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

Social Need for Digitization of Criminal-Procedural Legislation

Kobulov Bekzod Sherali oglu
Independent Researcher at The Tashkent State Law University, Uzbekistan

Received: 28 Feb 2026 | Received Revised Version: 14 Mar 2026 | Accepted: 02 Apr 2026 | Published: 29 Apr 2026

Volume 08 Issue 04 2026 | Crossref DOI: 10.37547/tajpslc/Volume08Issue04-07

Abstract

This article examines the need for the digital transformation of criminal procedural law in response to the rapid growth of cybercrime and technology-enabled criminal activity. The study argues that traditional procedural mechanisms are increasingly insufficient for detecting, investigating, proving, and preventing crimes committed in cyberspace, particularly where offenders use artificial intelligence, deepfakes, voice cloning, cryptocurrency, anonymous networks, and other digital tools. Special attention is given to the transboundary nature of cybercrime, the complexity of digital evidence, the vulnerability of victims' rights, and the limitations of existing procedural coercive measures and asset recovery mechanisms. The article substantiates the necessity of introducing new procedural institutions for the seizure of crypto-assets, preservation of digital traces, use of artificial intelligence in investigations, and protection of constitutional rights in digital environments. It concludes that criminal procedure must evolve from simple technological modernization toward a comprehensive normative transformation aligned with contemporary digital risks.

Keywords: Cybercrime; criminal procedure; digital evidence; artificial intelligence; digital rights; crypto-assets.

Cite This Article: Kobulov Bekzod Sherali oglu. (2026). Social Need for Digitization of Criminal-Procedural Legislation. The American Journal of Political Science Law and Criminology, 8(04), 40–46. https://doi.org/10.37547/tajpslc/Volume08Issue04-07

1. Introduction

In the contemporary period, the Internet and digital technologies have become deeply embedded in almost every sphere of social life. From the moment of birth, information about an individual may be recorded in electronic databases, including civil registration data, electronic birth certificates, medical records, information on treatment and medicines, attendance at preschool and school institutions, enrolment in higher education, employment applications, salary payments, pension fund accounts, workplace and residence data, and other categories of personal information. Ultimately, even the registration of death is increasingly reflected in electronic information systems. This demonstrates that the legal status, social activity, economic participation, and personal identity of an individual are now closely connected with digital records and digital infrastructure.

In modern society, it is difficult to imagine social, economic, and administrative life without the Internet. The term "Internet", derived from the Latin inter ("between") and the English word "net" ("network"), denotes a global, publicly accessible system of interconnected computer networks that exchange data through standard Internet Protocols. Its essential feature is the capacity to overcome borders, distances, and limitations that, for centuries, restricted human communication, access to knowledge, public administration, commerce, and social interaction.

At the same time, the digitalization of human life

inevitably creates new legal risks. As communication, access to knowledge, income generation, the provision of services, and social interaction increasingly take place in a digital environment, violations of personal, property, and other rights also occur within cyberspace. Criminal conduct that affects the interests of individuals, society, and the state is therefore acquiring new forms, methods, and instruments.

Despite ongoing judicial and legal reforms and the continuous improvement of legislation, crimes committed in cyberspace are increasing. Threats to the interests of individuals, society, and the state in the digital environment are becoming more intensive, while the share of offences committed through information technologies in the overall structure of crime continues to grow. According to available statistical data, crimes committed through information technologies accounted for 44.4 per cent of total crime in 2024, while in the first eleven months of 2025 this figure reached 47.7 per cent. Of particular concern are the relatively low rates of detection, identification of perpetrators, and compensation for material damage caused to victims.

International data also indicate the growing social relevance of cyber-related offences. According to a 2024 report of the World Health Organization, approximately one in six school-aged children in Europe, or 15–17 per cent, had experienced cyber-related victimization. At the same time, 12 per cent of young people were identified as having committed cyber-related acts against other children. Studies published in Frontiers in Public Health similarly show that the prevalence of cyberbullying victimization has increased from 13.9 per cent to 57.5 per cent, while the proportion of persons who have committed such acts has risen from 6 per cent to 46 per cent.

The rapid development of artificial intelligence and deep learning technologies has introduced particularly significant changes into the processing and synthesis of human speech, images, and behaviour. Voice cloning technologies, for example, enable the automated learning of a person's vocal characteristics and the subsequent reproduction of that voice in a natural and realistic manner. As a result, offenders increasingly use artificial intelligence, deepfake technologies, voice cloning, neural text-to-speech systems, SV2TTS, few-shot learning, generative adversarial networks, and transformer-based models to commit fraud, theft, extortion, defamation, and other crimes.

According to data published by the international IT company Sumsub, in 2023 the falsification of photographs, video images, and audio recordings of well-known persons through the use of artificial intelligence increased globally. The reported growth amounted to 1,740 per cent in North America, 1,530 per cent in the Asia-Pacific region, and 780 per cent in European countries. These figures demonstrate that artificial intelligence-enabled falsification is no longer an exceptional phenomenon, but an increasingly common tool of unlawful activity.

Investigative practice in this category of cases confirms the practical significance of these risks. In one case, on 28 July 2024, citizen A., as a result of a long-standing personal conflict with acquaintance G., created a Telegram profile under the name "1111" within the global Internet information network. Using artificial intelligence technologies, A. altered a photograph of G., produced video materials falsely suggesting that G. was engaged in prostitution, and disseminated these materials on the Internet.

In another case, citizen D. downloaded personal photographs of citizen N. from N.'s Telegram profile. D. then processed those photographs using artificial intelligence technologies and threatened to disseminate pornographic photo and video materials in groups and social networks promoting obscenity. D. was detained while receiving 30,000,000 Uzbek soums, a sum that had been extorted from the victim.

Cyber-enabled conduct is also observed in crimes against peace and the security of humanity. In a criminal case investigated by the Investigation Department of the State Security Service, it was established that citizen A., using the Internet, recruited persons identified as B., N., and others into terrorist activity and conducted online training for them on the preparation and use of explosive devices. On the basis of these instructions, citizens B. and N., from their respective places of residence, developed a criminal plan and prepared to carry out explosions in buildings housing state administrative bodies in the Republic of Uzbekistan. The purpose of these acts was to create panic among the population, undermine the constitutional order, and disrupt the functioning of state bodies and the stability of the socio-political situation in the country. As a result of a joint operation by law enforcement agencies, the planned criminal acts were prevented.

It should also be noted that a wide range of transnational

crimes, including trafficking in persons, arms trafficking, and the illicit circulation of narcotic drugs, their analogues, and psychotropic substances, are increasingly committed through Internet-based social networks and digital communication channels. Offenders actively use the Darknet, a segment of the World Wide Web consisting of hidden websites that are difficult to access and generally require specialized software such as the Tor Browser. Such platforms are widely recognized as environments in which illicit goods and services may be offered and unlawful transactions may be organized.

Researchers A.A. Konovalov, S.A. Naumov, and D.D. Kolesnikov emphasize that the commission of such crimes is facilitated by the specific characteristics of the networked information space. These include a high level of concealment supported by developed mechanisms of anonymity, the complexity of digital infrastructure, and other technical factors. The same scholars identify several essential features of network crimes: their transboundary character, the specialized training of offenders, the intellectual nature of criminal conduct, and the complexity, diversity, and frequent renewal of methods used to commit such offences. From this perspective, conventional methods of prevention and suppression are often insufficient for this category of crimes.

In the view of the present author, the prevention and suppression of such offences are hindered not only by the complexity of their forms, methods, and means of commission, but also by the insufficiency of existing norms of criminal procedural legislation. Modern cyber-enabled offences require new legal institutions and procedural mechanisms capable of ensuring timely detection, the collection and preservation of digital evidence, the identification of offenders, and the protection of victims' rights.

A detailed analysis of criminal activity in the Republic of Uzbekistan shows that approximately 64 categories of offences provided for in the Criminal Code are currently being committed in cyberspace or through the use of information technologies. The absence of adequate legal mechanisms for combating these offences contributes to the expansion of online criminal activity. Existing procedural possibilities are limited in proving new digital forms of traditional crimes, collecting and verifying evidence, and conducting investigative and procedural actions in a timely and effective manner. In some cases, legal gaps indicate the need to introduce new types of procedural actions into criminal procedural legislation.

For example, analysis of cybercrime indicates that 97.7 per cent of such offences consist of theft and fraud involving bank cards. Offenders usually dispose of unlawfully obtained electronic funds through various channels within a period ranging from three to twenty-four hours. However, the existing criminal procedural legislation does not provide sufficiently clear procedural actions or other legal mechanisms that would allow the movement of such funds to be suspended within a short period. Consequently, the ability to detect and investigate theft and fraud involving bank cards committed through information technologies remains significantly restricted.

A new ecosystem has emerged on the basis of modern information technologies. The speed of technological change may create institutional inertia: public authorities and legal systems that implement reforms gradually may fail to perceive the scale and consequences of digital transformation in time. Crime statistics and detection rates suggest that society and the state are now facing not merely isolated technological challenges, but a digital revolution in criminal activity, or, in practical terms, a "tsunami of digital crimes".

The state, acting under the authority entrusted to it by the people, regulates socially significant relations that arise in society. In criminal cases, law enforcement activity is of particular importance because it involves the application of the most stringent forms of state coercion. For this reason, criminal procedural activity must be regulated precisely, and the rights and obligations of its participants must be clearly defined.

The scale of damage caused by cyber-enabled offences, the number of persons affected, and the difficulty of restoring violated rights in unsolved cases require a comprehensive examination of guarantees for the protection of individual rights in the virtual environment. New forms of digital relations necessitate legal mechanisms that protect personal, property, moral, and other rights in cyberspace while preserving procedural safeguards and constitutional guarantees.

A.N. Yakubov defines "virtual objects" as intangible objects of the virtual world modelled by a computer program. Such objects may already possess economic value and circulate within the virtual environment, while remaining insufficiently regulated by law. He further defines "digital rights" as a set of obligations and other rights whose content and conditions of exercise comply with criteria established by an information system in

accordance with legislation and are determined by the rules of that information system.

In the opinion of the present author and the institution represented, virtual objects should not be understood solely as objects of economic circulation. They also encompass relations connected with social interaction, moral interests, personal inviolability, and other non-material values. Digital rights, in turn, constitute the form and manifestation of an individual's existing rights within information technologies, cyberspace, and digital relations.

A.Yu. Afanasyev defines artificial intelligence as an advanced form of contemporary digitalization and characterizes it as an information technology that can increase the efficiency of process management by automating the activities of inquiry and investigative bodies. Such technologies may improve the quality of decisions, accelerate the processing of information, and reduce the time required to make procedural decisions in specific situations. However, the integration of artificial intelligence into investigative activity must be accompanied by legal regulation of both the use of such technologies in criminal proceedings and the investigation of crimes committed with their assistance.

The prevailing scholarly discussion, however, is often characterized by a narrow understanding of the digitalization of criminal procedure. For example, S.A. Mukhamadiev considers the use of information-technology tools in criminal proceedings to be equivalent, in a literal sense, to the digitalization of criminal procedure. This position should be approached critically. Digitalization of criminal procedure is a broader concept. It involves not only the introduction of digital tools into existing procedural practice, but also the systematic review and adaptation of procedural norms, institutions, guarantees, and mechanisms to new forms of social relations and criminal conduct.

V.A. Milikova notes that contemporary law enforcement agencies and judicial bodies already use digital technologies extensively in their daily activity. She emphasizes that the effective and wider introduction of digital technologies into criminal proceedings requires not only the improvement of infrastructure, but also the modernization of criminal procedural legislation. Similarly, O. Halahan, I. Krytska, A. Tumanyants, and I. Dubivka argue that the digitalization of criminal procedure requires the modernization of institutions regulating the pre-trial stage of proceedings, the use of data contained in electronic information and communication systems, and the application of digital technologies in procedural actions.

N.V. Mikhaylenko, while not rejecting the use of digital technologies in criminal proceedings, identifies several risks. These include the incomplete development of relevant legislation, difficulties in comparing electronic documents with their originals, unequal access to electronic services, and the need to ensure cybersecurity. She therefore emphasizes that innovations in criminal proceedings must be implemented carefully and deliberately. The Hungarian scholar Andor Gal also observes that the evolution of crime, its integration with digital processes, and its increasingly transboundary character require the development of both criminal procedural norms and the relevant technical infrastructure.

These scholarly positions support the conclusion that the absence of comprehensive legislative modernization prevents digitalization from achieving its expected results. Legal norms and technologies must develop in parallel. If technology advances while procedural regulation remains static, the criminal justice system will not be able to provide effective investigation, fair adjudication, or adequate protection of rights in the digital environment.

Cybercrimes committed through information technologies possess several distinctive features that directly affect criminal procedure.

First, such offences are not limited by geography. They may be committed from one state or region while violating legally protected interests of persons, organizations, or public authorities located elsewhere.

Second, they are not limited by time. The acquisition, transfer, concealment, or disposal of unlawfully obtained data or assets may occur within seconds.

Third, unlike traditional crimes, which are often committed through tangible objects, many contemporary offences are carried out through software, communication networks, artificial intelligence technologies, and other digital instruments.

Fourth, the traces left by offenders are frequently non-material. They may appear in the form of data, codes, algorithms, logs, metadata, digital transactions, or other electronic traces.

Fifth, traditional investigative actions are inherently

limited in their ability to collect, verify, and evaluate this type of evidence.

Sixth, unlike material evidence that may be sealed in a package or placed in a physical container, digital evidence remains vulnerable to external interference, modification, deletion, encryption, or destruction through software and technological means.

Seventh, the procedure, form, and methods for storing such evidence require a higher level of technological capacity and institutional preparedness.

Eighth, offenders often benefit from a high degree of anonymity, including the use of encrypted communication, anonymization services, fake accounts, and transnational digital infrastructure.

Ninth, the authenticity of photographic, video, and audio materials used in the commission of offences is increasingly difficult to establish because such materials may be created or altered through artificial intelligence and advanced software. Existing types and methods of forensic examination may be insufficient to determine authenticity in a timely and reliable manner.

Tenth, existing procedural coercive measures do not always restrict the criminal activity of persons involved in cybercrime. Restricting a person's physical movement, for example, does not necessarily prevent that person from continuing unlawful conduct in cyberspace. In some cases, automated software may continue to operate even after the individual's movement has been restricted.

Eleventh, traditional mechanisms for property recovery and compensation are often ineffective in cases involving electronic funds, crypto-assets, and other digital values. Legal gaps limit the ability to seize such assets or restrict property-related rights in digital form.

Twelfth, the prevention of such crimes requires new methodologies and technological solutions. Pre-trial proceedings demand not only legal expertise, but also knowledge and competencies in information technologies. Accordingly, inquiry bodies, investigative authorities, prosecutors, and courts must be institutionally and technically prepared to operate in the digital environment.

Finally, despite the increasing scale and danger of cyber-enabled criminal activity, including offences that exceed the scope of conventional transnational crime, existing norms of international law do not yet fully address the practical issues of combating such crimes or ensuring effective cooperation among states. This creates difficulties in evidence collection, jurisdictional coordination, extradition, mutual legal assistance, and the recovery of digital assets.

A.N. Yakubov correctly identifies the transboundary nature of cyberspace as one of its principal features. This characteristic demonstrates the transjurisdictional nature of the relations developing in the digital environment. Resolving this issue requires unified international legal regulation of relations in cyberspace, including those connected with the circulation of cryptocurrency, digital assets, and virtual property.

This approach is particularly relevant because cybercrime has reached a level at which it may threaten the security not only of individual states, but of the international community as a whole. The creation of a legal foundation and practical mechanisms for combating cybercrime at the global level is therefore an urgent task for international cooperation.

M.Kh. Rustambaev emphasizes that, in the context of criminal justice, the state's principal objectives in response to crime are to detect and investigate offences, identify and prosecute offenders, and ensure compensation for victims. For this purpose, the state establishes law enforcement bodies and courts through its legal system. When a crime is committed, the state determines the procedure for investigation, judicial proceedings, sentencing, and enforcement of punishment.

In our view, the modernization of criminal proceedings in cases involving crimes committed in cyberspace through information technologies is one of the most urgent issues of contemporary legal scholarship and lawmaking. Such modernization must ensure the detection and investigation of offences, compensation for damage, the prosecution of offenders, the adjudication of criminal cases in court, and the adoption of judgments that correspond to the realities of the digital age. This requires not only the use of digital tools, but the digital transformation of criminal procedural norms themselves.

The preceding analysis demonstrates the social and legal necessity of digitalizing criminal procedural legislation for several reasons.

First, international legal norms do not adequately regulate cooperation in combating cyber-enabled offences in a manner proportionate to their scale and

risks.

Second, the current criminal procedural legislation, its principles, and the circle of procedural participants do not fully reflect the specific requirements of combating crimes committed through information technologies.

Third, existing criminal procedural norms are insufficient for identifying digital traces of crimes committed in the virtual environment through software, artificial intelligence technologies, and other digital tools.

Fourth, the possibilities for collecting, verifying, and evaluating digital evidence through traditional investigative actions remain limited.

Fifth, traditional procedures, forms, and methods for storing evidence are insufficient for the volume, vulnerability, and technical complexity of digital evidence.

Sixth, existing types and methods of forensic examination are inadequate for the collection, verification, and authentication of evidence in modern criminal cases involving artificial intelligence, deepfakes, digital transactions, and crypto-assets.

Seventh, restrictions on physical movement in cybercrime cases cannot be regarded as a direct restriction on criminal activity in the digital environment. Therefore, the scope of existing procedural coercive measures is insufficient to prevent continued criminal conduct by suspects and accused persons in this category of cases.

Eighth, compensation for damage caused by cyber-enabled offences cannot always be ensured through legal mechanisms designed for traditional property recovery. The seizure of property and the preservation of assets are limited by legal gaps, especially where unlawfully obtained assets exist in digital form. In particular, the Criminal Procedure Code does not establish sufficiently clear procedural actions or procedures for seizing crypto-assets in the virtual environment or restricting property-related rights in digital form. Nor does it provide comprehensive mechanisms for ensuring constitutional rights during the application of such procedural actions.

Therefore, the digitalization of criminal procedure should not be reduced to the introduction of information and communication technologies into criminal proceedings. It must be understood as a broader legal transformation: the modernization of criminal procedural norms, the creation of new procedural institutions, the development of safeguards for digital evidence and digital rights, and the adaptation of the Criminal Procedure Code to the growth of contemporary forms of crime. Only such an approach can ensure that criminal justice remains effective, rights-based, and institutionally capable in the conditions of the digital age.

References

1. K. Park, S. Mun, J. Kim, et al. ―A Review of Voice Cloning Technologies Using Deep Learning,‖ IEEE Access, vol. 9, pp. 80650–80669, 2021.
2. Зуфаров А.М. “Хавфсизликка таҳдидларнинг замонавий кўринишлари ва уларга қарши курашишнинг ўзига хос жиҳатлари”. “Ўзбекистон терговчиси” илмий-амалий журнали. №01(01)2023 й., 28-31-бетлар (Zufarov A.M. "Modern manifestations of security threats and the peculiarities of combating them". Scientific and practical Journal "investigator of Uzbekistan". №01 (01)2023., Pp. 28-31 .)
3. World Health Organization (2024). Health Behaviour in School-aged Children (HBSC) Study: International Report 2021/2022. WHO Regional Office for Europe.// https://www.hbsc.org
4. Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation. Frontiers in Public Health, 9:634909.// https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2021.634909/full
5. Коновалов А.А., Наумов С.А. ва Колесни-ков Д.Д. Киберпреступность как глобалтная угроза экономический безопасности: виды, особенности, проблемы воздействия// Ростовский научный журнал №1. 2018. С.-20-27 (Konovalov A.A., Naumov S.A. va Kolesnikov D.D. Cybercrime as a global threat to economic security: types, features, problems of impact// Rostov Scientific Journal No. 1. 2018. pp. 20-27)
6. И.Стребулаев, А.Данг., Венчур зеҳният Б-146 (I.Strebulaev, A.Dang, Venture Mindset P-146)
7. APAC Experiences 1530% Surge in Deepfake Incidents Amid Global Fraud Evolution/ https://cybersecurityasia. net/ apac-experiences-1530-surge-in-deepfake-incidents-amid-global-fraud-evolution.
8. М.Х.Рустамбаевнинг умумий таҳрири остида. Жиноят-процессуал ҳуқуқи дарслик. Тошкент-2023. Б-13-15 (Under M.X.Rustambaev's General

Ed. Textbook of Criminal-Procedural Law. Tashkent-2023. P-13-15)

9. 13. Якубов А.Н. Кибермаконда рақамли мулк ҳуқуқи ва уни ҳуқуқий тартибга солиш. Ю.ф.д. Дисс. Автореф. Т-2023. Б-5 (Yakubov A.N. The right to digital property in cyberspace and its legal regulation. Autoref. Diss. Doctor of Law. T-2023. P-28)
10. А.Ю.Афанасьев. Искусственный интеллект в уголовном процессе. Юридическая техника. 2021. № 15.Б-571-574. (A.Y.Afanasyev. Artificial intelligence in criminal proceedings. Legal technology. 2021. No. 15.B-571-574.)
11. С.Мухамадиев “Суриштирув ва дастлабки тергов жараёнида жиноят ишларини юритиш тартибини босқичма-босқич рақамлаштириш масалалари.” Юффд.диссертация Б-22. (S.Mukhamadiev "Issues of gradual digitization of the procedure for conducting criminal proceedings in the process of inquiry and preliminary investigation." Disser. PhD P-22.)
12. Миликова А. В. Актуальные вопросы цифровизации системы уголовно-процессуальных актов. Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2025. Т. 9. № 4. С. 624–632. https://doi.org/10.21603/2542-1840-2025-9-4-624-632 (Milikova A.V. Actual issues of digitalization of the system of criminal procedural acts. Bulletin of Kemerovo State University. Series: Humanities and Social Sciences. 2025. Vol. 9. No. 4. pp. 624-632.)
13. Oleksandr Halahan, Iryna Krytska, Anush Tumanyants, Iryna Dubivka “Digitalization of the criminal process: is simplification always for the better?” https://idp.uoc.edu IDP N.º 38 (October, 2023) I ISSN 1699-8154 1 Journal promoted by the Law and Political Science Department 2023,
14. Н.В.Михайленко. Перспективы и проблемы отправления цифрового правосудия в Российской Федерации. Закон и право. Диссертационные исследования. 2020. Б-201-205. (Н.В.Михайленко. Перспективы и проблемы отправления цифрового правосудия в Российской Федерации. Закон и право. Диссертационные исследования. 2020. Б-201-205.)
15. Andor Gál New Area of Judicial Cooperation on Criminal Matters in the European Union: The Transmission of Electronic Evidence between Member States / DOI: 10.17951/sil.2024.33.5.69-85 P-70
16. Якубов А.Н. Кибермаконда рақамли мулк ҳуқуқи ва уни ҳуқуқий тартибга солиш. Ю.ф.д. Дисс. Автореф. Т-2023. Б-5 (Yakubov A.N. The right to digital property in cyberspace and its legal regulation. Autoref. Diss. Doctor of Law. T-2023. P-22)
17. М.Х.Рустамбаевнинг умумий таҳрири остида. Жиноят-процессуал ҳуқуқи дарслик. Тошкент-2023. Б-13 (Under M.X.Rustambaev's General Ed. Textbook of Criminal-Procedural Law. Tashkent-2023. P-13)
18. Information of the Ministry of internal affairs of the Republic of Uzbekistan.
19. Materials from the criminal case in the archives of the Supreme Court of the Republic of Uzbekistan.
20. Criminal case materials in the investigative units of the Ministry of internal affairs
21. World Health Organization (2024). Health Behaviour in School-aged Children (HBSC) Study: International Report 2021/2022. WHO Regional Office for Europe.// https://www.hbsc.org
22. Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation. Frontiers in Public Health, 9:634909.// https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2021.634909/full