BULLETIN OF THE INSTITUTE OF LEGISLATION
AND LEGAL INFORMATION OF THE
REPUBLIC OF KAZAKHSTAN
ISSN 2788-5283
eISSN 2788-5291
TOM 80 No 3(2025), 357-368

UDC 343.3/.7
IRSTI 10.77.51
DOI 10.52026/2788-5291_2025_80_3_357
Scientific article

© N.M. Apsimet[1]*, 2025
[1] al-Farabi Kazakh National University,Almaty, Kazakhstan
(E-mail: Apsimet.nurdaulet@gmail.com)

CRIMES INVOLVING DEEPFAKE IN ONLINE FRAUD AND THE CHALLENGES OF PROVING THEM

Abstract. This research explores crimes committed using deepfake technology in the context of online fraud. The aim of the study is to analyze how deepfakes are applied in fraudulent schemes, identify key challenges in investigating and proving such crimes, and offer recommendations for improvement. The methodology includes forensic analysis of deepfake detection technologies, comparative review of international practices, examination of academic sources, and analysis of Kazakhstan's legislation on cybercrime.

The study identifies three major areas of criminal deepfake use: financial fraud, blackmail and extortion, and political manipulation. Cases are examined where deepfakes were used to bypass identity verification systems, produce fake videos and audio recordings to steal money, and spread disinformation. Particular focus is placed on the difficulties of classifying and proving these offenses due to the lack of specific legal norms and investigative tools. The study also reviews current detection technologies, such as microexpression analysis and audio spectral analysis.

The results of the study may contribute to improving Kazakhstan's criminal law, developing forensic techniques for investigating deepfake crimes, and raising awareness among experts and the public. The research concludes that deepfake technology presents a growing threat to information security and public order, complicating the process of criminal investigation and prosecution. The need for updated legislation, specialized detection methods, and international cooperation is strongly emphasized.

Keywords: deepfake, falsification, online fraud, cybercrime, proving, forensic analysis.

Introduction

Modern artificial intelligence significantly impacts the digital environment, offering societal benefits yet posing substantial information security risks. One of the most controversial innovations is deepfake technology, capable of creating highly realistic falsified audio and video content. Initially popular in entertainment and digital marketing, deepfakes have increasingly been utilized in criminal activities, notably online fraud.

The proliferation of deepfake-related crimes is facilitated by advanced machine learning algorithms enabling real-time manipulation of audio and video, convincingly replicating individuals' appearance and voice. This presents new opportunities for perpetrators in financial fraud, social engineering, and blackmail. For example, in 2019, criminals in the UK successfully defrauded a company of €220,000 by impersonating the CEO's voice using deepfake technology, underscoring its effectiveness

* Corresponding authors. E-mail: Apsimet.nurdaulet@gmail.com.

and detection challenges [1].

While Kazakhstan lacks official statistics specifically on deepfake fraud, broader cybercrime data indicate a significant increase in online fraud. According to Kazakhstan's Committee on Legal Statistics, 22,900 internet fraud cases were recorded in 2024, with 81.8% terminated due to unidentified perpetrators. Financial losses reached 11.4 billion tenge – 2.8 times higher than in 2023 – with individuals bearing the brunt of damage (11 billion tenge), followed by legal entities (385 million tenge) and state organizations (8.4 million tenge). Prominent fraud types included unauthorized access to personal data (6,500 cases), fraudulent online services (5,500), goods purchases (5,200), and fraudulent online loans (3,900). These figures emphasize the urgency of enhancing investigative and preventive strategies.

Criminal schemes utilizing deepfake technology, particularly fraudulent video calls impersonating financial institutions, government officials, or relatives, represent a significant concern. These tactics undermine traditional identity verification methods, exploiting inherent trust in visual communication. Additionally, deepfakes are widely employed in blackmail, defamation, and disinformation campaigns targeting public officials and influencing political stability, posing risks of reputational harm and public unrest.

Kazakhstan's President Kassym-Jomart Tokayev has repeatedly highlighted cybersecurity's importance, notably addressing these issues during the Shanghai Cooperation Organization summit. He directed law enforcement agencies to intensify measures against cybercrime and fraud. In response, Kazakhstan adopted the "Cyber Shield of Kazakhstan" Concept, aimed at safeguarding electronic information resources and infrastructure. However, despite these initiatives, combating deepfake crimes remains challenging due to inadequate specialized detection methods.

Current Kazakhstani criminal legislation lacks explicit regulations addressing deepfake-related crimes, creating legal gaps complicating investigation and prosecution. The absence of norms specifically targeting digital audiovisual forgery hampers evidence collection. Thus, there is a pressing need for enhanced forensic detection techniques, standardized judicial procedures, and legislative adaptation to address evolving digital threats.

This research aims to analyze deepfake applications in online fraud comprehensively, identify investigative and prosecutorial obstacles, and propose evidence-based legal responses. The scientific relevance lies in addressing synthetic media crimes through criminal law and forensic methodologies, contributing to stronger protective frameworks against digital threats.

Methods and materials

The research employed an interdisciplinary approach combining legal analysis, technological insights, and academic scholarship. It focused on criminal and cybercrime regulations in Kazakhstan, particularly the Criminal Code and the strategic initiative "Cyber Shield of Kazakhstan". Scholarly literature on deepfake technology, cyber fraud, and digital criminality was reviewed, alongside open-source materials and media reports on relevant incidents both domestically and internationally. Empirical data from international organizations and leading tech companies further enriched the analysis.

Forensic techniques assessed deepfake detection methods, while comparative legal analysis examined regulations in the US, EU, and China. A doctrinal review covered prevailing academic views. Collected data underwent analytical-synthetic processing, forming conclusions and policy recommendations.

Results

Deepfake technology has rapidly evolved, creating new cyber-enabled fraud threats that endanger personal privacy, financial systems, public institutions, and social structures. Current criminal trends reveal three primary fraudulent uses of deepfakes: financial scams, extortion schemes, and manipulation of political discourse. Each of these domains presents distinct challenges, including detection difficulties and significant social impacts, necessitating detailed investigation and tailored legal responses.

Financial fraud is a prevalent form of deepfake-related crime, as fabricated audio and video materials are employed to execute deceptive financial transactions.

Advanced artificial intelligence algorithms enable criminals to convincingly alter individuals' appearance and voice in real-time, creating authentic-looking communications purportedly from bank personnel, corporate executives, or business partners. The banking sector is particularly vulnerable to such deepfake schemes, where perpetrators impersonate clients or executives to fraudulently authorize fund transfers. The integration of sophisticated audio-visual manipulation with social engineering complicates the identification and prevention of these crimes.

A significant incident in 2020, in the United Arab Emirates, highlighted the severity of deepfake threats. Fraudsters effectively mimicked the voice and appearance of a high-ranking corporate executive, misleading a bank manager into approving an unauthorized transfer of roughly $35 million [2]. Such cases underscore the growing ineffectiveness of conventional verification methods, such as audio-visual identification, against advanced deepfake techniques.

Another widespread fraud method involves criminals leveraging artificially generated video and audio content to impersonate real clients when applying for loans or credit. Offenders produce realistic video statements, allegedly featuring genuine bank customers verifying their identities and explicitly consenting to loan terms. After obtaining the funds, perpetrators disappear, leaving victims with substantial financial losses and legal challenges, as the convincing fabricated evidence complicates disputing their purported involvement[1].

Financial institutions need to implement innovative safeguards because fraudulent activities continue to grow more complex and realistic. Advanced biometric verification systems which use multi-factor authentication together with microexpression recognition techniques and specialized algorithms for detecting digitally manipulated media show great potential as solutions. The financial ecosystem requires strong defense mechanisms against deepfake-enabled fraud to protect individual financial security and maintain trust stability in the face of escalating digital threats.

Deepfake technologies serve as powerful instruments for generating deceptive compromising material which criminals use to blackmail victims and exert coercive control. The ability to generate realistic fake visual content creates a distinctive threat because people risk facing false accusations from disturbingly convincing yet completely fabricated materials. The ability to identify genuine content from deepfakes has become increasingly complex which puts victims at risk of severe psychological damage and severe damage to their reputation.

People whose professional success depends on their public image face the highest risk including politicians and senior government employees and corporate leaders and famous celebrities. Criminals create fake videos showing these persons in compromising positions and then threaten to release the content unless they pay extortion money. The perpetrators intentionally spread false information through online channels to damage the victim's credibility while increasing social pressure.

The political consequences of deepfake misuse became evident through a major incident in the United States during 2024 which showed how these manipulations moved from personal harm to affect the wider public domain. A satirical video featuring Vice President Kamala Harris spread across social media platforms after artificial intelligence successfully replicated her voice with remarkable precision. Although she had never made the statements attributed to her in the clip, the video nonetheless left many viewers convinced of its authenticity. The incident triggered widespread public discourse and prompted scholars and legal experts to reexamine the ethical boundaries and regulatory gaps associated with AI-generated media in political contexts [3].

Adolescents and young adults represent a particularly at-risk group for deepfake-related exploitation. The capacity of such technology to fabricate highly realistic but fictitious video content makes it possible to depict individuals in

[1] Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks. A Report by the FS-ISAC Artificial Intelligence Risk Working Group. // URL: https://www.fsisac.com/hubfs/Knowledge/AI/DeepfakesInTheFinancialSector-UnderstandingTheThreatsManagingTheRisks.pdf (date of reference: 28.01.2025).

compromising or inappropriate contexts. These fabricated materials are frequently weaponized to apply psychological pressure, extort financial or other forms of compliance from victims, and often result in significant emotional harm and enduring psychological consequences.

Prosecuting deepfake-based blackmail and extortion poses a range of legal and technical difficulties. Proving the inauthenticity of manipulated media demands the use of cutting-edge digital forensic methods – such as metadata scrutiny, advanced content verification tools, and coordinated collaboration with global online platforms that serve as channels for distribution. The intricate nature of these cases highlights the urgent necessity for both the enhancement of investigative capabilities and reform of existing legal structures, which are often ill-equipped to handle rapidly evolving digital threats.

An equally alarming concern is the deployment of deepfakes as instruments of political manipulation. Synthetic media can simulate political figures making fabricated declarations or participating in staged scenarios, thus offering a potent method of defamation, political sabotage, or deliberate social destabilization. When disseminated tactically, such forgeries can undermine public confidence in institutions, distort the democratic process, and incite social divisions. There is mounting evidence of deepfakes being used during electoral campaigns to disseminate false statements attributed to political candidates [4, p. 455]. The technology behind deepfakes has moved beyond domestic political use and is now widely used in geopolitical relations for international propaganda and psychological operations. The goal of such utilization involves spreading false information while disrupting diplomatic relations and altering how people view reality. The quick development of this phenomenon creates major challenges for investigative journalism and academic research and human rights advocacy because it makes it harder to distinguish between authentic content and artificially created digital media.

A solution to deepfake political misuse requires multiple integrated measures. The regulation of synthetic audiovisual media requires specialized legislative frameworks together with advanced technological instruments to verify digital content authenticity and its creation and dissemination regulation. The establishment of independent expert panels dedicated to objective evaluation of questionable digital materials represents an essential measure. Public digital literacy programs combined with awareness initiatives create substantial societal resistance against manipulative tactics.

The fast development of artificial intelligence systems which merge with current digital communication networks creates complex legal challenges for defining and prosecuting deepfake-related crimes. Deepfake technology differs from standard fraudulent methods because it creates realistic audiovisual evidence that mimics authentic materials. Law enforcement agencies face major challenges when trying to classify and prosecute these cases because they involve complex technology and no established judicial guidelines.

The criminal legislation of Kazakhstan lacks specific provisions that directly address offenses related to deepfake technologies. At present, criminal cases tied to synthetic media usage are typically subsumed under general articles such as fraud (Article 190), dissemination of false information (Article 274), extortion (Article 194), or misuse of personal data (Article 147). These legal norms, however, were initially formulated without considering the distinct nature and implications of deepfake technology, thus creating ambiguity. The legal status becomes particularly uncertain in cases where synthetic audiovisual impersonation is used to secure financial or other gains, as it is unclear whether such acts constitute forgery, cybercrime, or a separate, specialized type of digital deception.

One of the primary investigative challenges in prosecuting crimes involving deepfake technology is verifying digital content authenticity. This issue intensifies when manipulated media intentionally distort critical judicial contexts, such as falsely representing a victim's consent. Historically, audiovisual evidence has been deemed credible proof in courts, making the rise of convincing synthetic materials particularly troubling regarding evidence reliability and admissibility.

Identifying deepfakes demands advanced forensic techniques and specialized digital expertise. Early deepfake content featured noticeable anomalies, like unnatural facial movements; however, technological progress has considerably reduced these evident flaws. Nonetheless, contemporary deepfakes still exhibit subtle visual or auditory imperfections identifiable through detailed forensic analysis. Automated detection tools, although increasingly utilized, currently recognize only approximately 65% of manipulated media, often without clearly contextualizing the specific alterations [5, p. 2]. Specialists emphasize that as generative AI evolves, these detection tools will face greater challenges, particularly with the increasing availability of sophisticated disinformation techniques.

Technological responses, such as digital watermarking, public-key cryptography, and advanced authentication processes, have been suggested to counter deepfake proliferation, yet they presently offer incomplete protection. A significant unresolved issue remains the absence of an internationally recognized framework for authenticating digital media.

The ease of deepfake creation, enabled by widely available software and minimal technical skills, has substantially facilitated their spread, especially through social media, rapidly undermining public trust in digital content. Consequently, deepfakes carry profound social implications beyond technological concerns, impacting public confidence in official institutions and traditional information sources. Experts underline that demonstrating falsification remains technically demanding, resource-intensive, and complex, even amid efforts to develop blockchain-based verification solutions.

The fight against deepfake technology is actively supported by researchers and forensic experts developing advanced analytical methods and machine learning models. The scientific community emphasizes creating automated tools capable of reliably detecting digital manipulations, thus strengthening anti-fraud measures in cyberspace.

One effective approach analyzes subtle facial movements and eye-blinking patterns. Studies indicate that deepfake videos often contain irregularities, such as unnatural eye movements, inconsistent facial expressions, and abnormal blinking rates. Although difficult for humans to detect, specialized algorithmic analysis efficiently identifies these anomalies. Modern detection frameworks frequently employ convolutional neural networks (CNNs) combined with long short-term memory (LSTM) models, effectively capturing temporal variations across sequential video frames, significantly improving detection accuracy [6, p. 229].

Similarly, in audio forensics, spectral analysis of sound signals is crucial. Synthetic audio generated by advanced voice-synthesis technologies exhibits distinct frequency-related distortions and subtle acoustic irregularities. Techniques like Short-Time Fourier Transform (STFT), Constant-Q Transform (CQT), and Wavelet Transform (WT), especially when combined with auditory filters such as Mel or Gammatone, successfully detect artificial audio features. These analytical methods enable forensic experts to identify synthetic audio often used in fraud, fake communications, or voice imitation attacks [7, p. 1].

Collaboration between law enforcement and major tech companies, including Google, Microsoft, and Meta, further strengthens efforts against deepfake threats. For instance, Meta initiated the global Deepfake Detection Challenge in 2020 to advance automated identification methods [8]. Initiatives of this kind accelerate technological developments and support countries in establishing national systems tailored to specific geopolitical and security contexts.

Combining advanced forensic methodologies across audio and visual domains with coordinated actions by state authorities and technology enterprises significantly improves global resilience against criminal activities involving deepfake technologies.

Discussion

Deepfake technologies empower criminals to execute sophisticated fraud by generating highly realistic audiovisual content distinct from traditional forgeries and misinformation. The synthetic media produced are extremely convincing, complicating forensic differentiation between genuine and artificial recordings.

Consequently, law enforcement faces considerable difficulties in identifying digital forgeries due to the absence of identifiable modifications or reference points.

Increasingly, deepfake-driven cybercrimes pose severe challenges to various sectors, notably financial institutions, by facilitating targeted attacks against both individuals and organizations. These offenses differ fundamentally from conventional fraud techniques, requiring significant revisions in digital evidence standards and specialized forensic methodologies designed explicitly to detect synthetic media.

Security systems relying on biometric verification methods such as facial recognition and voice authentication are particularly vulnerable to deepfake manipulations. Fraudsters use advanced machine-learning algorithms to produce realistic audiovisual content capable of deceiving even experienced security personnel. Recent cases demonstrate attackers employing deepfake technology to impersonate executives, prompting unauthorized financial transfers and accessing protected banking platforms without leaving traditional forensic traces.

Kazakhstan's existing criminal legislation inadequately addresses the unique characteristics of deepfake-enabled offenses. Current provisions in Article 190 (Fraud) and Article 385 (Forgery of Documents) of the Criminal Code target conventional falsification methods but fail to encompass the distinctive threats of synthetic digital identities. Therefore, legislative reform is essential to close this gap and enable effective law enforcement responses to crimes involving artificially generated personas.

The misuse of deepfake technologies further threatens critical public services, governmental processes, educational institutions, and notarization systems reliant on robust identity verification. By exploiting vulnerabilities within facial and vocal authentication procedures, offenders gain unauthorized access to protected platforms and confidential databases, perpetrating fraud under false digital identities.

A critical dimension of deepfake-related threats involves compromising official identity verification procedures through real-time audiovisual impersonations, circumventing conventional forensic detection methods. Traditional forensic techniques struggle to analyze intangible AI-generated evidence, underscoring the necessity for innovative investigative approaches.

The escalating threat of identity theft via deepfake tools increasingly compromises cybersecurity. Attackers leverage biometric data acquired from public social media and compromised databases to create fabricated identities. Traditional authentication methods, including passwords, PINs, and basic biometrics, are becoming inadequate against these threats, demanding prompt updates to Kazakhstan's cybersecurity framework. The iProov report underscores the urgency, noting a dramatic increase in deepfake-based attacks, with Native Virtual Camera attacks rising by 2,655% and Face Swap attacks growing by 300% over the past year [9].

Deepfake technology, initially prominent in financial and cyber offenses, now serves increasingly in personal crimes, including blackmail, defamation, disinformation, and public manipulation. By creating realistic audiovisual content falsely depicting individuals in criminal or compromising situations, deepfakes threaten both criminal justice integrity and personal reputations. Due to their realism, such materials often evade immediate scrutiny, causing substantial reputational harm even if proven false.

Deepfakes represent a new level of digital manipulation, commonly used for coercion, extortion, or political sabotage. Dissemination through social media, encrypted messengers, and pseudo-news platforms accelerates the spread, complicating timely debunking. This technology creates an illusion of credible evidence, enabling fabricated events to appear authentic, thereby undermining public perception, judicial processes, and democratic institutions.

Kazakhstan's criminal law currently addresses deepfake misuse through existing articles on dissemination of false information (Article 274), extortion (Article 194), and invasion of privacy (Article 147). However, there is no explicit regulation targeting identity falsification or synthetic audiovisual content, creating challenges in properly classifying and prosecuting such

offenses. Addressing this legislative gap by introducing specific provisions on digital identity fraud and enhancing investigative protocols becomes crucial.

Rapid advancements in deepfake technology challenge traditional forensic methods, which previously relied on visible editing traces. Unlike conventional modifications, deepfakes produce entirely new, highly realistic content, complicating detection and necessitating new forensic techniques. In response, forensic science prioritizes developing sophisticated verification tools and analytical frameworks, supported by updated legislation and investigative strategies.

Current forensic research emphasizes analyzing subtle physiological indicators such as facial muscle dynamics, emotional expressions, and speech synchronization. Despite improvements in synthetic media, deepfake algorithms often fail to accurately replicate natural facial expressions, eye movements, or speech synchronization [10, p. 1]. Researchers actively develop algorithms targeting these subtle anomalies. Additionally, forensic analysts increasingly examine nuanced elements like skin textures, shadow inconsistencies, and lighting imperfections, which neural networks still struggle to render flawlessly.

Acoustic forensic analysis also effectively identifies deepfake-generated audio by detecting subtle digital artifacts invisible to human listeners, using advanced spectral and frequency-based methods. Such analysis reveals unnatural tonal fluctuations, irregular pauses, and frequency deviations, allowing reliable differentiation between synthetic and genuine recordings.

Modern forensic approaches predominantly leverage artificial intelligence to automatically detect digital manipulations, analyzing extensive audio-visual data against established indicators of authenticity. However, continuous perpetrator advancements necessitate persistent and rapid technological progress in forensic detection tools.

The increasing spread of manipulated digital content prompts the judicial community to critically reassess the traditional reliance on audio, visual, and photographic evidence, given that their authenticity can no longer be presumed. Consequently, there is an urgent need to update procedural standards for validating digital evidence. In response, some jurisdictions, notably in the United States and several European Union countries, have already integrated advanced digital forensic protocols, enabling judicial bodies to systematically verify media authenticity prior to their use as admissible evidence in court. Leveraging AI-driven methods, these jurisdictions evaluate the authenticity and detect potential manipulation within digital files, thereby furnishing the judiciary with reliable scientific tools for accurate evaluation of evidence integrity[2].

At present, Kazakhstan's criminal legislation lacks explicit norms dedicated specifically to offenses involving deepfake technology. Investigative and prosecutorial efforts are thus guided by general provisions of existing criminal statutes, which frequently fail to fully address the nuanced complexities inherent in digital manipulation. This gap between current technological practices and legislative frameworks significantly hampers accurate criminal classification, investigation effectiveness, and judicial evaluation of such offenses.

At present, liability for crimes involving deepfake may arise under the following articles of the Criminal Code of the Republic of Kazakhstan:

– article 190 – fraud, in cases where deepfake is used to deceive financial institutions or private individuals for unlawful gain;

– article 385 – forgery of documents, when deepfake is used to simulate official identity documents or other legal instruments;

– article 147 – violation of privacy, in instances where deepfake content is used to unlawfully collect or disseminate personal information or to intrude upon a person's private life;

– article 274 – dissemination of knowingly false information, if deepfake materials are employed for the purpose of manipulating public opinion or spreading disinformation.

The distinct nature of deepfake-related offenses stems from their capability to substitute identities and create synthetic

[2] Electronic Evidence. Eucrim 2023/2. // URL: https://eucrim.eu/media/issue/pdf/eucrim_issue_2023-02.pdf (date of reference: 23.01.2025).

digital representations, or «digital doubles,» surpassing traditional forms of fraud or document forgery. Currently, Kazakhstan's criminal legislation lacks explicit provisions that establish criminal liability for producing and disseminating falsified digital images, audio, or videos, unless explicitly tied to fraud or extortion.

Globally, several jurisdictions have responded to the increasing threats posed by deepfake technologies by directly criminalizing the creation and dissemination of such content. These legislative actions reflect a growing awareness of deepfake-related risks to individual rights, public trust, and democratic processes.

In the United States, the DEEPFAKES Accountability Act established legal responsibility for distributing manipulated media without the consent of featured individuals. Moreover, multiple U.S. states introduced specific laws restricting deepfake use in political contexts, particularly during elections, aiming to protect voters from manipulation and misinformation. For example, Virginia amended its legislation to specifically criminalize the creation and distribution of pornographic deepfakes, addressing privacy violations and dignity infringements caused by synthetic explicit content [11, p. 371]. Similarly, Texas enacted provisions in 2019 prohibiting deepfake dissemination aimed at harming political candidates or altering electoral outcomes, with penalties including imprisonment and fines, reinforcing electoral authenticity and fairness [11, p. 374].

In 2023, the European Union implemented the Digital Services Act (DSA), requiring online platforms to effectively detect and label misleading deepfake content. The DSA differentiates between lawful harmful and illegal content, enhances digital literacy, promotes platform accountability through labeling and watermarking, and mitigates politically motivated synthetic media manipulation [12, p. 10].

China also introduced rigorous regulations through the «Provisions on the Administration of Deep Synthesis in Internet Information Services,» effective from January 2023. These provisions mandate clear labeling of synthetic media, impose transparency obligations on platforms, enhance data governance practices, and establish substantial financial and criminal penalties for non-compliance [13].

The international regulatory experience underscores the necessity for Kazakhstan to develop comprehensive legislative frameworks addressing ethical and legal complexities associated with synthetic media. By analyzing and incorporating global best practices, Kazakhstan can enhance its legal mechanisms for effectively preventing and prosecuting deepfake-related abuses.

Conclusion

The rapid advancement of artificial intelligence, particularly deepfake technologies, poses sophisticated challenges to information security and complicates cybercrime prevention. Initially designed for entertainment, deepfake technology has evolved into a potent instrument for crimes such as financial fraud, extortion, blackmail, and manipulation of public perception. These offenses have proliferated due to machine learning algorithms capable of generating hyper-realistic digital forgeries nearly in real-time. Current research identifies three primary categories of deepfake-related crime: financial deception, coercive blackmail, and political interference, each requiring targeted counterstrategies.

Kazakhstan's existing legislation lacks adequate frameworks to tackle deepfake-related offenses, highlighting significant regulatory gaps. The ambiguous nature of these crimes complicates their classification within existing Criminal Code provisions, potentially encompassing fraud, intentional dissemination of false information, extortion, and unauthorized use of personal data. The distinctive features of deepfake crimes, notably the fabrication of digital identities and entities, further challenge their precise legal categorization.

A key challenge in deepfake investigations lies in reliably verifying the authenticity of digital evidence. Despite significant technological improvements in forensic detection – such as analysis of facial micro-expressions, audio spectral features, and advanced digital forensic methods – the continuous evolution of deepfake techniques necessitates ongoing enhancement of detection strategies.

Considering the susceptibility of digital evidence to manipulation,

judicial procedures must develop robust verification methodologies. Kazakhstan would benefit significantly from examining and integrating best regulatory and forensic practices established internationally, especially those effectively implemented in jurisdictions such as the United States, China, and the European Union.

Effectively combating deepfake-related crimes requires an integrated approach across several interconnected areas: refining criminal legislation to address unique aspects of synthetic media; advancing specialized digital forensic methods; and establishing clear judicial standards for evaluating digital evidence. Moreover, promoting institutional cooperation among law enforcement agencies, scientific communities, and technology firms, as well as improving public awareness and digital literacy, are essential components of a comprehensive strategy.

Together, these measures will substantially enhance information security, strengthen legal protections, and ensure robust responses to emerging threats posed by synthetic media.

This research was funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP26103625 «Online fraud using deepfake-technologies and social engineering: problems of criminal law counteraction, prospects for legislative regulation»).

References:

1. Stupp, C. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case / C. Stupp // Retrieved from https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 (date of reference: 23.01.2024).
2. Brewster, T. Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find. / T. Brewster, // Retrieved from https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/ (date of reference: 23.01.2025).
3. Swenson, A. A parody ad shared by Elon Musk clones Kamala Harris' voice, raising concerns about AI in politics. / A. Swenson // Retrieved from https://apnews.com/article/parody-ad-ai-harris-musk-x-misleading-3a5df582f911a808d34f68b766aa3b8e (date of reference 30.01.2025).
4. Łabuz, M. On the way to deep fake democracy? Deep fakes in election campaigns in 2023 / M. Łabuz, C. Nehring // European Political Science. – 2024. – Volume 23. – P. 454-473.
5. Van der Sloot B. Deepfakes: regulatory challenges for the synthetic society / B. Van der Sloot, Y. Wagensveld // Computer Law & Security Review. – 2022. – Volume 46. – P. 1-15.
6. M.R. Sanil, Deepfake detection using eye-blinking pattern / M.R. Sanil, S. Saathvik, R. RaiK, P.M. Srinivas // International Journal of Engineering Applied Sciences and Technology. – 2022. – No3. – P. 229-234.
7. Pham, L. Deepfake Audio Detection Using Spectrogram-based Feature and Ensemble of Deep Learning Models / L. Pham, P. Lam, T. Nguyen, H. Nguyen, A. Schindler // 2024 IEEE 5th International Symposium on the Internet of Sounds (IS2). – 2024. – P. 1-4.
8. Ferrer, C.C. Deepfake Detection Challenge Results: An open initiative to advance AI / C.C. Ferrer, B. Dolhansky, B. Pflaum, J. Bitton, J. Pan, J. Lu // Retrieved from https://ai.meta.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/ (date of reference: 30.01.2025).
9. Seldon, M. Surge in Digital Injection and Deepfake Attacks on Identity Verification Systems / M. Seldon // Retrieved from https://www.hstoday.us/subject-matter-areas/cybersecurity/surge-in-digital-injection-and-deepfake-attacks-on-identity-verification-systems/ (date of reference: 01.03.2025).
10. Datta, S.K. Exposing Lip-syncing Deepfakes from Mouth Inconsistencies / S.K., Datta, S. Jia, S. Lyu // 2024 IEEE International Conference on Multimedia and Expo (ICME), Niagara Falls, ON, Canada. – 2024. – P. 1-6.

11. Lussier, N. Nonconsensual deepfakes: detecting and regulating this rising threat to privacy / N. Lussier // Idaho Law Review. – 2022. – Volume 58. – P. 353-383.
12. Khan, F. Does the Digital Services Act achieve a balance between regulating deepfakes and protecting the fundamental right to freedom of expression? / F. Khan // SSRN Electronic Journal. – 2024. – P. 1-15.
13. Interesse, G. China to Regulate Deep Synthesis (Deepfake) Technology Starting / G. Interesse // Retrieved from https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/ (date of reference: 18.02.2025).

© Н.М. Әпсімет[1], 2025
[1] әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы, Қазақстан
(E-mail: Apsimet.nurdaulet@gmail.com)

ИНТЕРНЕТТЕГІ АЛАЯҚТЫҚТА DEEPFAKE ҚОЛДАНАТЫН ҚЫЛМЫСТАР ЖӘНЕ ОЛАРДЫ ДӘЛЕЛДЕУ МӘСЕЛЕЛЕРІ

Аннотация. Бұл зерттеу интернеттегі алаяқтық саласындағы deepfake технологиясын қолдану арқылы жасалған қылмыстар мәселесін қарастырады. Жұмыстың мақсаты-deepfake-ті онлайн-алаяқтықта қолдану тетіктерін жан-жақты талдау, мұндай қылмыстарды тергеу және дәлелдеу процесінде бар проблемаларды анықтау, сондай-ақ оларды шешу бойынша ұсыныстарды тұжырымдау. Зерттеу әдістемесі ретінде deepfake танудың техникалық мүмкіндіктерін криминалистикалық талдау, deepfake-алаяқтықпен күресудің халықаралық тәжірибесін салыстырмалы талдау, тақырып бойынша ғылыми әдебиеттерді доктриналық зерттеу және Қазақстан Республикасының киберқылмыс саласындағы заңнамасын талдау пайдаланылды.

Зерттеу нәтижелері deepfake-ті қылмыстық пайдаланудың үш негізгі бағытын анықтады: қаржылық алаяқтық, бопсалау және саяси манипуляциялар. Deepfake-ті қаржы секторындағы жеке басын тексеру жүйелерін айналып өту, қаражатты ұрлау және жалған ақпарат тарату мақсатында жалған бейне және аудио материалдар жасау үшін пайдалану мысалдары талданды. Бұл қылмыстарды саралаудың қиындықтарына және мамандандырылған құқықтық нормалар мен әдістер болмаған жағдайда бұрмалау фактісін дәлелдеуге ерекше назар аударылады. Deepfake-ті анықтаудың заманауи техникалық құралдары, соның ішінде микромимика мен дыбыстың спектрлік сипаттамаларын талдау қарастырылған.

Зерттеу нәтижелерін қолдану саласы Қазақстан Республикасының қылмыстық заңнамасын жетілдіруді, deepfake-пен байланысты қылмыстарды анықтау мен тергеудің криминалистикалық әдістемелерін әзірлеуді, сондай-ақ мамандар мен жұртшылықтың осы қауіп туралы хабардарлығын арттыруды қамтиды.

Зерттеудің қорытындылары deepfake технологиясының дамуы ақпараттық қауіпсіздік пен құқықтық тәртіпке үлкен қауіп төндіреді, бұл онлайн алаяқтықтың жаңа түрлерін жасайды және оларды тергеу мен қудалау процесін қиындатады. Заңнаманы бейімдеу, deepfake анықтау мен сараптаманың мамандандырылған әдістерін дамыту, сондай-ақ қылмыстың осы түріне қарсы күресте халықаралық ынтымақтастық қажеттілігі атап өтілді.

Түйінді сөздер: deepfake, фейковизация, онлайн алаяқтық, киберқылмыс, дәлелдеу, криминалистикалық талдау.

© Н.М. Апсимет[1] , 2025
[1] Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
(E-mail: Apsimet.nurdaulet@gmail.com)

ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ DEEPFAKE В ОНЛАЙН-МОШЕННИЧЕСТВЕ И ПРОБЛЕМЫ ИХ ДОКАЗЫВАНИЯ

Аннотация. Настоящее исследование посвящено проблеме преступлений, совершаемых с использованием технологии deepfake в сфере онлайн-мошенничества. Целью работы является всесторонний анализ механизмов применения deepfake в онлайн-мошенничестве, выявление существующих проблем в процессе расследования и доказывания таких преступлений, а также формулирование предложений по их решению. В качестве методологии исследования использовались криминалистический анализ технических возможностей распознавания deepfake, сравнительный анализ международного опыта борьбы с deepfake-мошенничеством, доктринальное исследование научной литературы по теме и анализ законодательства Республики Казахстан в области киберпреступности.

Результаты исследования выявили три ключевые области криминального использования deepfake: финансовое мошенничество, шантаж и вымогательство, а также политические манипуляции. Проанализированы примеры использования deepfake для обхода систем верификации личности в финансовом секторе, создания поддельных видео- и аудиоматериалов с целью хищения средств и распространения дезинформации. Особое внимание уделено трудностям квалификации данных преступлений и доказывания факта фальсификации в условиях отсутствия специализированных правовых норм и методов. Рассмотрены современные технические средства обнаружения deepfake, включая анализ микромимики и спектральных характеристик звука.

Область применения результатов исследования включает совершенствование уголовного законодательства Республики Казахстан, разработку криминалистических методик выявления и расследования преступлений, связанных с deepfake, а также повышение осведомленности специалистов и общественности о данной угрозе.

Выводы исследования заключаются в том, что развитие технологии deepfake представляет серьезную угрозу для информационной безопасности и правопорядка, создавая новые формы онлайн-мошенничества и затрудняя процесс их расследования и судебного преследования. Подчеркивается необходимость адаптации законодательства, развития специализированных методов обнаружения и экспертизы deepfake, а также международного сотрудничества в борьбе с данным видом преступлений.

Ключевые слова: deepfake, фейковизация, онлайн-мошенничество, кибер-преступность, доказывание, криминалистический анализ.

Автор туралы мәліметтер:
Сведения об авторе:
Information about author:

Әпсімет Нұрдәулет Мұхамедияръұлы - хат-хабарларға арналған автор, **з**аң ғылымдарының магистрі, әл-Фараби атындағы Қазақ ұлттық университеті заң факультетінің докторанты, әл-Фараби даңғылы, 71, 050040, Алматы, Қазақстан.
E-mail: Apsimet.nurdaulet@gmail.com; ORCID: https://orcid.org/0000-0002-5127-5579.

Апсимет Нурдаулет Мухамедиярулы - автор для корреспонденции, **м**агистр юридических наук, докторант юридического факультета Казахского национального университета имени аль-Фараби, проспект Аль-Фараби, 71, 050040, Алматы, Казахстан.

E- mail: Apsimet.nurdaulet@gmail.com; ORCID: https://orcid.org/0000-0002-5127-5579.

Apsimet Nurdaulet Mukhamediyaruly - corresponding authors, **м**aster of Law, Doctoral student of the Faculty of Law, Al-Farabi Kazakh National University, 71 Al-Farabi Avenue, 050040, Almaty, Kazakhstan.

E-mail: Apsimet.nurdaulet@gmail.com; ORCID: https://orcid.org/0000-0002-5127-5579.