The American Journal of Political Science Law and Criminology
ISSN 2693-0803 Volume 08 - 2026

International Legal Standards for The Digitalization of Investigative Activity and The Experience of Foreign States

Boboev Mirshod Murotovich
Doctor of Philosophy (PhD) in Law, Head of the Digital Technologies Center, Prosecutor General's Office of the Republic of Uzbekistan, Uzbekistan

Received: 28 Feb 2026 | Received Revised Version: 16 Mar 2026 | Accepted: 04 Apr 2026 | Published: 30 Apr 2026

Volume 08 Issue 04 2026 | Crossref DOI: 10.37547/tajpslc/Volume08Issue04-14

Abstract

The article examines the international legal standards governing the digitalization of investigative activity and analyses the experience of the United States, the United Kingdom, Germany, Estonia, Singapore, the Republic of Korea and China in constructing electronic pre-trial proceedings. The author argues that digitalization is not a technical modernization of the work of the bodies of inquiry and preliminary investigation but a transformation of the procedural form itself, which for that reason requires an autonomous basis within criminal procedure legislation rather than within subordinate departmental regulation. On the basis of a comparative-legal analysis, two reform models are distinguished: the procedural-law-first model, in which the electronic form of proceedings is regulated by the code of criminal procedure before technical deployment, and the technology-first model, in which the information system precedes its own legal regulation.

Keywords: Digitalization of investigative activity; electronic criminal case; digital evidence; international legal standards; Budapest Convention; artificial intelligence in criminal procedure; digital forensics; proportionality; protection of personal data; "E-tergov".

Cite This Article: Boboev Mirshod Murotovich. (2026). International Legal Standards for The Digitalization of Investigative Activity and The Experience of Foreign States. The American Journal of Political Science Law and Criminology, 8(04), 81–84. https://doi.org/10.37547/tajpslc/Volume08Issue04-14

1. Introduction

The digitalization of pre-trial proceedings has become a transformation

of procedural form rather than a technical modernization. When investigative acts are created, signed, transmitted and stored electronically, authenticity, procedural deadlines, equality of arms and control over coercive measures depend on the architecture of the information system. For Uzbekistan, this issue is especially relevant in connection with the "E-tergov" system established under Presidential Decree No. DP-204 of 3 November 2025. Although the strategic framework provides for electronic criminal proceedings, digital supervision and artificial intelligence, procedural legislation still requires further development concerning

the electronic criminal case, the legal force of electronic procedural documents and the legal significance of automated analysis.

1. Concept and structure of digitalization of investigative activity

Digitalization differs from informatization.

Informatization transfers

an unchanged procedure into electronic form; digitalization reconstructs the procedure around data and therefore creates new legal objects. Three levels should be distinguished: instrumental, procedural and analytical. The instrumental level includes electronic document circulation, digital signatures and remote interaction. The procedural level includes the electronic criminal case, digital evidence and electronic registration of crime reports. The analytical level includes artificial intelligence and big-data tools capable of influencing procedural decisions.

The electronic criminal case cannot be treated merely as an archive of scanned documents. Its legal value depends on a legally significant digital trace recording the author, time, electronic signature, grounds, subsequent modifications, transmission and supervisory actions. Such a trace can make the chronology of proceedings independently verifiable. Without it, an electronic file may be less reliable than a paper file because alterations may occur without visible physical evidence.

Digital evidence requires documented identification, collection, acquisition and preservation, including integrity verification and an appropriate chain of custody. The ISO/IEC 27037 and 27041–27043 standards provide a technical framework for these processes. As R. Stoykova has shown, failure to regulate these matters procedurally transfers the assessment of reliability from the court to the expert and ultimately to the software vendor. Automation should be distinguished according to its function: generating records, calculating deadlines, transcription and notification may be auxiliary functions, while assessment of evidence, legal qualification and decisions on coercive measures require human procedural responsibility. Consequently, the electronic criminal case, digital evidence and legally significant digital trace should be defined in the Criminal Procedure Code rather than only in departmental acts.

2. International legal standards of digital investigation

The international framework combines investigative powers, human-rights and data-protection safeguards, and technical-organisational standards.

The Budapest Convention on Cybercrime establishes powers concerning preservation, production, search and seizure and real-time collection of traffic data, while Article 15 requires safeguards under domestic law, including independent supervision, justification and limits of scope and duration. The Second Additional Protocol develops cross-border cooperation.

The United Nations Convention against Cybercrime extends comparable principles to a wider group of States. For Uzbekistan, it represents an important framework for international exchange of electronic evidence The International Covenant on Civil and Political Rights and Convention 108+ require that interference with privacy be provided by law and be necessary and proportionate. The European Court of Human Rights has developed these requirements in cases concerning mass interception, communications data and IP information, emphasizing the quality and foreseeability of law.

For artificial intelligence, the CEPEJ Ethical Charter and the Council of Europe Framework Convention on AI emphasize human control, transparency and accountability. EU instruments additionally establish requirements for risk management, logging, data governance and human oversight. Technical and organisational guidance from INTERPOL, UNICRI, Europol and OECD similarly stresses forensic competence, chain of custody, accountability and interoperability.

The common international test can therefore be reduced to four requirements:

(1) an adequate statutory basis; (2) a legitimate aim; (3) necessity and proportionality; and (4) effective independent supervision and an accessible remedy. These requirements should be incorporated into the architecture of a national digital investigation system.

3. Comparative-legal experience of foreign states

The United States regulates digital investigation through constitutional guarantees, procedural rules and legislation concerning stored communications and cross-border access. The Stored Communications Act and the CLOUD Act of 2018, which authorises executive agreements permitting foreign authorities to address providers directly. Judicial decisions such as Riley v. California and Carpenter v. United States strengthened prior judicial control over access to digital information. The principal transferable elements are judicial authorization and mechanisms for obtaining data held by providers.

The United Kingdom combines statutory investigative powers with layered independent oversight. The “double

lock" for intrusive measures and statutory forensic regulation illustrate the importance of independent review and quality standards. Of particular relevance for Uzbekistan are formal forensic requirements and rules governing disclosure of large volumes of digital material to the defence.

Germany provides a clear procedural-law-first model. §§32–32f of the Code

of Criminal Procedure regulate the electronic file, while intrusive digital measures are separately regulated. Constitutional jurisprudence has established limits on automated analysis of police data. The principal lesson is that electronic case management and automated analytical powers must have an explicit statutory basis and defined intervention thresholds.

Estonia demonstrates infrastructure-based integration. The e-File system connects police, prosecution, courts and prisons through an interoperability layer, while citizens can obtain information about access to their data. The most valuable element for Uzbekistan is therefore not a particular software product but the combination of interoperability and legally meaningful access logging.

Singapore has developed an integrated criminal-justice environment connecting investigation, prosecution, courts and prisons. Its principal lesson is the use of a single case identifier throughout the proceedings, although external data-protection oversight is comparatively weaker.

The Republic of Korea represents another strong statute-first model. The 2021 Act on the Use of Electronic Documents in Criminal Justice Procedures established the legal basis for electronic case records and warrants before full technological deployment. AI functions remain auxiliary, such as retrieval, summarization and transcription. This sequence is particularly relevant to Uzbekistan.

China has treated electronic data as evidence in criminal procedure and developed big-data prosecutorial systems for detecting anomalies and checking evidentiary completeness. The transferable element is automated technical verification against formal criteria, while opaque or surveillance-oriented uses raise concerns regarding independent oversight and automation bias.

The comparison reveals two models. In the procedural-law-first model, exemplified particularly by Germany and Korea and substantially by Estonia, legislation defines electronic form, legal effects and limits before or alongside deployment. In the technology-first model, visible in China and partly in Singapore and analytical applications elsewhere, technological capacity may develop faster than legal control. For Uzbekistan, the first model offers stronger procedural guarantees.

4. Problems of digitalization in Uzbekistan

Uzbekistan has developed a broad strategic and legal basis for digital transformation. The Constitution, legislation on electronic documents, electronic signatures, informatization, electronic government, personal data and cybersecurity, the "Digital Uzbekistan–2030" Strategy and the 2025 "Digital Prosecution–2030" Strategy create the general framework.

Nevertheless, several procedural gaps remain. First, the Criminal Procedure Code does not sufficiently define the electronic criminal case and the legally significant digital trace. Second, technical guarantees for digital evidence require further specification, including integrity verification and chain of custody. Third, personal-data rules should be adapted to criminal proceedings through differentiated categories, access logging and retention periods. Fourth, the defence requires effective electronic access to the materials of the case. Fifth, cross-border access to electronic evidence remains difficult without broader international cooperation.

Thus, Uzbekistan is developing technologically faster than its procedural regulation. The principal risk is not technological inefficiency but the legal vulnerability of electronically generated procedural results.

5. Proposals for improving legislation and practice

First, the Criminal Procedure Code should contain a dedicated chapter on the electronic form of criminal proceedings. It should define the electronic criminal case, electronic procedural document and legally significant digital trace; recognize the legal force of digitally signed documents; require fixation of the author, time, grounds, signature and modification history; and prohibit retroactive alteration. Second, following the Korean approach, Uzbekistan could adopt a special law on electronic documents in criminal proceedings regulating electronic prosecutorial and judicial sanctions, electronic warrants, defence access and storage requirements. Third, legislation should establish technical standards for digital evidence, including integrity verification, an electronic chain of

custody and use of ISO/IEC 27037 and 27041–27043. Accreditation of forensic laboratories under ISO/IEC 17025 should be considered. Fourth, AI should be subject to a statutory boundary: an algorithmic result should not itself constitute evidence or independently justify a procedural decision. Human verification and reasoned confirmation should be mandatory; participants should be informed of AI use and allowed to challenge its results. Automated decisions on coercive measures should be prohibited. Fifth, personal-data legislation should contain criminal-procedure-specific rules on data categories, access logs, retention periods and, where appropriate, an individual's right to obtain the access history. Finally, Uzbekistan should conduct professional training and periodic certification in digital forensics for investigators, prosecutors and judges should accompany technological reform.

2. Conclusion

Digitalization of investigative activity is a transformation of procedural form. Its legitimacy depends not on the number of electronic documents produced but on whether each procedural act can be authenticated, its chronology verified and unlawful interference detected. International standards establish a common framework based on legality, legitimate aim, necessity and proportionality, independent supervision and effective remedy.

Comparative experience demonstrates the superiority of the procedural-law-first model for Uzbekistan. Germany, Korea and Estonia show that legislation can define the electronic form and its guarantees before technological deployment.

The United States and United Kingdom demonstrate the importance of judicial and independent oversight; Singapore illustrates end-to-end integration; China demonstrates the potential and risks of analytical automation.

For Uzbekistan, the priority should therefore be to align “E-tergov” with procedural legislation: define the electronic criminal case and digital trace, strengthen digital-evidence guarantees, regulate AI, ensure defence access and personal-data safeguards, build interoperable infrastructure and develop international cooperation. Technology and procedural law must evolve together; otherwise digitalization may increase administrative efficiency while weakening the legal certainty of criminal proceedings.

References

1. Council of Europe Framework Convention on AI (CETS No. 225), 5 September 2024.
2. CEPEJ. European Ethical Charter on AI in Judicial Systems, 2018.
3. Regulation (EU) 2024/1689; Directive (EU) 2016/680.
4. INTERPOL. Global Guidelines for Digital Forensics Laboratories, 2019; INTERPOL–UNICRI. Toolkit for Responsible AI Innovation in Law Enforcement, 2023–2024.
5. OECD. Recommendation on Artificial Intelligence, OECD/LEGAL/0449; Recommendation on Digital Government Strategies, OECD/LEGAL/0406.
6. ISO/IEC 27037:2012; ISO/IEC 27041:2015; ISO/IEC 27042:2015; ISO/IEC 27043:2015.
7. Bundesverfassungsgericht, judgment of 16 February 2023, 1 BvR 1547/19, 1 BvR 2634/20.
8. Germany: Strafprozessordnung, §§32–32f, 100a, 100b, 110(3).
9. United Kingdom: Investigatory Powers Act 2016; Police and Criminal Evidence Act 1984; Forensic Science Regulator Code of Practice, 2023.
10. Singapore: Criminal Procedure Code 2010, ss.39–40; Evidence Act 1893, s.116A.
11. China: Criminal Procedure Law, Article 50; Provisions on Electronic Data in Criminal Cases, 2016.
12. Estonia: Code of Criminal Procedure; regulations on the e-File (E-toimik).
13. Laws of Uzbekistan: On Personal Data; On Electronic Document Circulation; On Electronic Government; On Cybersecurity.
14. Stoykova R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Computer Law & Security Review. 2021. Vol.42.
15. Quattrocolo S. Artificial Intelligence, Computational Modelling and Criminal Proceedings. Springer, 2020.