https://doi.org/10.31489/2026L2/147-157
UDC 34.03 Received: 02.02.2026| Accepted:03.04.2026 | Published online: 30.06.2026

A.B. Saktaganova[1*], I.S. Saktaganova[2]

[1,2] *L.N. Gumilyov Eurasian National University, Astana, Kazakhstan*
(E-mail: aridnissakta.11@gmail.com, aridnis@mail.ru)
[1]*ORCID ID: https://orcid.org/0009-0008-0457-7794, Scopus Author ID: 58650812400*
[2]*ORCID ID: https://orcid.org/0000-0001-7218-197X, Scopus Author ID: 57202532606*
[2]*Researcher ID WOS: AAR-4135-2020*

Legal regulation and liability for online fraud based on the use of deepfake technologies and social engineering: foreign experience and directions for its adoption

In the context of the rapid development of digital technologies, online fraud based on the use of deepfake technologies and social engineering methods poses a significant threat to public safety. The aim of this study is to analyse the legal regulation and liability measures for such crimes in foreign countries, as well as to identify areas where positive international experience can be used to improve national legislation. The study employs general scientific and special methods of cognition, including analysis, synthesis, induction and deduction, as well as formal-legal, comparative-legal and systemic-structural methods. The work examines normative legal acts, judicial practice and doctrinal approaches in a number of foreign countries, including the European Union, the United States and Asian countries, regulating liability for digital forms of fraud. As a result, the main models of legal response to crimes involving deepfakes and social engineering were identified, and their strengths and weaknesses were established. The study concludes that a comprehensive approach to legal regulation is necessary, including clarifying the elements of offences, strengthening preventive measures, and developing international cooperation. The results obtained can be used to formulate proposals for improving criminal and information legislation.

Keywords: Deepfake, online fraud, cybercrime, digital security, social engineering, legislation, legal policy, legal analysis.

Introduction

The rapid development of digital technologies, artificial intelligence and global communication networks has led not only to expanded opportunities for socio-economic development, but also to the emergence of new forms of criminal activity. In this context, online fraud based on the use of deepfake technologies and social engineering methods, which allow attackers to imitate the appearance, voice and behaviour of real people and effectively manipulate the minds of users, poses a particular danger.

The relevance of researching this problem is due to the growing number of crimes committed using digital identity imitation, their high latency, cross-border nature, and the significant damage caused to both individual citizens and state and corporate structures. Despite the active development of legislation in the field of digital security, legal regulation of liability for online fraud using deepfakes and social engineering remains fragmented in many countries. In law enforcement practice, difficulties arise with the classification of such acts, the distinction between related offences, as well as with proving guilt and establishing the subjective side of the crime. This necessitates a comprehensive scientific analysis of foreign experience and the development of ways to borrow from it in order to improve national legal mechanisms for combating digital forms of fraud.

In recent years, the relevance of the issue under study has been confirmed by statistical data from international organisations and analytical centres. According to the US Federal Bureau of Investigation (FBI, Internet Crime Complaint Centre), the total damage from cybercrime in 2023 amounted to more than $12.5 billion, which is the highest figure for the entire observation period [1]. The largest share was accounted for by fraudulent schemes based on social engineering methods, including impersonation attacks and voice phishing, which actively use synthetic voice and image generation technologies.

According to Europol's Internet Organised Crime Threat Assessment (IOCTA, 2023) report, the use of artificial intelligence and deepfake technologies is considered one of the key factors in the transformation of cybercrime in Europe [2]. The document notes an increase in the number of cases of synthetic audio and video materials being used to impersonate individuals in financial crimes and corporate fraud.

* Corresponding author. E-mail: *aridnissakta.11@gmail.com*

An analytical study by Sumsub (2023) shows that the number of fraudulent transactions using deepfakes increased by more than 700 % between 2022 and 2023, with financial technology, cryptocurrency platforms and online banking being the most vulnerable sectors. In turn, a study by McAfee (2023) found that about 25 % of adult users in the US and Europe have encountered fraud attempts using synthetic voices, with attackers achieving partial success in 77 % of cases [3].

Kazakhstan has also seen steady growth in internet fraud. According to official data from the Ministry of Internal Affairs of the Republic of Kazakhstan, 43,900 cases of fraud were reported in 2024. Half of these were cybercrimes. Older people are often the victims of fraudsters' tricks. Last year, 4,785 cases of fraud against citizens over the age of 60 were recorded. The amounts of damage ranged from several thousand to tens of millions of tenge. The highest number of cases of Internet fraud last year was recorded in Astana (4,582 cases), Almaty (2,275) and the Karaganda region (1,906) [4]. Experts note a gradual increase in the proportion of schemes involving the use of social engineering and artificial intelligence technologies.

Thus, international statistics confirm the scale and transnational nature of online fraud based on the use of deepfakes and social engineering, which necessitates the improvement of legal mechanisms to combat these crimes.

In this regard, the purpose of this study is to analyse the legal regulation and legal liability for online fraud based on the use of deepfake technologies and social engineering methods in foreign countries, as well as to justify the directions for borrowing the most effective legal solutions. To achieve this goal, the study sets the following objectives: to reveal the essence and main forms of online fraud using deepfake and social engineering; to analyse the regulatory and legal approaches of foreign states to criminal and administrative liability for these acts; to identify the features of law enforcement practice; to determine the problematic aspects and contradictions of the existing legal regulation; to formulate proposals for borrowing and adapting foreign experience [5; 201].

Scientific literature reveals significant contradictions in approaches to the legal assessment of deepfake technologies. Some researchers view them exclusively as a tool for committing traditional crimes that does not require separate legal regulation, while others justify the need to establish special criminal offences and new institutions of liability. Similar discrepancies can be observed in methodological approaches: from narrowly focused criminal law analysis to interdisciplinary studies combining law, cybersecurity, and the psychology of influence. In practice, these contradictions manifest themselves in inconsistent court decisions and the absence of uniform standards of proof.

A significant gap in contemporary research is the insufficient systematisation of foreign experience specifically in the context of the combined use of deepfake technology and social engineering. Most scientific works focus either on the problems of digital forgeries or on the socio-psychological mechanisms of fraud, without revealing their interconnection. The authors of this study proceed from the position that effective legal regulation is only possible with a comprehensive approach that takes into account both the technological and behavioural nature of online fraud. An analysis of foreign doctrine and legislation leads to the conclusion that it is advisable to borrow flexible and preventively oriented models of legal response, adapted to national legal systems.

Methods and materials

The methodological basis of this study was a set of general scientific, specialised and interdisciplinary methods of cognition, the application of which is determined by the multifaceted nature of online fraud based on the use of deepfake technologies and social engineering methods. The choice of methods was focused on achieving the research goal—identifying the features of legal regulation and liability for these types of crimes in foreign countries, as well as justifying the directions for borrowing relevant experience for the national legal system.

The article used analysis and synthesis as basic general scientific methods, which made it possible to structure the array of scientific information, identify key elements of legal regulation, and reveal the interrelationships between the technological and legal aspects of online fraud. The inductive method was used to summarise individual law enforcement decisions and regulatory provisions of foreign countries in order to identify common patterns in the regulation of liability for crimes involving deepfakes and social engineering. The deductive method was used to verify general theoretical conclusions using specific examples from legislation and judicial practice.

The formal legal method was of particular importance in the study, through which the norms of criminal, administrative and information legislation of foreign states were analysed. It was used to examine

the elements of crimes, forms of guilt, types and limits of legal liability, as well as the specifics of the legal classification of online fraud committed using digital forgeries and manipulative technologies. Formal legal analysis made it possible to identify the specifics of the legislative techniques used to establish liability for new forms of digital crime [6; 216].

The comparative legal method became a key research tool. It was used to compare approaches to the legal regulation of online fraud in various legal systems, including the European Union, the United States, the United Kingdom, Japan, and the Republic of Korea. The comparative analysis examined both universal models of criminal liability and specialised norms aimed at countering the use of artificial intelligence and social engineering for criminal purposes. This made it possible to identify general trends in the development of foreign legislation, as well as national characteristics of the legal response to the threats of digital fraud.

A systemic-structural method was used to study the institutional and functional links between legal norms. It allowed us to consider the legal regulation of online fraud as a holistic system comprising criminal law, procedural, administrative and preventive elements. The use of this method helped to identify the role of law enforcement agencies, courts and specialised regulators in ensuring accountability for crimes involving deepfakes and social engineering.

Given the cross-border nature of the crimes under investigation, a functional method was also used in the study to analyse the effectiveness of legal norms in the context of digital globalisation. This method made it possible to assess the extent to which the existing legal mechanisms of foreign states are capable of responding to online fraud committed using foreign platforms, anonymous networks and distributed digital technologies.

The material basis of the study consisted of various sources selected for their relevance, reliability, and scientific significance. The main materials used were normative legal acts of foreign states, including criminal codes, special laws in the field of cybersecurity, personal data protection, and artificial intelligence regulation. Both the current versions of legislative acts and draft regulatory documents under discussion or implementation were analysed.

Court decisions and law enforcement practices in foreign countries occupy a significant place among the research materials. In particular, precedents related to prosecution for fraud, forgery, illegal use of personal data, and other crimes committed using deepfake technology and social engineering were analysed. Judicial practice was considered as a source for identifying problems of qualification, evidence and sentencing, as well as an indicator of the effectiveness of legal regulation.

Additional material was provided by official reports from international organisations and specialised agencies dealing with cybercrime and digital security issues. The study used analytical reports, statistical reviews and methodological recommendations reflecting the scale of online fraud and the main directions of countering it at the international level. These materials made it possible to substantiate the relevance of the topic and compare legal approaches with actual trends in the development of crime.

The article also draws on the findings of scientific research by foreign and domestic authors on the legal regulation of digital crimes, artificial intelligence, social engineering, and liability for fraud. The analysis of scientific literature was carried out using bibliometric and problem-thematic approaches, which made it possible to identify the main theoretical schools, controversial issues, and insufficiently researched aspects of the subject matter [7; 360].

Particular attention was paid to interdisciplinary materials, including works in the fields of information technology, cyberpsychology, and digital forensics. Their use made it possible to reveal in greater depth the technical and behavioural mechanisms of online fraud, which, in turn, provided a more informed legal analysis and a correct comparison of foreign experience.

Thus, the combination of methods and materials used ensured a comprehensive and systematic nature of the research, allowing not only to analyse foreign models of legal regulation of liability for online fraud based on the use of deepfake technologies and social engineering, but also to form scientifically sound conclusions and proposals for borrowing and adapting this experience.

Results

The study yielded results that provide a comprehensive assessment of the state of legal regulation and liability for online fraud based on deepfake technologies and social engineering methods in foreign countries, as well as identify areas for adopting the most effective legal solutions. The findings are based on an analysis of regulatory legal acts, judicial practice, and doctrinal sources, ensuring their validity and compliance with the study’s objectives.

The first significant result of the study was the identification of a persistent trend toward a broad interpretation of traditional fraud offences in foreign legal systems. An analysis of the legislation of the United States, the European Union, the United Kingdom, and Japan revealed that, in most cases, deepfake technologies are not recognized as an independent object of criminal regulation, but are considered a method or means of committing a crime. Judicial practice confirms that the use of counterfeit audio and video materials is classified in conjunction with fraud, illegal use of personal data, forgery, or interference with information systems. This observation demonstrates the pragmatic approach of legislators, focused on the flexibility of legal responses. The second result was the identification of differences in criminal liability models for online fraud involving social engineering. In a number of countries (the United States, Canada, and Australia), emphasis is placed on the subjective aspect of the crime, specifically the intent to mislead the victim through psychological influence. In countries with continental legal systems (Germany, France, and Spain), greater weight is placed on the objective aspect of the act and the fact of causing property damage. The author found that it is the combination of technological influence (deepfake) and behavioral manipulation (social engineering) that creates the greatest difficulties for law enforcement, as it requires proof of both the technical forgery and the psychological influence.

The third result of the study was the identification of fragmented legal regulation of deepfake technologies. It was found that even in countries with developed digital legislation, universal and uniform definitions of deepfake at the criminal law level are lacking. Typically, such technologies are mentioned in strategic documents, soft law acts, or special laws on artificial intelligence. This leads to the classification of crimes based on analogous legal structures, increasing the risk of ambiguous interpretation of norms and differences in judicial practice [8].

These findings are supported by international empirical studies demonstrating a steady increase in crimes using artificial intelligence technologies. Deloitte predicts that the use of generative AI could lead to fraud losses in the US reaching $40 billion by 2027, compared to $12.3 billion in 2023, demonstrating the scale of the threat and the need to adapt legal mechanisms to digital realities [9]. An analysis of international judicial practice shows that the most common cases involve the use of deepfake to impersonate company executives for the purpose of illegally transferring funds, as well as to defraud individuals through social media and instant messaging apps.

The study systematized international approaches reflecting the main models of legal regulation of liability for online fraud using deepfakes and social engineering (universal model, specialized model, and mixed model). The analysis revealed that the most widespread is the mixed model, which combines the application of general criminal law provisions with specific provisions aimed at protecting digital rights and personal data.

A significant finding was the identification of the development of preventive legal regulation mechanisms. In a number of foreign countries, criminal law measures are complemented by administrative and regulatory instruments aimed at preventing online fraud. These include the obligation of digital platforms to label synthetic content, the expansion of telecom operators' responsibilities to identify fraudulent schemes, and the introduction of digital identification standards. The author found that such measures significantly reduce the burden on criminal justice and increase the effectiveness of protecting potential victims.

A separate result of the study was a summary of the challenges in law enforcement practice related to proving crimes based on the use of deepfakes. Foreign court records point to a lack of specialized expertise, the difficulty of identifying the source of digital counterfeits, and the challenges of collecting cross-border evidence. These observations confirm the need for institutional development of digital forensics and specialized training for judges and investigative bodies.

Based on the analysis of the obtained data, the authors developed a concept for a comprehensive legal response to online fraud based on deepfakes and social engineering. This concept envisions the simultaneous development of criminal, procedural, and preventive mechanisms. Specifically, it proposes considering deepfakes not as an independent criminal offense, but as a qualifying feature or aggravating circumstance in the commission of fraud if their use significantly increases the social danger of the act.

The novelty of the obtained results lies in the systemic integration of the technological and behavioral aspects of online fraud within the framework of legal analysis. Unlike existing studies, which examine deepfakes and social engineering in isolation, the authors demonstrate that their combined use creates a qualitatively new level of criminal impact. This requires a revision of traditional approaches to classification and liability, which has so far been insufficiently addressed in the scientific literature.

Furthermore, the novelty of the study lies in the proposal to use a multi-level model for borrowing international experience, reflecting three levels: normative (changes in criminal and information legislation), institutional (development of specialized bodies and expert structures), and preventive (improving digital literacy and regulating platforms). This model is practical in nature and can be used in developing national programs to combat online fraud.

The results obtained are fully consistent with the stated goals and objectives of the article. The analysis allowed us to uncover the nature and forms of online fraud using deepfake and social engineering, identify the specifics of international legal regulation, identify problem areas, and suggest areas for adopting effective legal solutions. The practical significance of the results lies in their potential use in improving criminal and information legislation, as well as in the activities of law enforcement agencies.

Thus, the results of the study confirm the need for a comprehensive and adaptive approach to the legal regulation of online fraud in the context of digitalization and demonstrate that international experience can serve as an effective basis for developing modern legal liability mechanisms, provided it is systematically and critically adopted [10].

The recently adopted Law of the Republic of Kazakhstan "On Artificial Intelligence" (hereinafter referred to as the AI Law) establishes a fundamental legal framework for the control, development, and regulation of the use of artificial intelligence (AI) in the country. The Law defines key concepts such as artificial intelligence, data libraries, and synthetic AI outputs—which include audio, video, images, and text created or modified using AI and establishes principles of security, transparency, and accountability in the use of AI technologies.

Of particular importance for regulating online fraud is the prohibition on the creation and operation of AI systems capable of manipulating consciousness, distorting reality, or harming the rights and interests of citizens. The Law explicitly prohibits the use of AI for subconscious or manipulative influence on behavior, exploitation of vulnerabilities, or social evaluation of individuals without their consent, and also introduces the obligation to label content created with the participation of AI [11].

It is important to note that the AI Law does not provide for direct criminal liability for the creation of deepfakes or the use of social engineering as such. Instead, it establishes a regulatory framework for the application of appropriate administrative penalties and prepares the legal basis for incorporating such acts into other legal mechanisms. At the same time, the introduction of bans on manipulative technologies and mandatory labeling reduces the risk of spreading fraudulent messages using deepfake and minimizes the possibility of misleading users.

Considering international practices (for example, mandatory labeling of synthetic content in the European Union), the provisions of the AI Law are timely and important for preventing harm from technological disinformation. However, this law is primarily regulatory and administrative in nature, while criminal liability for online fraud is traditionally enshrined in other regulations. Traditional criminal defense against fraud in Kazakhstan is based on Article 190 of the Criminal Code of the Republic of Kazakhstan, "Fraud", which stipulates that an act aimed at theft of property or the acquisition of rights to another's property through deception or abuse of trust entails criminal liability, including large fines, imprisonment, and other sanctions.

With the development of the internet and digital communications, the Criminal Code of the Republic of Kazakhstan has expanded the list of qualifying elements of fraud to include internet fraud in accordance with paragraph 4, part 2, Article 190 of the Criminal Code of the Republic of Kazakhstan. An analysis of judicial practice shows that online fraud is classified in the context of electronic funds transfers, theft through remote services, and abuse of trust through digital communications, with penalties of up to 4 years' imprisonment or more in the presence of aggravating circumstances. An important development in criminal law was the introduction of Article 232-1 of the Criminal Code of the Republic of Kazakhstan on liability for dropshipping, which provides for criminal liability of up to 7 years' imprisonment with confiscation of property for participation in online fraud schemes (e.g., sharing access to other people's bank accounts or making illegal payments).

Currently, the Criminal Code of the Republic of Kazakhstan does not provide for direct criminal liability for the creation or distribution of deepfakes as a separate offense. However, such actions may be classified in conjunction with fraud, document forgery, use of personal data, or other offenses covered by the Criminal Code (in particular, the chapters on crimes in the field of information technology). This approach is consistent with international practice, where deepfakes are more often considered a means of committing a crime rather than an independent object of criminalization. Thus, criminal law provides tools for prosecuting

actions indirectly related to the use of deepfake or social engineering in the commission of crimes, but does not always contain special means of responding to new technologies as an independent phenomenon [12].

Civil liability in Kazakhstan is based on the principles of compensation for damages and protection of the property rights of parties to legal relations. The Civil Code regulates compensation for losses caused by illegal actions, including moral damages and property losses, for example, if deepfake content or a fraudulent scheme resulted in property losses.

In cases of online fraud, the injured party has the right to file civil claims for damages against those who caused the harm, including demands for restoration of violated rights, compensation for material damages, and recovery of penalties stipulated by contractual agreements. Furthermore, the Civil Code complements criminal law measures by providing victims with the opportunity to seek compensation outside of criminal proceedings, which is particularly important for victim-focused law enforcement practices in the context of digital crimes [13].

The Code of Administrative Offenses contains general principles and sanctions for illegal actions, including violations related to non-compliance with artificial intelligence legislation. With the introduction of the Law on AI, provisions were added to administrative legislation regarding violations of mandatory labeling of content created using AI, as well as violations in the management of high-risk AI systems that cause harm to citizens, which entails the imposition of fines equal to the monthly calculation index (MCI).

Administrative measures are characterized by the fact that they can be applied even in the absence of a criminal offense, making them an important tool for ensuring compliance with technological requirements of the law. Such measures may also include fines for consumer fraud and other violations stipulated by sections of the legislation on advertising and information technology [14].

The legal system of the Republic of Kazakhstan in the area of online fraud, deepfake content, and social engineering is a combination of criminal, administrative, and civil law mechanisms. The Law on Artificial Intelligence for the first time introduces direct prohibitions on dangerous AI practices and establishes a duty of transparency regarding synthetic content, thereby creating a foundation for preventing the abuse of deepfake content. The Criminal Code and other codes provide for criminal, civil, and administrative liability for the consequences of criminal acts, but do not always contain direct provisions specifically aimed at countering technological threats. This creates both modern protection mechanisms and potential for further legislative development. In the future, it may be necessary to clarify the provisions of the Criminal Code and the Code of Administrative Offenses of the Republic of Kazakhstan to individualize liability for the unlawful use of artificial intelligence tools in digital crimes.

Discussion

The results obtained in the course of the study generally correlate with the conclusions of a number of foreign and domestic scientific works devoted to the problems of digital crime and the legal regulation of online fraud. At the same time, the analysis revealed both significant points of contact with existing concepts and a number of discrepancies that require further theoretical consideration. This necessitates a critical comparison of the data obtained with previously published studies and an assessment of their scientific validity.

The prevailing view in scientific literature is that deepfake technologies are primarily seen as a tool for committing already known crimes, primarily fraud, defamation and illegal use of personal data. The author partially agrees with this position, as the results of the study confirmed that in most foreign legal systems, deepfakes do not constitute an independent offence, but are a means of committing one. This approach is reflected in the works of American and European researchers analysing judicial practice in cases related to digital forgeries. At the same time, the authors do not share the categorical conclusions of those scholars who deny the need for any special legal regulation of deepfakes, since their combination with social engineering methods significantly increases the public danger of such acts [15].

The results of this study largely coincide with the conclusions of authors who emphasise the complexity of proving crimes committed using artificial intelligence. Foreign studies point to a lack of technical expertise and insufficient training of law enforcement officers, which is confirmed by an analysis of judicial practice.

The results obtained are consistent with the conclusions of foreign researchers who consider deepfakes to be a qualitatively new form of digital threat. For example, Chesney and Citron (2019) note that synthetic media has a high degree of plausibility and can significantly undermine trust in digital information, creating new risks for law and order [16; 1787]. The works of Westerlund (2019) [17; 78] and

Kietzmann et al. (2020) emphasise that the spread of deepfakes is associated not only with fraud but also with disinformation, which increases their public danger.

A comparative analysis shows that countries with developed digital infrastructure demonstrate a higher level of detection of such crimes, which is associated with the effectiveness of monitoring and law enforcement. At the same time, in countries with less developed digital control systems, the latency of these crimes remains high, confirming the need for further research and improvement of mechanisms for their detection.

However, unlike a number of works that offer mainly technological solutions to this problem, the author proceeds from the need for a comprehensive legal approach that includes not only the development of digital forensics, but also the improvement of procedural mechanisms of evidence.

Significant discrepancies were identified when comparing the results obtained with studies in which social engineering is considered exclusively as a psychological phenomenon that falls outside the scope of legal analysis. The author disagrees with this position, as the results of the study showed that in foreign law enforcement practice, social engineering methods are increasingly taken into account when classifying crimes and determining the degree of guilt. This allows social engineering to be considered not only as an auxiliary element, but also as a significant factor in the formation of the subjective side of a crime.

An analysis of similarities and differences also revealed methodological discrepancies in the assessment of preventive measures. A number of foreign authors are critical of expanding the responsibilities of digital platforms, pointing to the risk of excessive interference with freedom of information. The results obtained in this study allow us to agree with these concerns only partially. On the one hand, excessive regulation can indeed lead to restrictions on users' rights. On the other hand, foreign experience shows that the introduction of obligations to label synthetic content and identify fraudulent schemes contributes to a reduction in the number of crimes—not by replacing criminal law measures, but by supplementing them.

The results obtained can be explained from the perspective of the concept of comprehensive digital criminalisation, according to which legal regulation should take into account not only the legal form of the act, but also its technological and behavioural nature. It is from this scientific perspective that it becomes clear why isolated regulation of deepfakes or social engineering is not effective enough. Their combined use forms a new type of criminal behaviour that goes beyond traditional models of fraud.

Summarising the results of the study, it can be argued that the identified foreign models of legal regulation demonstrate a tendency towards the functional adaptation of criminal law to digital challenges. Instead of creating an excessive number of special offences, legislators seek to make flexible use of existing legal constructs, supplementing them with qualifying characteristics and preventive mechanisms. This conclusion generally coincides with the results of a number of comparative legal studies, but in this work it is supplemented by an analysis of social engineering as an independent criminologically significant factor.

The assessment of the reliability of the results obtained is based on the breadth and representativeness of the empirical base used. Analysis of normative acts and judicial practice in several legal systems has minimised the risk of one-sided conclusions. At the same time, the authors are aware of certain limitations of the study related to differences in the availability of judicial materials and the heterogeneity of statistical data on digital crimes. However, these limitations do not diminish the overall scientific significance of the results, but only indicate directions for further research [18; 5].

Overall, the discussion allows us to conclude that the results obtained not only confirm certain provisions of existing theories, but also contribute to the development of scientific understanding of the legal regulation of online fraud in the context of digitalisation. The authors' position is that effective legal liability for crimes based on the use of deepfakes and social engineering is only possible if their complex nature is recognised and an interdisciplinary approach is applied. This, in turn, forms the theoretical basis for further improvement of legislation and law enforcement practice.

Conclusions

The study of legal regulation and liability for online fraud based on the use of deepfake technologies and social engineering methods has provided a comprehensive overview of current international approaches to combating these forms of digital crime and identified areas where the most effective legal solutions can be adopted. In the course of the work, theoretical provisions, the results of comparative legal analysis and conclusions obtained in the discussion process were systematised, which ensured the achievement of the research goals and objectives.

First of all, it was established that in most foreign countries, online fraud using deepfakes and social engineering is not considered a fundamentally new type of crime, but rather a transformation of traditional fraudulent schemes using modern digital technologies. Legislators and law enforcement agencies tend to adapt existing criminal law constructs, classifying these acts under general provisions on fraud, forgery, illegal use of personal data, and interference with information systems. This approach demonstrates a desire to maintain the consistency of criminal law and avoid excessive fragmentation of criminal offences.

At the same time, the results of the study showed that the combined use of deepfake technologies and social engineering methods significantly increases the level of public danger posed by online fraud. This is due not only to the technical complexity of detecting and proving such acts, but also to the heightened psychological impact on victims. In this regard, foreign practice increasingly uses qualifying characteristics, aggravating circumstances, and special procedural mechanisms aimed at an adequate criminal law assessment of such crimes. This conclusion confirms the need for a comprehensive approach to liability for digital forms of fraud.

Systematisation of the results has revealed three main models of legal regulation of liability for online fraud: universal, specialised and mixed. The mixed model, which combines the application of general criminal law norms with elements of special regulation in the field of digital technologies and artificial intelligence, is recognised as the most effective. It is this model that provides a balance between legal certainty, flexibility in law enforcement and the ability to respond quickly to technological changes.

The scientific value of the study lies in substantiating the need to consider deepfakes and social engineering not in isolation, but in their functional interrelationship. The author proves that it is their combined use that forms a qualitatively new type of criminal behaviour, requiring a review of traditional approaches to classification and liability. This position expands existing theoretical ideas about digital crime and contributes to the development of the concept of comprehensive legal regulation in the context of digitalisation.

The practical significance of the research results is expressed in the possibility of their use in improving criminal, information and procedural legislation. The conclusions and generalisations obtained on the basis of an analysis of foreign experience can serve as a guideline for the development of norms establishing liability for fraud involving the use of digital forgeries and manipulative technologies. Of particular value are proposals on the use of qualifying characteristics related to the use of artificial intelligence and social engineering, as well as on the development of preventive mechanisms for legal regulation.

The results of the study can also be used in law enforcement. In particular, they are of interest to judges, investigators and law enforcement officials when classifying online fraud and assessing evidence in cases involving the use of deepfakes. The systematisation of foreign judicial practice allows for the identification of typical mistakes and effective approaches that can be adapted to the specifics of the national legal system.

In addition, the conclusions drawn are relevant for educational and scientific activities. The research materials can be used in courses on criminal law, information law, cybersecurity, and digital criminology, as well as in the preparation of scientific and qualification works. The scientific generalisations made in the article provide a basis for further research in the field of legal regulation of crimes committed with the use of artificial intelligence.

Possible areas of application for the research results also include the activities of government agencies and specialised regulators responsible for digital security and the protection of citizens' rights in the information sphere. The concept of a multi-level legal response developed by the author can be used in the formation of national strategies to combat cybercrime, as well as in the development of international cooperation programmes in the field of combating online fraud.

Overall, the study confirms that effective legal regulation and legal liability for online fraud based on the use of deepfakes and social engineering are only possible if foreign experience is systematically borrowed and adapted, taking into account national legal traditions. The conclusions drawn not only summarise existing practice, but also form a scientifically sound basis for the further development of legislation and law enforcement in the context of the rapid digital transformation of society.

Acknowledgements

This research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (program no. AR26103625) on the topic: "Online fraud using deepfake technologies and social engineering: problems of criminal law counteraction, prospects for legislative regulation"

References

1 Protecting Our Digitally-connected World is a Top Priority and Focus of the FBI. — [Electronic resource]. — Access mode: https://www.ic3.gov/

2 Beware: scams involving fake correspondence from Europol. — [Electronic resource]. — Access mode: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/beware-scams-involving-fake-correspondence-europol

3 Your personal info, finances, and digital life-secured with McAfee+. — [Electronic resource]. — Access mode: https://www.mcafee.com/

4 Cybercrime statistics for Kazakhstan. — [Electronic resource]. — Access mode: https://special.zakon.kz/cyber_fraud

5 Smanova A.B. Deepfake technologies and social engineering in online fraud forms, mechanisms, and legal challenges / A.B. Smanova, A.Zh. Muratova, S.R. Zhumagulova // Bulletin of L.N. Gumilyov Eurasian National University. Law Series. — 2025. — No. 3. — P. 188–211.

6 Beaver K. International and domestic legal frameworks on online fraud and deepfake technologies: a comparative criminal law analysis / K. Beaver // Bulletin of L.N. Gumilyov Eurasian National University. Law Series. — 2025. — Vol. 152, No. 3. — P. 212–228.

7 Apsimet N.M. Crimes involving deepfake in online fraud and the challenges of proving them / N.M. Apsimet // Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan. — 2025. — No. 3 (80). — С. 357–368.

8 Nowak A. Legal Challenges of Deepfakes: Liability, Harm, and Regulatory Responses [Electronic resource] / A. Nowak, B. Tóth, A. Ionescu // Legal Studies in Digital Age. — 2025. — Access mode: https://jlsda.com/index.php/lsda/article/view/306

9 Deloitte 2024 Financial Services Industry Predictions: AI Expected to Transform Retail Investing, Increase Banking Fraud and Drive New Insurance Market; Climate Change Expected to Further Increase Insurance Costs for Commercial Real Estate. — [Electronic resource]. — Access mode: https://www.deloitte.com/us/en/about/press-room/deloitte-2024-fsi-predictions.html

10 Davey O.M. Deepfake in Online Fraud Cases: The Haze of Artificial Intelligence's Accountability Based on the International Law [Electronic resource] / O.M. Davey, L. Sauerwein // Sriwijaya Crimen and Legal Studies. — 2025. — Access mode: https://journal.fh.unsri.ac.id/index.php/SCLS/article/view/2654

11 Об искусственном интеллекте. Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/Z2500000230

12 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V. — [Электронный ресурс]. — Режим доступа: https://online.zakon.kz/Document/?doc_id=31575252

13 Гражданский кодекс Республики Казахстан (особенная часть). Кодекс Республики Казахстан от 1 июля 1999 года № 409. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/K990000409_

14 Об административных правонарушениях. Кодекс Республики Казахстан от 5 июля 2014 года № 235-V ЗРК. — [Электронный ресурс]. — Режим доступа: https://adilet.zan.kz/rus/docs/K1400000235

15 Romero-Moreno F. Deepfake detection in generative AI: a legal framework proposal to protect human rights [Electronic resource] / F. Romero-Moreno // Computer Law & Security Review. — Access mode: https://www.sciencedirect.com/science/article/pii/S2212473X25000355

16 Chesney R. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security / R. Chesney, D. Citron // California Law Review. — 2019. — Vol. 107. — P. 1753–1819. https://doi.org/10.2139/ssrn.3213954

17 Westerlund M. The Emergence of Deepfake Technology: A Review / M. Westerlund // Technology Innovation Management Review. — 2019. — Vol. 9. — P. 40–53. https://doi.org/10.22215/timreview/1282

18 Lumen C. Deepfakes and the Limits of Law: a comparative analysis of regulatory frameworks in the U.S., EU, and China / C. Lumen // Journal of Advanced Artificial Intelligence. — 2025. — Vol. 2, No. 3. — P. 1–7.

А.Б. Сактаганова, И.С. Сактаганова

Deepfake және әлеуметтік инженерияны қолдануға негізделген онлайн алаяқтық үшін құқықтық реттеу және жауапкершілік: шет мемлекеттердің тәжірибесі және оның қолданылуы

Цифрлық технологиялардың қарқынды дамуы жағдайында deepfake технологиялары мен әлеуметтік инженерия әдістерін қолдануға негізделген онлайн-алаяқтық қоғамдық қауіпсіздікке ерекше қауіп төндіреді. Зерттеудің мақсаты шет мемлекеттердегі қылмыстардың көрсетілген түрлері үшін құқықтық реттеу мен құқықтық жауапкершілік шараларын талдау, сондай-ақ ұлттық заңнаманы жетілдіру үшін оң шетелдік тәжірибе алу бағыттарын анықтау. Зерттеу барысында жалпы ғылыми және арнайы таным әдістері, соның ішінде талдау, синтез, индукция және дедукция, ресми-құқықтық, салыстырмалы-құқықтық және жүйелік-құрылымдық әдістер қолданылды. Жұмыс шеңберінде алаяқтықтың цифрлық нысандары үшін жауапкершілікті реттейтін бірқатар шет елдердің, атап айтсақ, Еуропалық одақ, АҚШ және Азия елдерінің нормативтік құқықтық актілері, сот практикасы және

доктриналық тәсілдері зерттелді. Нәтижесінде deepfake және әлеуметтік инженерияны қолдана отырып, қылмыстарға құқықтық жауап берудің негізгі модельдері және олардың күшті және әлсіз жақтары анықталды. Қылмыстардың құрамын нақтылауды, алдын алу шараларын күшейтуді және халықаралық ынтымақтастықты дамытуды қамтитын құқықтық реттеуге кешенді көзқарастың қажеттілігі туралы қорытынды жасалды. Алынған нәтижелер қылмыстық және ақпараттық заңнаманы жетілдіру бойынша ұсыныстар әзірлеу кезінде пайдаланылуы мүмкін.

Кілт сөздер: Deepfake, онлайн-алаяқтық, киберқылмыс, цифрлық қауіпсіздік, әлеуметтік инженерия, заңнама, құқықтық саясат, құқықтық талдау.

А.Б. Сактаганова, И.С. Сактаганова

Правовое регулирование и ответственность за онлайн-мошенничество, основанное на применении deepfake и социальной инженерии: опыт зарубежных государств и направления его заимствования

В условиях стремительного развития цифровых технологий особую угрозу общественной безопасности представляет онлайн-мошенничество, основанное на применении технологий deepfake и методов социальной инженерии. Целью данного исследования является анализ правового регулирования и мер юридической ответственности за указанные виды преступлений в зарубежных государствах, а также определение направлений заимствования положительного зарубежного опыта для совершенствования национального законодательства. В ходе исследования были использованы общенаучные и специальные методы познания, включая анализ, синтез, индукцию и дедукцию, формально-юридический, сравнительно-правовой и системно-структурный методы. В рамках работы исследованы нормативные правовые акты, судебная практика и доктринальные подходы ряда зарубежных стран, в том числе государств Европейского союза, США и стран Азии, регулирующие ответственность за цифровые формы мошенничества. В результате выявлены основные модели правового реагирования на преступления с использованием deepfake и социальной инженерии, а также установлены их сильные и слабые стороны. Сделан вывод о необходимости комплексного подхода к правовому регулированию, включающего уточнение составов преступлений, усиление превентивных мер и развитие международного сотрудничества. Полученные результаты могут быть использованы при разработке предложений по совершенствованию уголовного и информационного законодательства.

Ключевые слова: Deepfake, онлайн-мошенничество, киберпреступность, цифровая безопасность, социальная инженерия, законодательство, правовая политика, правовой анализ.

References

1 (n.d.). Protecting Our Digitally-connected World is a Top Priority and Focus of the FBI. *ic3.gov*. Retrieved from https://www.ic3.gov/

2 (n.d.). Beware: scams involving fake correspondence from Europol. *europol.europa.eu*. Retrieved from https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/beware-scams-involving-fake-correspondence-europol

3 (n.d.). Your personal info, finances, and digital life-secured with McAfee+. *mcafee.com*. Retrieved from https://www.mcafee.com/

4 (n.d.). Cybercrime statistics for Kazakhstan. *special.zakon.kz*. Retrieved from https://special.zakon.kz/cyber_fraud

5 Smanova, A.B., Muratova, A.Zh., & Zhumagulova, S.R. (2025). Deepfake technologies and social engineering in online fraud forms, mechanisms, and legal challenges. *Bulletin of L.N. Gumilyov Eurasian National University. Law Series*, 3, 188–211.

6 Beaver, K. (2025). International and domestic legal frameworks on online fraud and deepfake technologies: a comparative criminal law analysis. *Bulletin of L.N. Gumilyov Eurasian National University. Law Series*, *152* (3), 212–228. https://bullaw.enu.kz/index.php/main/article/view/609

7 Apsimet, N.M. (2025). Crimes involving deepfake in online fraud and the challenges of proving them. *Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, 3 (80), 357–368.

8 Nowak, A., Tóth, B., & Ionescu, A. (2025). Legal Challenges of Deepfakes: Liability, Harm, and Regulatory Responses. *Legal Studies in Digital Age*. https://jlsda.com/index.php/lsda/article/view/306

9 Deloitte 2024 Financial Services Industry Predictions: AI Expected to Transform Retail Investing, Increase Banking Fraud and Drive New Insurance Market; Climate Change Expected to Further Increase Insurance Costs for Commercial Real Estate. *deloitte.com*. Retrieved from https://www.deloitte.com/us/en/about/press-room/deloitte-2024-fsi-predictions.html

10 Davey, O.M., & Sauerwein, L. (2025). Deepfake in Online Fraud Cases: The Haze of Artificial Intelligence's Accountability Based on the International Law. *Sriwijaya Crimen and Legal Studies*. Retrieved from https://journal.fh.unsri.ac.id/index.php/SCLS/article/view/2654?utm_source=chatgpt.com

11 (2025). Ob iskusstvennom intellekte. Zakon Respubliki Kazakhstan ot 17 noiabria 2025 goda № 230-VIII ZRK [On Artificial Intelligence. Law of the Republic of Kazakhstan dated November 17, 2025 No. 230-VIII ZRK]. *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/Z2500000230 [in Russian].

12 (2014). Ugolovnyi kodeks Respubliki Kazakhstan ot 3 iiulia 2014 goda № 226-V [Criminal Code of the Republic of Kazakhstan dated July 3, 2014 No. 226-V]. *online.zakon.kz.* Retrieved from https://online.zakon.kz/Document/?doc_id=31575252 [in Russian].

13 (1999). Grazhdanskii kodeks Respubliki Kazakhstan (osobennaia chast). Kodeks Respubliki Kazakhstan ot 1 iiulia 1999 goda № 409 [Civil Code of the Republic of Kazakhstan (Special Part). Code of the Republic of Kazakhstan dated July 1, 1999 No. 409]. *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/K990000409_ [in Russian].

14 (2014). Ob administrativnykh pravonarusheniiakh. Kodeks Respubliki Kazakhstan ot 5 iiulia 2014 goda № 235-V ZRK [On Administrative Offenses. Code of the Republic of Kazakhstan dated July 5, 2014 No. 235-V ZRK]. *adilet.zan.kz.* Retrieved from https://adilet.zan.kz/rus/docs/K1400000235 [in Russian].

15 Romero-Moreno, F. (2025). Deepfake detection in generative AI: a legal framework proposal to protect human rights. *Computer Law & Security Review*. Retrieved from https://www.sciencedirect.com/science/article/pii/S2212473X25000355?utm_source=chatgpt.com

16 Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, *107*, 1753–1819. https://doi.org/10.2139/ssrn.3213954

17 Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, *9*, 40–53. https://doi.org/10.22215/timreview/1282

18 Lumen, C. (2025). Deepfakes and the Limits of Law: a comparative analysis of regulatory frameworks in the U.S., EU, and China [Deepfakes and the Limits of Law: a comparative analysis of regulatory frameworks in the U.S., EU, and China]. *Journal of Advanced Artificial Intelligence*, *2* (3), 1–7.

Information about the authors

Saktaganova Akmaral Bakytovna — PhD, Senior Lector of the Department of Criminal Law Disciplines, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: aridnissakta.11@gmail.com

Saktaganova Indira Sovetovna — Doctor of Law, Professor of the Department of Constitutional and Civil Law, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: saktaganova@enu.kz