WORLD CONFERENCE ON STUDENT - CENTERED LEARNING APPROACHES

CONSTITUTIONAL AND LEGAL SAFEGUARDS FOR ATTORNEY–CLIENT CONFIDENTIALITY IN THE DIGITAL AGE

Abdurayimov Mukhammad Suvankul ugli
Lecturer at the Department of Constitutional Law,
Tashkent State University of Law
E-mail: abdurayimov.mukhammad@gmail.com
ORCID: 0009-0000-7965-7512

Abstract: The digitalization of legal practice has expanded opportunities for communication, document management and legal research, while also increasing risks of unauthorized access to confidential information. This paper examines attorney–client confidentiality as a condition for the effective exercise of the right to qualified legal assistance and the protection of human rights. Drawing on Uzbekistan's constitutional and legislative framework, it analyses challenges related to electronic storage, cloud services, digital devices and artificial intelligence. It proposes a doctrinal model termed "digital immunity of a lawyer", understood as a combination of legal, procedural-organizational and technical safeguards. The paper argues that this concept should not mean absolute immunity from lawful procedural measures; rather, it should support lawful, proportionate and controlled access to digital information while protecting materials covered by professional confidentiality. It also emphasizes the need to preserve the lawyer's professional judgment and responsibility when using artificial intelligence.

Keywords: attorney–client confidentiality; qualified legal assistance; constitutional safeguards; digitalization; digital immunity of a lawyer; personal data; artificial intelligence; Uzbekistan.

INTRODUCTION

Digital technologies have become an integral part of legal practice. Electronic

communication, cloud storage, online platforms and artificial intelligence tools can make legal research and document preparation more efficient. At the same time, they create new risks, including unauthorized access to electronic files, disclosure through third-party services, insecure storage, data breaches and unintended retention of confidential information.

Attorney–client confidentiality is not merely a professional or ethical obligation. It is an important condition for the practical exercise of the right to qualified legal assistance. A client must be able to disclose relevant facts to a lawyer without unreasonable fear that the information will be exposed to unauthorized persons. If confidentiality is weakened, clients may withhold information, limiting the lawyer's ability to provide effective assistance and protect their rights.

In Uzbekistan, the constitutional recognition of the right to qualified legal assistance and the statutory framework governing advocacy, guarantees of lawyers' activities and personal data provide the principal legal basis for addressing this issue [1–5]. However, traditional safeguards must be applied to circumstances in which confidential information is stored, copied, transmitted and processed across multiple digital environments.

The purpose of this paper is to identify the constitutional and legal significance of attorney–client confidentiality in digital practice and to propose directions for strengthening its protection. The study uses formal-legal, systemic and comparative methods and is doctrinal in nature; it does not claim original empirical or statistical findings.

MAIN PART

1. Confidentiality as a condition for effective legal assistance

The right to qualified legal assistance is meaningful only where a person can communicate with a legal professional under conditions that protect the confidentiality of their interaction. Confidentiality allows a lawyer to obtain facts necessary to assess

a case, identify legal risks and formulate a position. It also supports trust in the legal profession and the effective protection of other rights. Attorney–client confidentiality should therefore be understood not only as an individual professional duty but also as a functional safeguard supporting constitutional rights.

The Constitution of the Republic of Uzbekistan recognizes the right to qualified legal assistance and establishes constitutional foundations for the legal profession [1]. The Law "On Advocacy" and the Law "On Guarantees of Advocacy and Social Protection of Advocates" further regulate professional duties and safeguards [2; 3]. These rules must be applied to modern forms of information, including electronic correspondence, digital files, backups and cloud-based systems.

Attorney–client confidentiality and personal data protection are related but not identical. Personal data law regulates information relating to an identifiable individual [4], while professional confidentiality may cover a wider range of information connected with seeking legal assistance, communications, documents and legal strategy. The two regimes may overlap in digital practice and should be applied consistently without treating them as interchangeable.

2. Digital risks and procedural safeguards

Digital information is often duplicated across devices, e-mail accounts, cloud services, backups and third-party applications. A device used by a lawyer may contain information relating to several clients and matters. Unrestricted access to an entire device or data set may therefore expose confidential material unrelated to the purpose of a particular procedural measure.

The appropriate response is not absolute immunity for lawyers' devices or a prohibition on lawful action by competent authorities. Instead, the legal framework should reconcile legitimate procedural objectives with professional confidentiality. Potential safeguards include defining the scope of relevant information, separating protected material from unrelated data, restricting access to authorized persons,

documenting access and establishing a procedure for resolving disputes over confidentiality.

Digitalization of advocacy in Uzbekistan has been supported by measures to introduce information and communication technologies into legal practice [5]. Such developments may improve access to legal services, but they should be accompanied by clear rules on access, storage, transfer and protection of confidential information. The fact that information is stored electronically should not, by itself, reduce its legal protection.

3. The proposed concept of "digital immunity of a lawyer"

This paper proposes the doctrinal concept of "digital immunity of a lawyer" to describe the integrated protection required in digital legal practice. It means a combination of legal, procedural-organizational and technical safeguards designed to protect a lawyer's digital professional environment and prevent unjustified access to information covered by professional confidentiality. This is a proposed analytical concept, not a claim that current Uzbek legislation already recognizes a separate legal institution under this name.

The model has three elements. First, legal safeguards define the protected character of confidential information, permissible grounds and limits of access, professional duties and consequences of unlawful disclosure. Second, procedural-organizational safeguards establish how protected information should be identified, separated, accessed and handled during legally authorized procedures. Third, technical safeguards may include access controls, encryption, secure backups, multi-factor authentication and digital-security training.

These elements are interdependent. Technical security cannot replace legal rules and accountability, while statutory confidentiality obligations may be insufficient without reasonable measures to secure electronic systems. The concept should

therefore be understood as a framework for coordinating existing safeguards and identifying areas where further legal and professional development is needed.

4. Artificial intelligence and professional responsibility

Artificial intelligence can assist lawyers in legal research, document organization and preliminary analysis. However, generated outputs may contain errors, outdated legal references or incomplete reasoning. A lawyer should verify sources and conclusions before relying on AI-generated material in advice or documents submitted to a court or public authority.

The Human-in-the-loop approach is relevant because AI may support professional work, but the lawyer retains control, evaluates the output and makes the final legally significant decision. Responsibility for the legal position should not be transferred to an automated system. Professional guidance on generative AI highlights issues such as competence, confidentiality and verification of results [6; 7].

A further concern arises when confidential client information is uploaded to external AI services. Before using such services, lawyers should assess data storage, access by providers or third parties, possible reuse of uploaded information and deletion and security controls. Professional guidance should therefore address confidentiality, personal data, verification of AI outputs and continuing professional responsibility. International and foreign approaches may provide comparative reference points, but they should be adapted to Uzbekistan's legal system rather than copied mechanically [6–8].

CONCLUSION

The digitalization of legal practice creates new opportunities but also new challenges for attorney–client confidentiality. Confidentiality should be treated as a condition for effective qualified legal assistance and the protection of human rights. Existing legal guarantees must be applied with due regard to digital storage, duplication, transmission and the involvement of third-party services.

The proposed concept of "digital immunity of a lawyer" offers a doctrinal framework for understanding the relationship between legal, procedural-organizational and technical safeguards. It does not imply absolute immunity from lawful procedural measures. Its purpose is to support lawful, proportionate and controlled access while preventing unjustified disclosure of protected information.

Further development should focus on procedural rules for handling digital materials, coordination between professional confidentiality and personal data protection, practical guidance for the secure use of AI, and continuing education in digital security. Such measures could strengthen constitutional and legal protection of attorney–client confidentiality in Uzbekistan's evolving digital environment.

REFERENCES

1. Constitution of the Republic of Uzbekistan. Adopted by referendum on 30 April 2023.
2. Law of the Republic of Uzbekistan No. 349-I of 27 December 1996, "On Advocacy".
3. Law of the Republic of Uzbekistan No. 721-I of 25 December 1998, "On Guarantees of Advocacy and Social Protection of Advocates".
4. Law of the Republic of Uzbekistan No. ZRU-547 of 2 July 2019, "On Personal Data".
5. Resolution of the President of the Republic of Uzbekistan No. PP-263 of 30 May 2022 on the introduction of information and communication technologies into advocacy.
6. American Bar Association. Formal Opinion 512: Generative Artificial Intelligence Tools. 29 July 2024.
7. The Florida Bar. Ethics Opinion 24-1: Generative Artificial Intelligence. 19 January 2024.

8. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).