COLLECTION AND PRESERVATION OF ELECTRONIC EVIDENCE: COMPARATIVE ANALYSIS OF INDIA AND UZBEKISTAN

Kosimov Doniyorjon Bakhtiyor ugli
Master's degree student at Tashkent State University of Law

Annotation: This article examines the legal and procedural mechanisms for the collection and preservation of electronic evidence in India and Uzbekistan, comparing statutory search-and-seizure powers and forensic institutions in each country. Using comparative-legal analysis, it identifies the absence of a unified chain-of-custody standard as a structural gap shared by both systems and proposes targeted legislative recommendations.

Key words: electronic evidence, digital forensics, collection of evidence, chain of custody, preservation of evidence, cybercrime, comparative law, India, Uzbekistan.

Аннотация: В статье рассматриваются правовые и процессуальные механизмы сбора и сохранения электронных доказательств в Индии и Узбекистане, сопоставляются полномочия по обыску и выемке, а также судебно-экспертные институты двух стран. На основе сравнительно-правового анализа выявлено отсутствие единого стандарта цепочки хранения доказательств как общая структурная проблема, предложены практические рекомендации.

Ключевые слова: электронные доказательства, цифровая криминалистика, сбор доказательств, цепочка хранения, сохранность доказательств, киберпреступность, сравнительное право, Индия, Узбекистан.

Annotatsiya: Maqolada Hindiston va O'zbekistonda elektron dalillarni to'plash va saqlashning huquqiy-protsessual mexanizmlari qiyoslanadi, ikki davlatdagi qidiruv-olib qo'yish vakolatlari va sud-ekspertiza institutlari tahlil qilinadi. Qiyosiy-huquqiy tahlil asosida har ikki tizimga xos umumiy kamchilik — yagona saqlash zanjiri (chain of custody) standartining yo'qligi — aniqlanib, amaliy tavsiyalar ilgari surilgan.

Kalit so'zlar: elektron dalillar, raqamli sud-ekspertiza, dalillarni to'plash, saqlash zanjiri, dalillarni saqlash, kiberjinoyatchilik, qiyosiy huquq, Hindiston, O'zbekiston.

Introduction

A previous stage of this research addressed the authentication and admissibility of electronic evidence in India and Uzbekistan; the present article extends that analysis backward to the collection and preservation stage, on the premise that the reliability of evidence presented at trial cannot exceed the reliability of the procedures by which it was obtained and stored.[1]

India and Uzbekistan were again selected for comparison because they represent, respectively, the common law and post-Soviet civil law traditions, yet both have undergone significant digitalisation of investigative and judicial practice over the past decade. The article compares the statutory powers of search and seizure, the institutional actors responsible for forensic handling of digital media, and the extent to which each system codifies chain-of-custody requirements, before offering recommendations for reform.

[1] S. Mason and D. Seng (eds.), Electronic Evidence, 4th edn (University of London, 2017), ch. 2.

Research methodology

The functional comparative approach was chosen over a purely textual comparison because the two jurisdictions regulate collection and preservation through formally different instruments — India through criminal procedure combined with specialised IT legislation, Uzbekistan through general criminal procedure supplemented by departmental acts.[2] A functional approach makes it possible to identify how each system answers the same practical question — how the integrity of digital evidence is guaranteed between seizure and trial — regardless of the legislative technique used. This methodology also allows for the evaluation of the practical effectiveness of legal mechanisms rather than merely comparing statutory language. By focusing on the functions performed by legal rules, similarities and differences in procedural safeguards become more apparent. Such an approach facilitates the identification of best practices that may be adapted to improve national legislation and strengthen the reliability and admissibility of digital evidence in criminal proceedings.

Research results

In India, collection of electronic evidence is governed primarily by the general search-and-seizure provisions of the Code of Criminal Procedure, read together with the Information Technology Act, 2000. In practice, digital evidence is collected by cyber-crime cells attached to state police forces and by forensic science laboratories, which apply internally developed standard operating procedures for imaging storage media, including write-blockers and hash-value computation to demonstrate that a forensic copy is identical to the original.

In Uzbekistan, collection of electronic evidence proceeds under the general provisions of the Criminal Procedure Code governing search and seizure of objects and documents, applied by analogy to digital media in the absence of a dedicated statutory chapter[3]. Forensic-technical examination is conducted by the Republican Centre for Forensic Expertise and specialised units of the Ministry of Internal Affairs, with the Cybersecurity Agency playing an increasingly prominent role in cases involving critical information infrastructure.

Recommendations

1. Uzbekistan should strengthen its legal framework governing electronic evidence by introducing either a separate chapter within the Criminal Procedure Code or a comprehensive subordinate regulation dedicated specifically to digital evidence. Such legislation should establish uniform minimum technical standards for the identification, collection, preservation, and documentation of electronic evidence. In particular, it should require the mandatory use of cryptographic hash-value verification to ensure data integrity, the application of certified write-blocking devices during forensic acquisition, and the maintenance of a standardised digital chain-of-custody record documenting every stage of evidence handling from seizure to its presentation before the court.

2. India should modernise its existing legal framework to address the growing reliance on cloud computing and third-party digital service providers. While the current procedural rules regulate the seizure of physical electronic devices, they provide limited guidance on obtaining

[2] Information Technology Act 2000 (India); Code of Criminal Procedure 1973 (India), ss. 91, 93, 100; Criminal Procedure Code of the Republic of Uzbekistan; Law of the Republic of Uzbekistan No. 562-II 'On Electronic Document Circulation' (2004).
[3]); Code of Criminal Procedure 1973 (India), ss. 91, 93, 100; Criminal Procedure Code of the Republic of Uzbekistan; Law of the Republic of Uzbekistan No. 562-II 'On Electronic Document Circulation' (2004).

and preserving remotely stored data. Therefore, the law should expressly regulate the collection of cloud-based evidence by introducing clear procedures for issuing preservation orders to internet service providers, cloud storage companies, and other intermediaries. Such measures would help prevent the alteration or deletion of digital data while ensuring that investigators obtain judicial authorisation through established legal procedures.

3. Both Uzbekistan and India should formally incorporate internationally recognised digital forensic standards into their domestic legal systems. In particular, standards such as ISO/IEC 27037:2012 should be recognised as authoritative guidance for the identification, collection, acquisition, and preservation of digital evidence. The adoption of internationally accepted technical standards would promote consistency in forensic practice, improve the reliability and admissibility of electronic evidence before courts, and facilitate international cooperation in cross-border cybercrime investigations.

4. Continuous professional education on digital evidence should become an institutional requirement for all criminal justice actors in both jurisdictions. Regular and specialised training programmes should be developed for investigators, prosecutors, judges, and forensic experts to improve their understanding of modern digital technologies, forensic acquisition methods, evidence preservation techniques, and the legal requirements governing electronic evidence. Strengthening institutional expertise would reduce procedural errors, increase judicial confidence in digital evidence, and enhance the overall effectiveness and fairness of criminal investigations involving electronic information.

5. Bilateral and multilateral cooperation mechanisms should be further strengthened to facilitate the timely preservation, exchange, and cross-border transfer of electronic evidence in cases involving cybercrime and transnational offences. Given that electronic evidence is frequently stored across multiple jurisdictions and may be controlled by foreign service providers, effective international cooperation has become essential for successful criminal investigations. Both Uzbekistan and India should enhance cooperation through mutual legal assistance mechanisms, bilateral agreements, and participation in international frameworks that enable the prompt preservation and lawful transfer of digital evidence. Strengthening these mechanisms would reduce procedural delays, improve the efficiency of cross-border investigations, and ensure that electronic evidence remains authentic, reliable, and admissible throughout criminal proceedings.

Conclusion

The comparative analysis demonstrates that although India and Uzbekistan approach the collection and preservation of electronic evidence through different legislative techniques, both face a common structural deficiency: the absence of a unified, technology-neutral standard governing the integrity of digital evidence from seizure to trial. India's more elaborate departmental framework offers technical detail that Uzbekistan could draw upon in codifying its own chain-of-custody requirements, while Uzbekistan's centralised forensic institutions offer a model of consolidation India's more fragmented structure could consider. Strengthening these earlier procedural stages is a necessary complement to the reforms in authentication doctrine addressed in the preceding stage of this research.

List of references

1. Information Technology Act, 2000 (India). *Official source:* https://www.indiacode.nic.in/handle/123456789/13116?view_type=browse

2. Indian Evidence Act, 1872, as amended by the Information Technology Act, 2000. *Official source: https://www.indiacode.nic.in/bitstream/123456789/2188/1/A1872-1.pdf*
3. Code of Criminal Procedure, 1973 (India), ss. 91, 93, 100. *Official source: https://www.indiacode.nic.in/bitstream/123456789/15272/1/the_code_of_criminal_procedure,_1973.pdf*
4. Criminal Procedure Code of the Republic of Uzbekistan. *Official source: https://lex.uz/docs/111463*
5. Law of the Republic of Uzbekistan No. 611-II 'On Electronic Document Circulation' (2004). *Official source: https://lex.uz/docs/165074*
6. Presidential Decree of the Republic of Uzbekistan No. UP-6079 'On the Strategy of Digital Uzbekistan 2030' (2020). *Official source: https://lex.uz/docs/5031048*
7. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1. *Official source: https://indiankanoon.org/doc/172105947/*
8. Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473. *Official source: https://indiankanoon.org/doc/187283766/*
9. ISO/IEC 27037:2012, 'Guidelines for identification, collection, acquisition and preservation of digital evidence'. *Official source: https://www.iso.org/standard/44381.html*
10. UNCITRAL, 'Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods' (United Nations, 2009). *Official source: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/08-55698_ebook.pdf*
11. Council of Europe, Cybercrime Convention Committee, 'Guidance Notes' (Council of Europe). *Official source: https://www.coe.int/en/web/cybercrime/guidance-notes*
12. S. Mason and D. Seng (eds.), Electronic Evidence, 4th edn (University of London, 2017). *Official source: https://uolpress.co.uk/book/electronic-evidence/*