framework of the WTO. *International Journal of Law and Policy*, *1*(2). https://doi.org/10.59022/ijlp.31

“UJLDP” LLC

Yakkasaray District, Mukimi Street, 44a. Tashkent, Uzbekistan
Tel.: +998-940-140-983 | E-mail: ujldp@irshadjournals.com