IRSHAD Uzbek Journal of Law and Digital Policy | Volume: 4, Issue: 1
2026

Legal Frameworks for Combating Deepfake-Driven Fraud in Autonomous Systems

Naeem AllahRakha
Tashkent State University of Law

Abstract

Deepfake technology has emerged as a critical legal threat to autonomous systems worldwide, yet Uzbekistan's existing legal framework remains fundamentally unprepared to address it. This research examines the adequacy of Uzbekistan's Criminal Code, Cybersecurity Law of 2022, and Personal Data Law of 2019 in combating deepfake-driven fraud targeting autonomous systems. The central research question asks to what extent these laws provide sufficient legal protection and where they critically fail. Employing a qualitative methodology combining doctrinal legal analysis and document analysis, this research systematically evaluates Uzbekistan's legislative gaps through comparative examination of legal frameworks from the United States, the European Union, China, and South Korea. Official legal texts were retrieved from Lex.uz, while scholarly sources were drawn from peer-reviewed legal databases. Findings reveal significant deficiencies across five critical areas: criminal law, cybersecurity legislation, civil liability, digital evidence standards, and biometric data protection. This research proposes dedicated synthetic media legislation, targeted amendments to existing laws, certified forensic evidentiary standards, enhanced biometric data protections, and establishment of an independent AI regulatory body, offering Uzbekistan a concrete and achievable legal reform roadmap suited to its institutional capacity and legal tradition.

Keywords: Deepfake Technology, Autonomous Systems, Digital Fraud, Legal Frameworks, Regulatory Compliance, Cyber Law

APA Citation:

AllahRakha, N. (2026). Legal Frameworks for Combating Deepfake-Driven Fraud in Autonomous Systems. *Uzbek Journal of Law and Digital Policy, 4*(1), 1–19. https://doi.org/10.59022/ujldp.518

I. Introduction

Imagine a self-driving car receiving a fake voice command, or a security system unlocking for a criminal wearing a deepfake face, this is no longer science fiction. Deepfake technology has evolved from a digital curiosity into a serious legal threat. It can now deceive autonomous systems with alarming accuracy and speed (Folorunsho & Boamah, 2025). The consequences are real for financial loss, security breaches, and justice denied. What makes this threat even more dangerous is the absence of strong legal responses. Most legal systems, including Uzbekistan's, were not designed for this reality. Uzbekistan's Criminal Code, Cybersecurity Law, and Personal Data Law provide only partial protection. Critical gaps remain in liability, evidence, and enforcement. As autonomous systems become more embedded in public life, the risk grows every day. This research examines how Uzbekistan's existing legal framework addresses deepfake-driven fraud in autonomous systems. It also identifies where the law falls short and what urgent reforms are needed.

The rise of artificial intelligence has transformed the way society's function, but it has also introduced threats that existing legal systems were never designed to handle. Deepfake technology, which uses AI to create convincingly fake audio, video, and images, first gained public attention around 2017. Initially, it was associated with manipulated celebrity content and political misinformation. Over time, however, its application shifted toward organized fraud, identity theft, and attacks on critical digital infrastructure. Autonomous systems including self-driving vehicles, AI-powered security platforms, and automated financial tools became particularly vulnerable targets (Durlik et al., 2024). Globally, lawmakers began responding at different speeds. The United States introduced the Deepfake Task Force Act, China regulated synthetic media through its Deep Synthesis Provisions in 2022, and the European Union embedded AI risk governance within its landmark AI Act of 2024. Uzbekistan, however, has followed a slower path. Its legal instruments address digital threats only in broad and general terms. No existing Uzbek law specifically defines deepfake technology, assigns liability for AI-driven fraud, or establishes evidentiary standards for synthetic media in court.

It is already known that deepfake technology poses a serious and growing threat to autonomous systems worldwide. It is also known that countries like the United States, China, and the European Union have begun developing legal responses to this threat. What is equally clear is that Uzbekistan has not yet done the same. Uzbekistan's current legal system relies on general provisions scattered across multiple laws the Criminal Code, the Cybersecurity Law, and the Personal Data Law none of which specifically address deepfake fraud or its impact on autonomous systems. This fragmented legal landscape creates a dangerous vacuum. Courts cannot properly prosecute deepfake criminals because the law does not define the crime

clearly. Victims cannot claim compensation because liability rules for AI-driven harm do not exist. Law enforcement cannot act decisively because digital evidence standards for synthetic media are absent. The exact problem this research addresses is therefore threefold the absence of a legal definition for deepfake fraud, the lack of a liability framework for autonomous systems compromised by deepfakes, and the inadequacy of Uzbekistan's evidentiary and enforcement mechanisms (Easttom, 2025).

The growing intersection of deepfake technology and autonomous systems has attracted increasing scholarly attention, yet significant gaps remain, particularly in the context of developing legal systems like Uzbekistan. Deepfake technology has rapidly moved beyond entertainment into criminal activity. Criminals use synthetic media to bypass biometric authentication, manipulate autonomous vehicles, and deceive AI-powered security systems. The law has consistently failed to keep pace with this technological evolution, leaving victims without adequate legal remedies (Sunil et al., 2025). Traditional fraud laws were designed for human actors committing deception through conventional means. They were never anticipated to cover AI-generated synthetic identities or automated system manipulation. This legal mismatch creates impunity for deepfake criminals operating in jurisdictions with outdated criminal codes (Park et al., 2024).

A growing body of comparative legal research examines how different jurisdictions have responded to deepfake fraud. The United States Deepfake Task Force Act and China's Deep Synthesis Provisions of 2022 represent two distinct regulatory approaches. The American model focuses on criminalization and federal enforcement, while the Chinese model emphasizes platform accountability and content labeling. The European Union's AI Act of 2024 takes a broader risk-based approach, regulating AI systems according to their potential for harm. The question of legal liability when autonomous systems cause harm remains one of the most debated issues in technology law. Existing product liability frameworks were designed for physical goods, not intelligent machines capable of independent decision-making. When a deepfake attack causes an autonomous system to malfunction or cause harm, it becomes extremely difficult to assign responsibility among developers, operators, and users (Hynek et al., 2025a).

Deepfake creation depends heavily on the availability of personal biometric data. Research has consistently shown that weak biometric data protection laws increase the risk of deepfake fraud. When facial images, voice recordings, and fingerprint data are inadequately protected, they become raw material for synthetic identity fraud. The European Union's General Data Protection Regulation sets a strong international standard for biometric data governance. One of the most significant practical challenges in prosecuting deepfake fraud is the admissibility and authentication of digital evidence. Courts in many jurisdictions have no established

standards for evaluating synthetic media as evidence. Defense attorneys can easily challenge the authenticity of deepfake-related evidence, creating reasonable doubt even in clear cases of fraud (Babaei et al., 2025).

Cybersecurity legislation across many jurisdictions was developed primarily to address network intrusions, data breaches, and malware attacks. These laws were not designed to regulate AI-generated content or deepfake-driven fraud targeting autonomous systems. Deepfake fraud is inherently transnational. Criminals can generate and deploy synthetic media from any jurisdiction, making domestic legal responses insufficient on their own. Existing cooperation mechanisms, such as the Budapest Convention on Cybercrime, provide a useful but incomplete foundation. They require significant updating to address AI-specific threats like deepfake fraud targeting autonomous systems (Hynek et al., 2025b).

Scholarly work on deepfake regulation has made meaningful progress in recent years. Researchers have explored deepfake technology as a legal threat, proposed comparative regulatory models, debated liability in autonomous systems, and emphasized the importance of international legal cooperation. These contributions have built a useful foundation for understanding how law can respond to AI-driven fraud. However, a careful review of this body of knowledge reveals a consistent and critical weakness almost all studies are concentrated on legally advanced jurisdictions such as the United States, the European Union, China, and South Korea. Developing legal systems, particularly those in Central Asia, have received virtually no scholarly attention in this context. Uzbekistan is a clear example of this neglect. No published legal study has examined how Uzbekistan's specific legislative instruments interact with or fail to address deepfake-driven fraud in autonomous systems. The following objectives guide this research and define its scope, direction, and intended outcomes:

To examine the adequacy of Uzbekistan's existing legal framework in addressing deepfake-driven fraud in autonomous systems.

To conduct a comparative legal analysis of deepfake fraud regulations in selected jurisdictions.

To identify the specific legal gaps in Uzbekistan's regulatory framework concerning deepfake fraud and autonomous systems.

To what extent does Uzbekistan's current legal framework adequately address deepfake-driven fraud in autonomous systems, and where do these laws fail to provide sufficient legal protection?

As autonomous systems become increasingly embedded in Uzbekistan's public infrastructure, transportation, and security sectors, the legal risks associated with deepfake fraud grow more urgent every day. Yet no dedicated legal study has addressed this threat within the Uzbek legal context. It expands the geographic scope of AI law research beyond Western-dominated scholarship and introduces Central Asian legal systems into a global conversation that has largely ignored them. It does

not merely identify problems; it proposes solutions that are realistic within Uzbekistan's legal tradition and institutional capacity. By proposing evidentiary standards for synthetic media and clarifying liability rules for autonomous system harm, this study strengthens Uzbekistan's capacity to deliver justice in AI-related fraud cases. Deepfake fraud threatens individual identity, personal safety, and public trust in autonomous systems. When the law fails to protect people from emerging technological threats, it is ordinary citizens who suffer the consequences. This research contributes to a safer, more just, and more digitally secure society.

II. Methodology

This research adopts a qualitative research design. Qualitative methods are most appropriate for legal research because they allow for deep interpretation, critical analysis, and contextual understanding of laws, regulations, and legal scholarship. This study does not rely on numerical data or statistical measurements. Instead, it examines the meaning, scope, and adequacy of legal texts, judicial frameworks, and scholarly arguments. A qualitative approach allows this research to critically evaluate how Uzbekistan's legal framework responds to deepfake-driven fraud in autonomous systems and where it falls short. This method is well suited to the nature of the research question, which requires analytical judgment rather than quantitative measurement. Two specific qualitative approaches are applied as doctrinal legal analysis and document analysis, both of which are widely recognized and accepted methodologies in legal research.

The population of this research consists of all legal instruments, regulatory frameworks, and scholarly literature relevant to deepfake fraud, autonomous systems, and digital law governance. The sample is deliberately focused and purposively selected to ensure relevance and precision. For Uzbekistan's domestic legal framework, the sample includes the Criminal Code of Uzbekistan, the Law on Cybersecurity (2022), the Law on Personal Data (2019), and the Law on Electronic Documents. These laws were selected because they represent the primary legislative instruments most directly applicable to the research problem. For comparative analysis, the sample includes selected legal frameworks from the United States, the European Union, China, and South Korea. For scholarly literature, the sample consists of peer-reviewed legal journal articles, academic book chapters, and authoritative legal reports published within the last five years, ensuring currency and relevance to the rapidly evolving field of AI and deepfake law.

Data for this research was collected through two primary channels. First, all Uzbek laws, regulations, and official legal texts were retrieved directly from Lex.uz, the official legal information portal of the Republic of Uzbekistan. This portal is the authoritative and government-maintained source for all currently applicable Uzbek

legislation, ensuring that only official and legally valid texts are used in this research. Second, scholarly literature was retrieved from recognized academic databases including Google Scholar, and Scopus. These databases were searched using the following keywords and keyword combinations derived directly from this research topic: deepfake technology, autonomous systems, digital fraud, legal frameworks, regulatory compliance, and cyber law. These keywords were used individually and in combination to ensure comprehensive coverage of the relevant scholarly landscape. No surveys, interviews, or field experiments were conducted, as this research is entirely desk-based and document-driven.

The primary instruments used in this research are official legal documents and peer-reviewed scholarly articles. All Uzbek legislative texts were accessed and verified through Lex.uz to ensure authenticity and current applicability. Foreign legal instruments, including the EU AI Act, China's Deep Synthesis Provisions, and the United States Deepfake Task Force Act, were retrieved from their respective official government and institutional portals. Scholarly articles were selected based on their publication in recognized law journals and their direct relevance to the research topic. No questionnaires or survey instruments were used in this research, as the methodology is entirely based on legal text analysis and academic literature review.

Followings measures were taken to ensure the validity and reliability of this research. With respect to scholarly literature, only recent publications were prioritized to ensure currency and relevance to the fast-moving field of deepfake and AI law. Where foundational works older than five years were referenced, this was done only where those works remain widely cited and academically authoritative in the field. All selected scholarly sources were published in peer-reviewed law journals, ensuring a baseline standard of academic quality and credibility. Authors of selected works include university professors, legal researchers, and policy experts, ensuring that sources reflect informed and credible legal opinion. All claims drawn from scholarly sources are properly cited, and sources used in this research are themselves supported by evidence and cited by other researchers in the field. With respect to legal texts, only currently applicable laws retrieved from Lex.uz and official foreign government portals were used, ensuring that the legal analysis reflects the law as it stands today. The objective of all selected sources is scientific and analytical, consistent with the legal research purpose of this study.

This research employs two complementary data analysis techniques. The first is doctrinal legal analysis, which is the primary method of legal research. Doctrinal analysis involves the systematic examination, interpretation, and critical evaluation of legal texts, including statutes, regulations, and legal principles. This method is used to assess the content, scope, and adequacy of Uzbekistan's existing laws in relation to

deepfake fraud and autonomous systems. It identifies how legal provisions apply, where they are silent, and where they conflict with the needs of effective legal governance. The second technique is document analysis, which is applied to scholarly literature, comparative legal frameworks, and official reports. Document analysis involves critically reading, categorizing, and synthesizing written materials to draw meaningful legal conclusions. Together, these two techniques allow this research to move from description to analysis, and from analysis to concrete legal reform recommendations grounded in both law and scholarship.

This research was conducted with full regard for academic integrity and research ethics. All data used in this study is drawn exclusively from publicly available official documents and peer-reviewed scholarly publications. No private, confidential, or restricted information was accessed or used at any point. Every scholarly article, legal text, and official document from which ideas, arguments, or findings were derived is fully and accurately cited in the reference list of this research. This practice ensures proper attribution to original authors and upholds the ethical obligation to respect intellectual contributions. The researcher has no conflict of interest in relation to this study. This research was conducted solely for academic and scientific purposes, with the objective of contributing to legal knowledge and informing legislative reform in Uzbekistan. No human participants were involved in this research, and therefore no issues of informed consent, anonymity, or participant welfare arise.

Delimitations define the boundaries that this research has intentionally set. This study is geographically delimited to Uzbekistan as the primary jurisdiction of analysis, with the United States, the European Union, China, and South Korea included only for the purpose of comparative legal analysis. The research focuses exclusively on the legal dimensions of deepfake fraud in autonomous systems and does not examine technical, economic, or sociological aspects of the problem. The time period considered for Uzbek legislation is limited to currently applicable laws, and for scholarly literature, preference is given to publications from the last five years.

Limitations reflect constraints that fall outside the researcher's control. The most significant limitation of this research is the rapidly evolving nature of both technology and law. Deepfake technology is continuously advancing, and the legal and regulatory landscape governing it is subject to frequent amendment and development. Laws and policies referenced in this research may be revised, repealed, or supplemented after the date of publication, which could affect the currency of some findings and recommendations. Additionally, the scarcity of published legal scholarship specifically addressing deepfake fraud within Uzbekistan's legal context

means that this research relies heavily on comparative sources, which may not fully capture the nuances of Uzbekistan's domestic legal tradition. These limitations do not undermine the validity of the research but should be considered when applying its conclusions to future legal and policy developments.

This research proceeds on the basis of several reasonable assumptions. It is assumed that all legal texts retrieved from Lex.uz accurately reflect the current state of Uzbekistan's law at the time of writing. It is further assumed that the comparative legal models examined in this research from the United States, the European Union, China, and South Korea represent genuine and enforceable legal frameworks that offer meaningful lessons for Uzbekistan's legislative reform process. It is also assumed that the scholarly sources selected for this research represent credible, evidence-based, and academically sound contributions to the field of AI and digital law. Finally, it is assumed that the findings and recommendations of this research are generalizable to Uzbekistan's broader legal reform needs in the area of deepfake fraud governance, even as specific legislative details may evolve over time.

III. Results

Uzbekistan does not have a specific law targeting deepfake fraud. This is a serious legal gap. The current Criminal Code of Uzbekistan covers general fraud under Article 168. However, it does not mention deepfake technology or autonomous systems. Deepfake fraud is a new and complex crime. It uses artificial intelligence to create fake audio, video, or images. These fakes can deceive autonomous systems easily. The law must catch up with this technology. Some countries, like the United States, have already passed deepfake-specific laws. China has also introduced regulations on synthetic media. Uzbekistan can learn from these examples. Without a clear law, courts in Uzbekistan cannot properly punish deepfake criminals. The government must act quickly. A new legal framework is urgently needed to address this growing threat.

Uzbekistan adopted the Law on Cybersecurity in 2022. This was an important step forward. The law protects critical information systems from cyber threats. However, it does not specifically address deepfake technology. Autonomous systems are not clearly defined in this law either. This creates confusion for law enforcement agencies. Officers do not know which legal tool to apply. The law focuses more on network security than on AI-generated fraud. Deepfake fraud operates differently from traditional cybercrime. It manipulates human identity using artificial intelligence. This makes it harder to detect and prosecute. Estonia and South Korea have broader cybersecurity laws that cover AI threats. Uzbekistan should revise its Cybersecurity Law. New provisions on deepfake detection and liability must be

added. This revision will strengthen the country's legal response to AI-driven fraud.

Autonomous systems are machines that make decisions without human input. They are used in transport, banking, and public services. When deepfakes attack these systems, serious harm can occur. For example, a fake voice command can mislead an autonomous vehicle. A deepfake face can bypass facial recognition in a security system. Uzbekistan's civil law does not clearly assign liability in such cases. It is unclear whether the manufacturer, operator, or user is responsible. The Civil Code of Uzbekistan covers general damages under Article 985. But it was not designed for AI-related harm. Germany's approach to product liability in autonomous systems offers a useful model. Uzbekistan needs clear rules on who is legally responsible. Without this clarity, victims of deepfake attacks on autonomous systems cannot seek justice. A dedicated liability framework is necessary and urgent.

Proving deepfake fraud in court requires strong digital evidence. Uzbekistan's Law on Electronic Documents provides a basic foundation. However, it does not address AI-generated or manipulated content. Deepfake videos and audio are difficult to authenticate. Standard evidence rules were not built for synthetic media. Judges and prosecutors lack technical training in this area. This weakens the prosecution of deepfake cases. The United Kingdom has developed clear standards for digital forensic evidence. Uzbekistan should adopt similar evidentiary standards. Courts must be able to distinguish real content from deepfakes. This requires certified forensic tools and trained experts. The Law on Electronic Documents should be amended accordingly. New rules on the admissibility of deepfake evidence are essential. Without reliable evidence standards, deepfake criminals may escape punishment. Legal reform in this area is both practical and necessary.

Deepfake fraud relies heavily on personal data. Criminals use photos, videos, and voice recordings without consent. Uzbekistan adopted the Law on Personal Data in 2019. This law protects citizens from unauthorized use of their personal information. However, it does not specifically cover biometric data used in deepfakes. Biometric data includes facial features, voice patterns, and fingerprints. Autonomous systems often use this data for identification purposes. If this data is stolen, deepfakes can be created easily. The European Union's GDPR offers strong biometric data protection. Uzbekistan's law must be updated to reflect similar protections. Strict rules on biometric data collection and storage are needed. Penalties for misusing biometric data should also be increased. Stronger data protection will reduce the risk of deepfake fraud. Protecting personal data is the first line of legal defense.

Deepfake fraud does not respect national borders. Criminals can operate from any country. Uzbekistan is a member of the Shanghai Cooperation Organisation (SCO). The SCO has agreements on combating cybercrime among member states.

However, these agreements do not specifically cover deepfake technology. This is a clear limitation. Deepfake criminals targeting Uzbekistan's autonomous systems may be based abroad. Without international cooperation, prosecution becomes very difficult. Interpol has begun addressing AI-related crimes globally. Uzbekistan should actively engage with Interpol on this issue. Bilateral agreements with technologically advanced countries are also helpful. For example, cooperation with South Korea or the EU could bring legal expertise. Uzbekistan must update its international legal commitments. New treaties focusing on AI fraud and deepfake crimes are necessary. Global problems require global legal solutions.

Uzbekistan needs a comprehensive legal response to deepfake fraud. A new dedicated law on AI and synthetic media is recommended. This law should define deepfake technology clearly. It should also criminalize the fraudulent use of deepfakes in autonomous systems. Penalties must be proportionate to the harm caused. Regulatory agencies should be given clear enforcement powers. An independent body to monitor AI-related fraud is also advisable. The law should require mandatory reporting of deepfake incidents. Public awareness campaigns must support the legal framework. Singapore's Model AI Governance Framework offers a practical example. Uzbekistan can adapt such models to its own legal tradition. Coordination between the Ministry of Justice and the Agency for Cybersecurity is essential. Legal education on deepfake fraud should be introduced in universities. A strong legal framework will protect citizens and autonomous systems alike.

IV. Discussion

A. Specific Law on Deepfake Fraud

Uzbekistan's legal system is facing a serious challenge it was never designed to handle. The central question is whether existing laws can effectively address deepfake fraud targeting autonomous systems. The answer, based on careful legal analysis, is that they cannot. Article 168 of the Criminal Code covers general fraud, but it was written for human actors using conventional deception. It was never intended to capture AI-generated synthetic identities or machine-level manipulation. This legislative silence is not a minor technical oversight, it is a fundamental protection gap that leaves citizens and autonomous systems legally exposed.

The practical consequences of this gap are deeply significant. When a deepfake attack deceives an autonomous security system or manipulates an AI-driven decision-making process, prosecutors have no clear legal provision to apply. Courts are left interpreting outdated language to fit entirely new forms of criminal conduct. This produces inconsistent judicial outcomes and, in many cases, complete impunity for offenders. The absence of a legal definition for deepfake technology alone makes prosecution extremely difficult. Without defining the crime, the law cannot punish it

effectively or predictably.

A comparison with other jurisdictions makes Uzbekistan's position even more concerning. The United States passed the Malicious Deep Fake Prohibition Act and introduced the Deepfake Task Force Act to address synthetic media fraud directly. China enacted its Deep Synthesis Provisions in 2022, requiring platforms to label AI-generated content and holding service providers legally accountable. South Korea amended its Act on Special Cases Concerning the Punishment of Sexual Crimes to criminalize deepfake misuse. These countries recognized the threat early and acted decisively. Uzbekistan has not yet taken a comparable step, placing it significantly behind the international legal curve on this issue.

It is also important to acknowledge that this legal gap does not exist in isolation. Uzbekistan is actively modernizing its digital economy and expanding the use of autonomous technologies in transport, public administration, and security. This rapid technological growth is happening faster than the law can follow. The wider Uzbekistan is adopting autonomous systems, the greater the legal vulnerability becomes. Technology is advancing at a pace that naturally outstrips legislative response, and this is a challenge faced by many developing legal systems. However, this reality makes urgent reform more necessary, not less. Uzbekistan's must treat deepfake legislation not as a future consideration but as an immediate legal priority before the consequences of inaction become irreversible.

B. Cyber Law in Uzbekistan

Uzbekistan's adoption of the Law on Cybersecurity in 2022 represented a genuine and important legislative milestone. It signaled that the government recognized digital threats as a serious national concern worthy of dedicated legal attention. However, the critical question this research raises is whether this law is sufficient to address deepfake-driven fraud in autonomous systems. A careful legal reading of the law reveals that it is not. The law was designed primarily to protect critical information infrastructure from conventional cyber intrusions such as hacking, data breaches, and network attacks. Deepfake fraud is a fundamentally different kind of threat. It does not break into a system, it deceives one. This distinction matters enormously in law, because the legal tools designed to address unauthorized access are simply not equipped to handle AI-generated identity manipulation targeting autonomous decision-making systems.

The insufficiency of the 2022 Cybersecurity Law creates very real operational confusion for law enforcement. When a deepfake attack occurs, officers and prosecutors must decide which law applies. The Cybersecurity Law points toward network protection. The Criminal Code points toward general fraud. Neither provision captures the specific nature of deepfake fraud with enough precision to support a confident prosecution. This legal ambiguity is not merely an academic concern, it directly affects whether criminals are charged, prosecuted, and punished. In legal

systems where the law is unclear, the benefit of the doubt typically favors the accused. Deepfake criminals in Uzbekistan currently enjoy that advantage, and the 2022 law does nothing meaningful to remove it.

Comparing Uzbekistan's position with Estonia and South Korea reveals how significant this legislative gap truly is. Estonia, widely regarded as one of the world's most digitally advanced legal systems, has built cybersecurity legislation that explicitly accounts for AI-generated threats and autonomous system vulnerabilities. South Korea has similarly broadened its cybersecurity framework to address synthetic media manipulation as a distinct category of digital crime. Both countries understood that AI-driven fraud requires AI-specific legal language, general cybersecurity provisions are insufficient substitutes. Uzbekistan's 2022 law, despite being relatively recent, did not anticipate this distinction. Its silence on deepfake technology and autonomous systems reflects the speed at which AI threats have evolved, outpacing even newly drafted legislation.

One important factor influencing this limitation is the legislative model Uzbekistan followed when drafting its Cybersecurity Law. Post-Soviet legal systems have historically drawn heavily from Russian legislative frameworks in the area of digital and cybersecurity law. Russian cybersecurity legislation similarly lacks deepfake-specific provisions, which means the foundational model Uzbekistan relied upon carried the same blind spots. This is not a criticism of Uzbekistan's legislative intent; it reflects a broader regional pattern. However, it does mean that revision cannot be superficial. Uzbekistan must look beyond its traditional legislative influences and draw from more technologically progressive models. Adding targeted provisions on deepfake detection obligations, autonomous system definitions, and AI fraud liability to the existing Cybersecurity Law would be a practical and achievable first step toward closing this dangerous legal gap.

C. Autonomous Systems Create New Legal Liability Questions

The emergence of autonomous systems as critical components of modern infrastructure has introduced a legal liability problem that Uzbekistan's civil law was never designed to solve. The fundamental question this result raises is straightforward but legally complex when a deepfake attack causes an autonomous system to malfunction and harm occurs, who is legally responsible? Under Uzbekistan's current Civil Code, Article 985 provides a general framework for damages arising from harmful acts. However, this provision was drafted with human actors and conventional physical harm in mind. It does not contemplate a scenario where an AI-generated fake voice command misleads an autonomous vehicle, or where a synthetic face bypasses a facial recognition security system with devastating consequences. The law's silence on these scenarios is not a gap that creative legal interpretation can easily fill. It is a structural deficiency that demands direct legislative attention (Monga, 2023).

The liability question in deepfake-autonomous system cases is particularly complex because multiple parties are involved at every stage. The manufacturer designs and builds the autonomous system. The operator deploys and manages it. The user interacts with it daily. When a deepfake attack exploits a vulnerability in any of these layers, determining which party bears legal responsibility requires a clear statutory framework. Without one, victims face an almost impossible legal journey. They must navigate overlapping provisions across civil, criminal, and administrative law, often without finding a satisfactory answer in any of them. This uncertainty does not only harm individual victims, it undermines public confidence in autonomous systems as a whole and discourages responsible investment in AI-driven technologies within Uzbekistan.

Germany's legal approach to autonomous system liability offers Uzbekistan a highly instructive comparative model. Germany amended its Road Traffic Act to address liability in autonomous vehicle incidents, establishing clear rules that distribute responsibility among manufacturers, operators, and users based on the specific circumstances of each case. Germany also introduced mandatory event data recording requirements, ensuring that evidence of system behavior is preserved for legal proceedings. More recently, the European Union's AI Liability Directive has proposed harmonized rules for assigning civil liability in AI-related harm cases across member states. These developments reflect a growing international consensus that general tort law principles are insufficient for the AI age and that dedicated liability frameworks are essential. Uzbekistan stands to benefit enormously from studying and adapting these models to its own legal and institutional context.

It is also important to recognize that autonomous systems in Uzbekistan are not a distant future prospect, they are an emerging present reality. Uzbekistan has been actively developing its digital economy and smart city initiatives, with autonomous technologies increasingly appearing in transport planning, public administration, and financial services. This rapid adoption is happening in a legal environment that provides no clear liability rules for AI-driven harm. The faster autonomous systems are deployed, the more urgent the need for a dedicated liability framework becomes. Technology in this field does not wait for the law to catch up, and every day that passes without clear liability rules is a day that victims of deepfake attacks on autonomous systems are left without a meaningful path to justice. Uzbekistan's must treat this not as a theoretical legal exercise but as a pressing and practical obligation to its citizens.

D. Digital Evidence

The ability to prove a crime in court is just as important as the existence of a law that criminalizes it. This result addresses a critical but often overlooked dimension of Uzbekistan's legal response to deepfake fraud, the capacity of its evidentiary framework to support successful prosecution. Uzbekistan's Law on

Electronic Documents provides a foundational recognition that digital materials can serve as legal evidence. However, this law was drafted in an era when digital evidence meant emails, scanned documents, and basic electronic records. It was never designed to handle AI-generated synthetic media, where the very nature of the content is designed to appear authentic while being entirely fabricated. Deepfake videos and audio recordings present courts with an entirely new evidentiary challenge, one that existing legal standards are wholly unprepared to meet. The result is a justice system that can identify a crime but struggle to prove it beyond reasonable doubt (Allah Rakha, 2024).

The practical consequences of this evidentiary weakness are serious and immediate. Judges presiding over deepfake fraud cases must evaluate synthetic media without any legally established framework for doing so. Prosecutors attempting to introduce deepfake evidence face defense challenges they cannot always overcome, because no certified authentication standard exists to confirm whether submitted content is genuine or manipulated. This evidentiary uncertainty creates a dangerous opening for deepfake criminals to escape punishment, not because they are innocent, but because the legal system lacks the tools to prove their guilt convincingly. The absence of technical training among judges and prosecutors compounds this problem further. Legal professionals cannot apply standards that do not exist, and they cannot evaluate evidence they are not equipped to understand. This combination of legislative silence and institutional unpreparedness significantly weakens Uzbekistan's ability to deliver justice in deepfake fraud cases.

A comparison with the United Kingdom's approach to digital forensic evidence illustrates how much stronger Uzbekistan's evidentiary framework could be with targeted reform. The United Kingdom has developed the Association of Chief Police Officers guidelines on digital evidence, establishing clear standards for the collection, preservation, authentication, and presentation of digital materials in court. The UK's Crown Prosecution Service has also issued specific guidance on handling AI-generated content as evidence, ensuring that prosecutors and judges operate within a consistent and legally sound framework. Similarly, the United States Federal Rules of Evidence have been interpreted and applied to address the authentication of digital and AI-generated content, with courts increasingly requiring expert forensic testimony to establish evidentiary reliability. These models demonstrate that strong digital evidence standards are legally achievable and practically effective. Uzbekistan does not need to reinvent the wheel; it needs to adapt proven frameworks to its own judicial context.

Several important factors influence the urgency of this reform. Deepfake detection technology is advancing rapidly, with AI-powered forensic tools now capable of identifying synthetic media with increasing accuracy. However, these tools only serve justice if courts are legally authorized to rely on them and if forensic

experts are formally recognized within the evidentiary framework. Without legislative reform, even the most sophisticated detection technology cannot be effectively deployed in Uzbek courtrooms. Furthermore, the global trend toward digital court proceedings and electronic evidence submission makes this reform even more pressing. As Uzbekistan modernizes its judicial infrastructure, it has a timely opportunity to embed deepfake-specific evidentiary standards into its broader digital justice reforms. Amending the Law on Electronic Documents to include provisions on synthetic media authentication, certified forensic tools, and expert witness qualifications would transform Uzbekistan's courts from legally unprepared to genuinely capable of confronting deepfake fraud with confidence and credibility (Abdel-Wahab & Alkhatib, 2026).

E. Key Role of Data Protection Law

Deepfake fraud does not begin with the creation of a fake video or a synthetic voice, it begins with the theft or misuse of personal data. This result identifies data protection law as a foundational pillar in any serious legal response to deepfake-driven fraud in autonomous systems. Uzbekistan's Law on Personal Data, adopted in 2019, represents a meaningful legislative commitment to protecting citizens' personal information from unauthorized use. However, a careful legal examination reveals that this law was drafted before biometric data became the primary raw material for deepfake creation. It protects conventional personal data such as names, addresses, and identification numbers with reasonable effectiveness. What it fails to do is provide specific, enforceable protections for biometric data, the facial features, voice patterns, and physiological characteristics that deepfake technology exploits most directly. This omission is not a minor technical gap. It is a fundamental weakness at the very foundation of Uzbekistan's anti-deepfake legal architecture.

The legal significance of this gap becomes clear when examining how autonomous systems operate. These systems rely heavily on biometric data for identification and authentication purposes. Facial recognition systems, voice-activated autonomous devices, and biometric access control platforms all process sensitive biological information as a core functional requirement. When this biometric data is inadequately protected by law, it becomes dangerously accessible to criminals seeking to create convincing deepfakes. A stolen facial image or voice recording can be transformed into a synthetic identity capable of deceiving an autonomous system within hours. Uzbekistan's 2019 law provides no specific rules governing how biometric data must be collected, stored, encrypted, or deleted. It imposes no special obligations on organizations that handle biometric information, and it prescribes no enhanced penalties for its misuse. This leaves autonomous systems built on biometric authentication legally exposed at their most vulnerable point.

The European Union's General Data Protection Regulation provides the most instructive and widely adopted comparative model for biometric data governance. The

GDPR classifies biometric data as a special category of sensitive personal data, subjecting it to significantly stricter processing conditions than ordinary personal information. Organizations must demonstrate an explicit legal basis for processing biometric data, obtain clear and informed consent, implement robust technical security measures, and conduct mandatory data protection impact assessments before deploying biometric systems. Violations attract substantial financial penalties, with fines reaching up to four percent of annual global turnover. This rigorous framework has set a global standard that many countries are now adopting or adapting. Brazil's Lei Geral de Proteção de Dados and South Korea's Personal Information Protection Act both incorporate similarly strong biometric data protections. Uzbekistan's 2019 law, by contrast, remains significantly behind this international standard, leaving a legal vacuum that deepfake criminals are well positioned to exploit.

Several additional factors amplify the urgency of reforming Uzbekistan's data protection framework. Uzbekistan has been actively expanding its digital public services, including biometric identification systems for government administration and border control. The wider these biometric databases grow, the more attractive they become as targets for data theft and deepfake exploitation. At the same time, Uzbekistan's ambitions to integrate more deeply with international digital trade and data sharing frameworks will increasingly require it to demonstrate adequate data protection standards equivalent to those of its trading partners. Updating the Law on Personal Data to include explicit biometric data protections, mandatory security standards for biometric storage, enhanced penalties for biometric data misuse, and clear rules governing biometric data use in autonomous systems would simultaneously strengthen Uzbekistan's domestic legal defenses and advance its international digital credibility. Strong data protection is not merely a legal obligation, it is the first and most essential line of defense against deepfake fraud in an increasingly autonomous world.

F. Research Implication

The findings of this research fundamentally challenge the long-held legal assumption that existing general laws are sufficiently adaptable to govern emerging AI-driven threats. This assumption has guided Uzbekistan's legislative posture for years, but the evidence presented across all five results demonstrates that it is no longer tenable. General legal provisions simply cannot stretch far enough to cover the precision, speed, and complexity of deepfake fraud in autonomous systems. On the positive side, this research provides Uzbekistan's lawmakers, judges, prosecutors, and regulatory agencies with a clear, evidence-based diagnosis of where the law fails and a directionally sound roadmap for reform. Citizens whose biometric data is processed by autonomous systems, victims of AI-driven fraud, and institutions deploying autonomous technologies in transport, security, and public administration all stand to benefit directly from the legal reforms this research advocates. However, a significant

challenge remains, technology evolves faster than legislation, and any legal framework adopted today risks becoming outdated as deepfake capabilities advance further. Policy amendments will require continuous review mechanisms built into the law itself. Uzbekistan must move beyond reactive legislation and build a proactive legal culture capable of anticipating AI-driven threats before they outpace the law entirely.

G. Research Recommendations

Uzbekistan must move decisively from legal awareness to legislative action. The most urgent step is the enactment of a dedicated law on synthetic media and AI-generated fraud. This law should clearly define deepfake technology, criminalize its fraudulent use in autonomous systems, and establish proportionate penalties. The Criminal Code, the Cybersecurity Law of 2022, and the Personal Data Law of 2019 must all be amended to include specific provisions addressing deepfake threats and biometric data misuse. Uzbekistan should establish an independent regulatory body with the authority to monitor AI-driven fraud, certify forensic detection tools, and enforce compliance across both public and private sectors. Drawing inspiration from the EU AI Act of 2024 and Singapore's Model AI Governance Framework, Uzbekistan can adapt these internationally tested models to reflect its own legal tradition and institutional capacity. Judges and prosecutors must receive specialized training in synthetic media forensics and digital evidence standards. These are areas that current legal education in Uzbekistan does not adequately cover. Scholarly attention should also expand toward examining how other Central Asian legal systems are responding to deepfake threats, as regional comparative research remains almost entirely absent from academic discourse. As deepfake technology continues advancing rapidly, any legal framework adopted today must include built-in review mechanisms ensuring the law remains current, enforceable, and genuinely protective of citizens and autonomous systems alike.

Conclusion

Artificial intelligence has fundamentally changed the nature of fraud, and the law must change with it. Deepfake technology now threatens the integrity of autonomous systems that millions of people rely on every single day. Uzbekistan sits at a critical crossroads, its digital economy is expanding rapidly, its smart city initiatives are growing, and autonomous technologies are becoming embedded in transport, security, and public administration. Yet its legal defenses against AI-driven fraud remain dangerously underdeveloped. The Criminal Code, the Cybersecurity Law of 2022, and the Personal Data Law of 2019 each carry significant blind spots when confronted with deepfake fraud targeting autonomous systems. These are not minor technical oversights that careful judicial interpretation can resolve. They

represent a fundamental and structural mismatch between the threats Uzbekistan faces today and the legal instruments it currently holds. This mismatch grows more dangerous with every autonomous system deployed without adequate legal protection behind it.

The evidence presented throughout this research tells a consistent and deeply urgent story. No single existing law in Uzbekistan adequately defines, criminalizes, or provides meaningful remedies for deepfake fraud in autonomous systems. Liability for AI-driven harm remains legally unclear, leaving victims without a reliable path to justice. Digital evidence standards are insufficient for synthetic media, weakening prosecution in every deepfake fraud case that reaches a courtroom. Biometric data protection falls critically short of international benchmarks, exposing the very data that autonomous systems depend upon to criminal exploitation. Countries that recognized this threat early and acted decisively now have measurably stronger legal frameworks and more confident enforcement capacities. Their legislative experiences confirm a shared conclusion that dedicated, precise, and regularly reviewed legislation is the only genuinely effective legal response to AI-driven fraud. Uzbekistan cannot responsibly treat this as a future legislative priority any longer.

The path forward is both clear and entirely achievable within Uzbekistan's existing legislative and institutional capacity. A dedicated law on synthetic media fraud, targeted amendments to the Criminal Code and Cybersecurity Law, enhanced biometric data protections, certified digital forensic standards, and an independent AI regulatory body are all practical and proportionate reform steps. The EU AI Act of 2024, which introduced a comprehensive risk-based governance framework for artificial intelligence, and China's continuously refined Deep Synthesis Provisions demonstrate that even the most complex AI governance challenges can be addressed through focused, well-designed legal reform. Scholars, policymakers, judges, and legal practitioners across Central Asia must now engage with these questions seriously, collaboratively, and urgently.

Bibliography

Abdel-Wahab, A., & Alkhatib, M. (2026). Toward Robust Deepfake Defense: A Review of Deepfake Detection and Prevention Techniques in Images. *Computers, Materials & Continua*, *86*(2), 1–34. https://doi.org/10.32604/cmc.2025.070010

Allah Rakha, N. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*, 23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Babaei, R., Cheng, S., Duan, R., & Zhao, S. (2025). Generative Artificial Intelligence and the Evolving Challenge of Deepfake Detection: A Systematic Analysis. *Journal of Sensor and Actuator Networks*, *14*(1), 17. https://doi.org/10.3390/jsan14010017

Durlik, I., Miller, T., Kostecka, E., Zwierzewicz, Z., & Łobodzińska, A. (2024). Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge? *Electronics*, *13*(13), 2654. https://doi.org/10.3390/electronics13132654

Easttom, W. (2025). Deepfake Technology: Emerging Threats and Security Implications. *International Conference on Cyber Warfare and Security*, *20*(1), 79–85. https://doi.org/10.34190/iccws.20.1.3283

Folorunsho, F., & Boamah, B. F. (2025). DEEPFAKE TECHNOLOGY AND ITS IMPACT: ETHICAL CONSIDERATIONS, SOCIETAL DISRUPTIONS, AND SECURITY THREATS IN AI-GENERATED MEDIA. *INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY AND MANAGEMENT INFORMATION SYSTEMS*, *16*(1), 1060–1080. https://doi.org/10.34218/IJITMIS_16_01_076

Hynek, N., Gavurova, B., & Kubak, M. (2025a). Risks and benefits of artificial intelligence deepfakes: Systematic review and comparison of public attitudes in seven European Countries. *Journal of Innovation & Knowledge*, *10*(5), 100782. https://doi.org/10.1016/j.jik.2025.100782

Hynek, N., Gavurova, B., & Kubak, M. (2025b). Risks and benefits of artificial intelligence deepfakes: Systematic review and comparison of public attitudes in seven European Countries. *Journal of Innovation & Knowledge*, *10*(5), 100782. https://doi.org/10.1016/j.jik.2025.100782

Monga, G. (2023). LEGAL ACCOUNTABILITY OF AUTONOMOUS AI SYSTEMS IN CRIMINAL JUSTICE. *ShodhKosh: Journal of Visual and Performing Arts*, *4*(2), 5848–5852. https://doi.org/10.29121/shodhkosh.v4.i2.2023.6172

Park, P. S., Goldstein, S., O'Gara, A., Chen, M., & Hendrycks, D. (2024). AI deception: A survey of examples, risks, and potential solutions. *Patterns*, *5*(5), 100988. https://doi.org/10.1016/j.patter.2024.100988

Sunil, R., Mer, P., Diwan, A., Mahadeva, R., & Sharma, A. (2025). Exploring autonomous methods for deepfake detection: A detailed survey on techniques and evaluation. *Heliyon*, *11*(3), e42273. https://doi.org/10.1016/j.heliyon.2025.e42273