Ashur Journal of Legal and political Sciences (AJLSP) is published by the Iraqi Association for Legal Sciences
ISSN: 3005-3269, Vol 3(No.1), pages: 341-358 (2026)
https://ashurjournal.com/index.php/AJLPS/about

The Legal Framework for Combating Deepfakes and its Impact on the Criminal Evidence

Assistant Professor Dr: Ayad Abdul Hamza Beawee

Ministry of Interior/ Iraq , ayadesawy@yahoo.com

ARTICLE INFORMATION

Received:18 Dec 2025
Accepted:28 Dec 2025
Published:1 Mar 2026

Keywords: Deepfakes, Artificial Intelligence, Cybercrime, Criminal Evidence.

ABSTRACT

One of the most salient uses of generative artificial intelligence is deepfakes because it uses sophisticated algorithms that are capable of creating images, sounds, and videos that are hard to believe as fake. The complex legal and ethical issues have appeared due to this technological advancement as now it is possible to exploit this technology to infringe on privacy, defamation, manipulation of digital evidence, and even impact the democratic process by misinforming the media and creating a fake news. The threat of deepfakes is that they compromise the concept of trust in the digital content, and it puts the legislators in dilemmas of establishing the legal framework that would provide the freedom of invention and at the same time safeguard the basic rights of individuals. Among others, one of the biggest is the issue of finding criminal responsibility in creating or sharing fake content and the degree to which this action could be regarded as a type of cyber fraud. Thus, it is important to discuss this phenomenon on academic and legal level with the purpose to comprehend its technical and social aspects and to develop the balanced legislation in order to prevent the prevention of technological innovation, while simultaneously protecting the privacy of individuals and society.

مجلة آشور للعلوم القانونية والسياسية تصدر عن الجمعية العراقية للعلوم القانونية
المجلد الثالث (العدد الاول)، الصفحات:341-358، (2026) ISSN: 3005-3269
https://ashurjournal.com/index.php/AJLPS/about

الإطار القانون لمكافحة جرائم التزييف العميق وأثره على الاثبات الجنائي

الأستاذ المساعد الدكتور: اياد عبد الحمزة بعيوي

وزارة الداخلية/ العراق ، ayadesawy@yahoo.com

معلومات المقالة

تاريخ الاستلام : ١٨ كانون الثاني ٢٠٢٥
تاريخ القبول :٢٨ كانون الثاني ٢٠٢٥
تاريخ النشر : ١ اذار ٢٠٢٦

الملخص

يُعدّ التزييف العميق أحد أبرز استخدامات الذكاء الاصطناعي التوليدي، إذ يعتمد على خوارزميات متطورة قادرة على إنشاء صور وأصوات وفيديوهات يصعب تصديق أنها مزيفة. وقد برزت قضايا قانونية وأخلاقية معقدة نتيجة لهذا التقدم التكنولوجي، حيث أصبح من الممكن استغلال هذه التقنية لانتهاك الخصوصية، والتشهير، والتلاعب بالأدلة الرقمية، بل وحتى التأثير على العملية الديمقراطية من خلال تضليل وسائل الإعلام ونشر الأخبار الكاذبة. يكمن خطر التزييف العميق في أنه يُقوّض مفهوم الثقة في المحتوى الرقمي، ويضع المشرّعين أمام معضلة وضع إطار قانوني يضمن حرية الإبداع ويحمي في الوقت نفسه الحقوق الأساسية للأفراد. ومن أبرز هذه المعضلات مسألة تحديد المسؤولية الجنائية عن إنشاء أو مشاركة المحتوى المزيف، ومدى إمكانية اعتبار هذا الفعل نوعًا من أنواع الاحتيال الإلكتروني. لذا، من المهم مناقشة هذه الظاهرة على المستويين الأكاديمي والقانوني بهدف فهم جوانبها التقنية والاجتماعية، ووضع تشريعات متوازنة لمنع عرقلة الابتكار التكنولوجي، مع حماية خصوصية الأفراد والمجتمع في الوقت نفسه.

الكلمات المفتاحية: التزييف العميق، الذكاء الاصطناعي، الجرائم الإلكترونية، الأدلة الجنائية.

1. Introduction

One of the most perilous creations of artificial intelligence in the digital era is deepfakes because they are based on the application of sophisticated technologies to create counterfeit visual or sound material that can hardly be identified with the original one. It has resulted in the dawn of risks that endanger the basic criminal values like safeguarding the right to reputation, upholding privacy, and developing trust in criminal evidence. In criminal terms, the technology brings up some fundamental questions about whether it is legal or not, and what its locus is in the criminalization and punishment context .

There are those legal researchers who have viewed it as a novel type of digital forgery that undermines data and evidence credibility. The other angle sees it as a different type of cybercrime, as it has its own unique nature and far-reaching implications on the safeguarded criminal values, the most significant among them being the right to reputation and position, the right to privacy, and information protection. This technology has not only the effects on a personal level but also covers cybercrime toward information security and sabotage of the judicial system .

The need to approach this phenomenon in the framework of criminal law dictates itself as an academic and legislative requirement in an attempt to define criminal acts, police the area of criminal liability, and expansion solutions that guarantee deterrence and prevention.

1.1 The importance of the study: Deep fakes can be considered one of the most burning legal issues nowadays regarding the rapid growth of artificial intelligence technologies. Their significance is that they can create very precise visual or audio content that can hardly be differentiated with the reality and, therefore, can be used as an instrument to abuse personal rights, mislead the opinion of the masses, defame, and interfere with evidence. Thus, it is a legal issue that should be addressed to secure the trust of people and assure the safety of the information.

1.2 The problem of the study: Deepfakes provoke legal questions regarding the sufficiency of the existing laws in regulating their harmful consequences, especially in the area concerning the liability of the perpetrators of the forgery acts, and the safety of people against the attacks on their image and personal data, where there is a possibility of manipulation of visual or audio records in court. This study seeks to answer a number of questions, most notably: What is the current legal framework for addressing the phenomenon of deepfakes? Branches from this question into several]questions, including:

1- Are there current criminal laws that are adequate in dealing with this phenomenon?
2- How do deep faking systems fountain trouble on the judicial evidence system?
3- What methods can be developed to come up with balanced legislative solutions that will ensure that individual rights are not violated and at the same time technological innovation is encouraged?

1.3 Research Objectives: The proposed study is intended to study the phenomenon of deepfakes through the lens of an academic legal approach and outline the inefficiencies of the existing legislation governing this issue and the shortcomings of current policies on the topic,

as well as to suggest some practical measures in this area to address the risks associated with the issue, with considering the exclusive attributes of the digital environment.

1.4 Research Methodology: The study used the method of analytical approach, which is descriptive, by giving the nature of deep forgery and illustrates the technical and legal aspects of forgery, and the legislative texts and international agreements are analyzed to demonstrate the various experiences of the legislations using the comparative approach.

1.5 Outline of the study: This study is founded on a two-section format. The former part defines the overall structure of deepfakes based on two conditions. The former need is related to the essence of deepfakes and their technical aspects, as it defines the concept of deepfakes, its origins, and then describes its features and its most obvious criminal usage. The second requirement concerns the criminal basis for addressing deep forgery by identifying the scope of criminalization in national criminal legislation and examining the most important international trends in combating deep forgery. The second section then reviews criminal liability and evidence in deep forgery crimes through two subsections. The first requirement was to examine the criminal liability arising from deepfakes, whether for producing the fake content or for publishing and using it. Finally, the second requirement was dedicated to studying deepfakes and the challenges of criminal proof by demonstrating the impact of deepfakes on the credibility of digital evidence and the mechanisms for judicial and technical confrontation to establish the truth.

2. Deepfake Overview of Deepfakes

Deepfakes are among the most prominent emerging criminal phenomena resulting from the technological development of artificial intelligence, as they are based on producing high-precision fake audio or visual content that is difficult to detect by traditional means. Recent criminal research has also confirmed that the danger of deepfakes is not limited to individuals, but extends to society as a whole, through the possibility of using them for media manipulation or undermining confidence in the judicial system. Therefore, establishing a general framework for this phenomenon requires defining it and distinguishing it from other crimes, and stating the criminal basis that allows for its criminalization and the punishment of its perpetrators in accordance with modern national and international legislative trends.

2.1 What is deep faking and its technical nature?

Deep faking is one of the most prominent applications of generative artificial intelligence that has created unprecedented challenges in both the legal and technical fields. Its basic idea is based on the use of deep neural network techniques, especially adversarial generative networks (GANs), in order to produce images, videos, or audio recordings that simulate reality with a high degree of accuracy, making it difficult to distinguish between the real and the artificial.[1] The advent of this technology is associated with the huge leap in computing science and big data processing that has given remarkable possibilities to alter and redefine digital material in intricate forms that are hard to recognize using the conventional methodologies.[2]

Accordingly, the concept of deepfakes and their technical specifics is a two-story base of any criminal approach to this phenomenon, since it determines the cognitive structure, in accordance with which the criminalization and responsibility in the legal aspect are later developed.

2.1.1 Defining and Originating Deepfakes

Understanding the definition and origins of deep forgery is essential from a criminal law perspective for several reasons, including: it helps determine when an act of forgery is considered a crime; that is, determining when deep forgery has crossed the line from freedom of expression or creativity and entered the realm of crime.

It also allows for determining the responsibility of criminals by knowing the technology used and the mindset of the crime (intent/purpose), and whether there is knowledge that the content is fake? Thus, it facilitates the development of specialized criminal legislation based on an accurate understanding of technology and not just abstract accountability, leading to appropriate criminalization and deterrent punishment.

2.1.1.1 General Technical Definition

Deepfakes are a concept that refers to digital content, whether image, video, or audio, that is produced or modified using artificial intelligence techniques, particularly deep neural networks (Deep Learning) or generative adversarial networks (GANs), to make it appear as if someone is saying or doing something they did not actually say or do, or to present it in a way that is fake and conceals the truth.[3]

One of its modern definitions is: "Deepfakes are the application of artificial intelligence capable of generating digital content (visual, audio, or both) that represents a person in a way that appears realistic but is contrary to reality, and is used with the intent to harm them or expose their legally protected interests to harm or danger".[4]

2.1.1.2 The Origin and Historical Development of Deepfake

The term (Deepfake) first appeared around 2017 on the "Reddit" platform, when an anonymous user posted videos in which the faces of celebrities were replaced with their own faces in obscene content, using artificial intelligence algorithms.[5] Then, in 2018, open-source tools such as (FakeApp) and similar software platforms spread, allowing amateurs and ordinary programmers to produce this type of fake media.[6] With the development of deep learning algorithms and the availability of large datasets of images and videos, the quality of deepfake technology has improved rapidly, making the production of highly realistic videos possible even for those without extensive technical expertise.[7]

The development of adversarial generative networks (GANs) is a pivotal point, as this technology is based on two models: one generates fake content, and the other evaluates whether this content is fake, and learns from its differences in order to improve the quality of the fake so that it becomes difficult to distinguish.[8] The years since 2018 have witnessed a rapid spread of deepfakes via social media, especially in the context of (pornographic deepfake) and the posting of pictures or videos of famous faces without consent.[9]

2.1.2 Characteristics of deepfakes and their most prominent criminal applications

This phenomenon is characterized by technological features that increase its criminal risk and facilitate its exploitation in committing multiple crimes. Studying its characteristics and understanding its criminal applications requires a specialized legal approach to determine the scope of criminalization and liability.

2.1.2.1 Characteristics of Deepfakes

1- **High Realism and Advanced Similarity:** The technology used, such as Generative Adversarial Networks (GANs) and deep learning, allows the production of content (images, video, audio) in which people's features, movements, and voices are simulated with such accuracy that it is difficult to distinguish between fake and real, especially for non-specialist observers.[10]

2- **Easy access and pooling of digital resources:** With the availability of open-source software and tools, and huge datasets of faces and voices, the ability to produce (deep fakes) has become available even to those who do not have much technical expertise.[11]

3- **Lowering the technical threshold:** User interfaces have evolved so that the average user without advanced technological knowledge can generate fake videos using user-friendly applications or online. This lowers the barrier to committing criminal acts related to the use of (deep fake).[12]

4- **Speed of dissemination and the ability to copy and modify:** Fake content spreads rapidly across social media networks and the Internet, and can be republished or modified multiple times. This dissemination makes criminal harm faster and more widespread, and increases the difficulty of legal control.[13]

5- **The possibility of manipulating the legal implications of evidence:** One of the most important legal characteristics is that (deep fakes) can be used to falsify evidence or to influence its credibility before the judiciary, thus either justifying or casting doubt on the original evidence.[14]

2.1.2.2 The most prominent criminal applications of deepfakes:

1- **Blackmail and sexual revenge ("Revenge Porn"):** Deepfakes are used to create fake sexual images or videos of a person without their consent, then threaten to publish them for financial gain or personal revenge. These crimes represent a serious violation of privacy and human dignity.[15]

2- **Financial fraud and forgery:** Criminals use (deepfakes) to imitate the voices of officials or employees to give fake financial orders, or to exploit trust in personal or professional relationships in order to transfer money or obtain sensitive information or data.[16]

3- **Defamation and damage to reputation:** by publishing fake clips or recordings that show a person saying or doing what they did not do, which leads to defamation of their reputation, and the public's belief in incorrect behavior, and may lead to significant legal damages in terms of honor and dignity.[17]

4- **Political manipulation and dissemination of fake news**: The (deep fake) is used in the election campaign, or in influencing public opinion, by portraying a politician saying or doing controversial things, or fabricated scenes aimed at undermining confidence in public institutions.[18]

5- **Violation of identity and falsification of personal matters:** such as impersonating someone through voice or image for blackmail, to obtain privileges, to gain access to secure places, or to bypass biometric security systems.[19] In March 2019, a number of perpetrators managed to deceive the CEO of a British energy company by using fake voice technology, where his voice was expertly imitated to convince him to transfer an amount of US$243,000 to a supplier in Hungary.[20]
6- **Exploitation of minors and child sexual content:** This is one of the most dangerous applications, as the technology is used to produce fake child sexual content or to exploit a child's face without consent, which constitutes a serious crime in most criminal legislations.[21]

2.2The criminal basis for confronting deepfakes

The nature of deepfakes as a direct challenge to the values under the protection of the criminal law is the fact that it is used in the criminal process that hurts the reputation, privacy, and information safety. This accents the need to look into the criminal foundation of addressing them so as to identify the sufficiency or insufficiency of the available texts in taking care of this new phenomenon .

It is also possible to identify deepfakes in the context of criminalization and punishment with the help of this research and define the range of criminal responsibility. Thus, examining the criminal foundation is a significant move towards comprehending the processes of deterrence and safeguarding against this technology.

2.2.1 Scope of Criminalization in National Criminal Laws

The Iraqi legislation does not contain any explicit legal text that defines deepfakes and criminalizes them with the same specific technical interpretation. Deepfakes have not been criminalized in a specific manner, but the extent of criminalization is short and piecemeal based on other criminal statutes touching on other categories of crimes, and not the specific criminal statute concerning deepfakes. The existence of a draft cybercrime law may constitute the most appropriate framework for including an explicit criminalization of deepfakes, provided that its texts are formulated precisely, taking into account the technical characteristics and defining the criminal responsibilities.

2.2.1.1 Penal Code

The existing Iraqi Penal Code does not include an explicit provision criminalizing deepfakes as a newly developed technology or the use of artificial intelligence to produce fake content aimed at media deception, defamation, or other purposes. However, the Iraqi judiciary relies on traditional texts to prosecute some cybercrimes.[22]These texts are general and do not cover all the technical dimensions of Deepfake. They do not take into account the technical characteristics of deepfakes such as audio or visual modification using artificial intelligence, or dissemination via digitization and modern technological media. Therefore, Iraqi legislation suffers from the absence of criminal treatment for cybercrimes.[23]

2.2.1.2 Draft Cybercrime Law

There is a draft cybercrime law that has been proposed since about 2011, and since then it has been on the table for discussion in Parliament. This law aims to protect individuals and society from cybercrimes and combat them, and to raise awareness of their dangers, but so far

the law has not been approved in its final form despite being read in the House of Representatives in 2019, in 2021, Parliament refrained from continuing its reading until the necessary amendments were made to it.[24]

2.2.2 International Trends in Combating Deepfakes

Deepfakes have become a subject of increasing international concern due to their cross-border effects and the threats they pose to security, society, and public trust. Many comparative legislations have sought to establish special criminal frameworks to confront them, whether through cybercrime laws or through independent texts. International trends are increasingly focused on adopting strategies and laws that define the scope of criminalization and establish accountability for the production or dissemination of fake content. Therefore, studying these comparative experiences can help guide national legislators in formulating more effective solutions.

2.2.2.1 Legislative experiences at the international level

The international community has recognized the seriousness of deepfakes in undermining trust in digital information and impacting public security and the legal system. Therefore, international and regional attention has focused on strengthening cooperation to combat cybercrime in general, including the exploitation of artificial intelligence technologies. However, no explicit international text has been issued that explicitly criminalizes deepfakes.

Nevertheless, the 2001 Budapest Convention on Cybercrime has formed an international reference for criminalizing attacks arising from the misuse of information technology,[25] and has opened the door to including newly developed images such as (deep fake) within the concepts of forgery and information fraud.

1- **The European Union:** Among international experiences, the European Union adopted a regulatory framework based on the "Digital Services Act" of 2022. This law addressed the regulation of illegal content, transparent advertising, and combating misinformation, including fake content aimed at deceiving the public or manipulating information.[26] The Artificial Intelligence Act of 2023 imposes obligations on technology companies to be transparent and to disclose fake content, while also allowing criminal accountability in cases of media manipulation or violation of fundamental rights.[27]

Similarly, the General Data Protection Regulation (GDPR 2016) is especially crucial in the fight against deepfake crimes as it helps to increase the privacy and personal data protection of any individual. It guarantees their right to control their data and imposes strict restrictions on the collection, processing, or use of this data without explicit consent.[28]

2- **United States of America:** Texas is the first US state to enact special provisions criminalizing deepfakes when used to influence elections, specifying appropriate penalties by Texas Election Interference Law 2019. By the end of 2024, fourteen states had enacted new legislation and regulations aimed at regulating the use of deepfake technologies in the political sphere, particularly in communications and election campaigns, these states have also adopted new policies regarding the role of artificial intelligence in managing electoral processes, focusing on ways to employ it in

enhancing election security on the one hand, and limiting its use in undermining its integrity or influencing the will of voters on the other hand.[29]

1.2.2.2 Legislative experiences at the level of Arab countries:

1- **Egypt:** Law No. (175) of 2018 AD concerning combating information technology crimes punishes deepfake acts, as the Egyptian legislator criminalized, according to it, the publication of misleading information and the exploitation of modern technologies in falsifying images and videos, including what is known as deepfake.[30]

2- **Jordan:** In keeping with the rapid developments in the field of cybercrimes, Jordan issued the Cybercrimes Law of 2023, with the aim of addressing the various forms of crimes that occur in the digital space. This law included an indirect reference to one of the forms of deepfakes by punishing anyone who used an information network, information technology, information system or website to commit acts that fall under some forms of deepfakes, such as extortion and deep pornographic revenge in article (20/2).[31]

3. Criminal liability and proof in deepfake crimes

Deepfake poses a complex challenge to criminal law, not only in terms of defining the scope of criminalization, but also in terms of assigning criminal liability to the perpetrator or accomplices in producing or disseminating the fake content. The issue is even exacerbated by the fact that it is not easy to determine the identity of the offender in an online environment where hiding and disguising is straightforward.[32]

Thus, criminal responsibility and evidence in deepfake crimes should be researched as the step to understand how to address this phenomenon on the legislative and judicial level and whether it is possible to strike the balance between safeguarding individual rights and upholding criminal justice.

3.1 Criminal liability arising from deepfakes

Deepfakes cause some basic problems with the issue of criminal responsibility, because the activity of creating or spreading fake information is associated with a direct violation of individual rights and the common good. This creates concerns regarding how to establish the initial violator of digital space, and the level of responsibility of partners or the technical intermediaries. Hence the importance of researching criminal liability arising from deep forgery to clarify its foundations and limits in light of the general rules of criminal law.

3.1.1 Responsibility for producing fake content

The production of fake content through deepfake technology represents the most dangerous behavior in this phenomenon, as it constitutes the starting point that enables the commission of the remaining subsequent criminal acts such as publishing, distribution, or exploitation. The question arises here about the criminal nature of this act, and the legal basis for assigning responsibility to the one who creates it.

3.1.1.1 Adapting the act from a criminal perspective

The production of fake content is considered a crime in itself when its material and moral elements are available. From a material perspective, the criminal behavior is realized when the perpetrator, with his full will, uses artificial intelligence tools to generate fake images, sounds, or videos in a way that mimics reality.[33] The nature of the criminal behavior in deepfake crimes is highlighted by the perpetrator's positive action of using, directing, or exploiting deepfake applications unlawfully to harm the victim. This crime cannot be conceived as being committed through a negative act such as refraining from performing a specific act.[34]

From a moral standpoint, criminal intent is established when the perpetrator is aware that he is using forgery by using artificial intelligence tools to produce fake content, and his will to direct it towards illegitimate purposes to use it for blackmail, defamation, or misleading.[35] The moral element is a dividing element that distinguishes between legitimate uses of technology and criminal uses, and the objectives sought by the perpetrator are not taken into account, whether they are to achieve material gains, to take revenge on the victim, to reach political goals, or were motivated by curiosity and entertainment only.[36]

3.1.1.2 The legal basis for liability

In the absence of specific criminal provisions in many legislations, liability for producing fake content can be attributed to the general rules of the Penal Code. The act may fall under the crimes of information forgery, fraud, or defamatory publication, and it can also be classified as a crime of violating the sanctity of private life when the content relates to the personal lives of individuals.[37]

Criminal liability is based primarily on the original perpetrator who creates the fake content. However, the nature of digital crime makes criminal complicity common. According to the general rules of criminal law, these individuals are considered accomplices when forms of criminal contribution such as incitement, agreement, or assistance are present, and the penalty prescribed for the same crime is applied to them.[38]

Therefore, deepfakes using artificial intelligence techniques are, from a legal standpoint, a technical tool that does not possess independent will or self-awareness. Consequently, criminal responsibility for unlawful acts committed by it falls on the person who intentionally uses it to carry out the crime, this person is often the programmer or the end user, as the moral actor who directs the system and exploits its technical capabilities to achieve the intended criminal result.[39]

3.1.2 Responsibility for publishing and using fake content

Publishing or circulating fake content is a stage no less dangerous than producing it, as it contributes to expanding the circle of harm and reaching the largest number of people with the content, thus multiplying its criminal effects. This act raises questions about the extent of its independence as a crime in itself, or whether it is considered a form of participation in the original crime.

3.1.2.1 The criminal characterization of the act of publishing

Most legislations consider the publication of false content through any means of publicity to be a criminal act when it involves a criminal intent represented by knowledge of

the falsity of the content and the will to publish it. The act takes the form of an independent crime if the publication is done with the intent of defamation, misleading or influencing public opinion, however, if the publication is done without clear criminal intent, the debate may arise regarding the publisher's responsibility, especially if he is merely a transmitter of content.[40]

3.1.2.2 The legal scope of liability

The act of publishing can fall under the provisions criminalizing defamation, electronic slander, or the dissemination of false news. It can also be classified as a crime of assault on public order if it results in inciting chaos or threatening information security. The most prominent problem facing criminalization in this context is the difficulty of distinguishing between intentional publication to harm others and accidental or unintentional publication. Also, the wide scope of publication in the digital space makes it difficult to control all cases of circulation, and this calls for the development of precise texts that define the standard of knowledge and will as a condition for assigning responsibility.[41]

This point also raises a complex issue concerning the responsibility of individuals who share fake content on social media platforms. Is this considered a criminal act when the person sharing it is aware of its falsity? The existing criminal opinion is that sharing with such knowledge concerning the nature of the content publicly is a kind of a criminal involvement that should be punished.[42]

3.2 Deepfakes and the Challenges of Criminal Evidence

The criminal evidence forms the foundation of attaining criminal justice and being able to punish the perpetrator in a fair way. But the introduction of the deepfakes technology has given a dark cloud on this principle because of the high capacity it has given to create visual and audio materials that are hard to differentiate between the reality and the visual or audio content.[43]

This has made the work of investigators and the judiciary to establish the authenticity of the digital evidence difficult and this has even caused serious anxiety on the probability of frustrating justice by providing fabricated evidence which is hard to detect by use of the conventional process. Therefore, the issue of deepfakes becomes one of the most salient modern challenges of the criminal evidence system, which needs to be thoroughly studied in order to understand how to deal with them on the legislative and technical levels.

3.2.1 The impact of deepfakes on the credibility of digital evidence

The surge in the technological aspect of artificial intelligence has resulted in the creation of deepfakes as the instrument that can harm the conventional system of criminal evidence. The digital evidence, which used to be regarded as one of the most valid ways to attain evidence, faces the danger of losing its value in the presence of the capability of this technology to create fake content that is hard to discern.[44] Therefore, the relevance of the research on the effects of deepfakes on the validity of the digital evidence becomes one of the most severe current issues of the criminal justice.

3.2.1.1 Undermining confidence in traditional evidence

Criminal justice at one time treated audio and visual evidence as one of the most powerful forms of evidence due to the fact that it has a direct relationship with reality and at the time it was hard to fake. This belief has, however, been undermined with the advent of deepfake technology, which has made it possible to create such fake recordings or image that would replicate reality at an insane level of accuracy. This has radically changed the perception of the courts of admissibility in case of digital evidence and it is under constant scrutiny.[45] Moreover, it is possible to confuse the judges or investigators with false evidence that proves the crime did not exist. Given that a manipulated image or video may be used as evidence, the court may use it to convict an innocent individual or free a true offender, thus jeopardizing the concept of criminal justice.[46]

3.2.1.2 Difficulty of technical verification

The digital evidence is described as being malleable and changeable, however, deepfakes complicate the process of identifying the manipulation due to the artificial intelligence algorithms that generate content more similar to reality[47]. Thus, it is no longer possible to detect the forgery using conventional methods or human experience as it is, but rather using sophisticated methods and precise tools of digital analysis.[48] These challenges necessitate that criminal legislation reconsider the rules of evidence. Audio and visual evidence no longer possesses the same absolute power, but must it be accompanied by digital technical reports that prove its authenticity and integrity [49]

In addition, courts are now required to conduct a greater degree of investigation before adopting digital evidence, with the assistance of digital experts,[50] while setting clear standards for accepting digital evidence in a way that ensures a balance between its validity and the risk of tampering with it.[51]

3.2.2 Judicial and technical mechanisms for proving the truth

Deepfakes have created complex challenges for criminal justice, especially in the field of proving criminal truth, as doubts increase about the credibility of digital evidence, it has become necessary to examine the judicial and technical mechanisms that can ensure the integrity and validity of evidence. Hence, it is necessary to study the available means of confrontation to enhance the judiciary's confidence in digital evidence and protect the proof system from the risks of misrepresentation.[52]

3.2.2.1 Technical tools for detecting forgery

Experts in the field of digital evidence have developed a range of specialized technical tools for analyzing audio and visual content to detect signs of manipulation.[53] Among the most prominent of these tools are:

1- **Digital Forensic Analysis**: This is based on studying the metadata of images and videos to determine the date of their creation or modification.[54]
2- **Intelligent counter-techniques(AI-based Detection)**: where AI algorithms are trained to detect abnormal patterns in images or videos that indicate the use of deepfakes.[55]
3- **Detailed visual examination:** which relies on tracking minute details in lip movements, facial expressions, or lighting effects to detect inconsistencies.[56]

3.2.2.2 The role of technical expertise in advance the judiciary

Addressing the issue of deepfakes would mean that the judiciary would have to base its case on the reports of the experts in the field of digital evidence. They are charged with the responsibility of investigating the dubious content and handing in technical reports on its authenticity. This supports the concept of judicial impartiality since the judge cannot apply his own discretion to differentiate between authentic and counterfeit content since the technological advancement in this area is enormous.[57]

Although technical tools have been developed to identify deepfakes, they are not yet effective enough to do so due to a number of reasons, such as: deepfakes keep on getting better, so even the technical means of detecting them are not able to keep up with the quality of the fake content wholeheartedly.[58] Numerous court systems also do not have qualified experts in the digital field, which restricts the possibilities of the courts to verify evidence.[59]

Besides, digital forensic analysis procedures can be costly in terms of money and technicalities, and this cannot be consistently practiced on any subject. It has consequently emerged that there is a need to hire the services of technical professionals in order to recover digital evidence[60]. Collaboration and feedback of experience between centers and institutions of the technical sphere should also be reinforced, and the goal to confer the gap that is caused by the lack of experience and the expensive nature of gathering evidence using technical tools.[61]

3.2.2.3 Procedural mechanisms for confronting transnational deep forgery crimes in light of Iraqi legislation

Deep forgery crimes are characterized by their transnational nature, as the criminal act often occurs outside the state's territory while its effects are felt within it. This limits the practical effectiveness of the criminal framework unless it is supported by flexible procedural mechanisms derived from existing Iraqi legislation. In this context:

1- The Iraqi Penal Code allows for the prosecution of perpetrators whenever the result of the crime is achieved within Iraq or affects its fundamental interests, in line with the modern trend in criminal policy to confront serious digital crimes[62] .

2- The Code of Criminal Procedure allows for the use of technical expertise and the use of judicial evidence,[63] as well as obligating digital service providers to preserve data or provide it as an alternative to judicial delegations that are not possible[64] .

3- If it is impossible to bring the accused, the law allows the case to proceed in absentia,[65] with the possibility of pursuing the financial proceeds obtained from the crime in accordance with the Anti-Money Laundering and Counter-Terrorism Financing Law[66] .

4- Despite the absence of a specific regulation for deepfake crimes, the general rules of criminal liability allow for holding accountable those who contribute to the dissemination of criminal content or refrain from removing it,[67] in addition to enabling the judiciary to issue temporary orders to stop or remove the illegal content in order to protect victims.[68]

Conclusion

Having examined the issue of The Criminal Framework of Combating Deepfakes. and its Effect on the Evidence System, we may say that this phenomenon is a qualitative problem of the traditional criminal legal system as it has a significant effect on the loss of trust in digital evidence and the weakening of the evidence system. It has now become evident that even the

general provisions of the criminal law, so extensive as they are, are not adequate, separate laws and special technical judicial apparatus are necessary, which can be used to combat the dangers of this phenomenon. Lastly, the very efficient response to deepfakes is the combination of legislation, technology, and the judiciary to guarantee the integrity of the criminal justice system and safeguard society against the grave consequences of such an occurrence.

First: findings

1- Deepfakes are a qualitative jump in cybercrime since they provide enormous opportunities to create evidence falsifications that are hard to identify by conventional means.
2- Digital evidence, especially audio and visual evidence is no longer being taken seriously during criminal proceedings but it has since been treated with a lot of suspicion.
3- The flaws in national criminal laws in facing this phenomenon directly, which in many cases is confined to general clauses, which are not keeping up with the change in technology.
4- Technical skills and modern technologies still play a key role in criminal evidence in the deep forgery cases, which provokes legal doubts over the admissibility of criminal evidence.
5- The international aspect of these crimes is that it cannot be fought by acting unilaterally, but rather using international laws.

Second: Recommendations

1- Criminalize the creation and sharing of deepfakes through the enactment of specific criminal legislation and the creation of the criminal liability scope.
2- Create articulate criteria on admissibility of digital evidence which the courts should rely on expert technical reporting before admitting such evidence.
3- Establish national centers of digital forensics to offer technical assistance to the courts and investigative agencies.
4- Making it obligatory to the companies that possess applications and online platforms to create tools to detect and report fake contents.
5- Bilateral and multilateral agreements on sharing information and technical expertise on the area of combating deepfakes.
6- Organizing legal and technical awareness campaigns to teach people about the harmfulness of deepfakes and their recognition..

الهوامش :

[1] Ali Mawloud Fadel, and Saif Abbas Adnan, Deepfakes/The Language of Artificial Intelligence in Cyber Media Wars, Amjad Publishing and Distribution House, Amman, 2021, p. 25.

[2] Muhammad Salama Abdel Moneim Al-Sharif, The Crime of Revenge Pornography Through Deepfake Technology and Responsibility for It, Journal of Law for Legal Research, Volume (2), Issue (1), pp. (366-485), 2022 ,p.367.

[3] Ali Mawloud Fadel, and Saif Abbas Adnan, previous source, p. 17.

[4] Sahar Fouad Majeed Al- Najar, Criminal Response to Crimes Stemming from the Use of Deepfake Technology, Journal of Legal Science, Volume (39), Issue(2), pp.(575-633),2024, p.580.

[5] Laura Carvajal, and Andrew Iliadis, Deepfakes: A preliminary Systematic Review of The Literature. AOIR Selected Papers of Internet Research, (2020), pp.(1-4), p.2. https://spir.aoir.org/ojs/index.php/spir/article/view/11190/9860 Last visit 5/11/2025.

[6] Reda Ibrahim Abdullah Al-Bayoumi, Legal Protection from the Risks of Deep faking Applications in Islamic Jurisprudence and Positive Law: A Comparative Analytical Study, The Spirit of Laws Journal , Faculty of Law-Tanta University, Special Issue for the Eighth International Scientific Conference (Technology and Law) for the period (7-8/5/2023), pp. (815-878), 2023,p.828.

[7] Sahar Fouad Majeed Al- Najar, previous source, p.585.

[8] Gauri Jaiswal et al, Deepfake Technology: The Threat of AI-Generated Misinformation, International Journal of Research Publication and Reviews, Volume (6), Issue (3), pp.(930-934),2025 ,p.930.

[9] Muhammad Salama Abdel Moneim Al-Sharif, previous source,p.373.

[10] Sahar Fouad Majeed Al- Najar, previous source, p.581.

[11] Nik Hynek et al., Risks and benefits of artificial intelligence deepfakes: Systematic review and comparison of public attitudes in seven European Countries, Journal of Innovation & Knowledge, Volume (10) Issue (5) pp.(1-19), 2025, p.1.

[12] Reda Ibrahim Abdullah Al-Bayoumi, previous source, p. 841.

[13] Ali Mawloud Fadel, and Saif Abbas Adnan, previous source, p.101.

[14] Sahar Fouad Majeed Al- Najar, previous source, p.583.

[15] Ali Mawloud Fadel, and Saif Abbas Adnan, previous source, p. 17.

[16] Ali Mawloud Fadel, and Saif Abbas Adnan, previous source, p. 32.

[17] Gauri Jaiswal et al, Deepfake Technology: The Threat of AI-Generated Misinformation, International Journal of Research Publication and Reviews, Volume (6), Issue (3),2025 , pp.(930-934),p.931.

[18] Nik Hynek et al., previous source, p.1.

[19] Mahmoud Hussein Sayed Abu Seif, The Legal Regulation of Deepfake in the European Union Artificial Intelligence Act, Journal of Legal and Economic Sciences, Issue (1), Year (67), pp.(1642- 1741), 2025, p.1692.

[20] Reda Ibrahim Abdullah Al-Bayoumi, previous source, p. 842.

[21] Abigail Olson, "The Double-side of Deepfakes: Obstacles and Assets in the Fight Against Child Pornography," Georgia Law Review, Volume (56). Issue (2), pp.(856-892), (2022), p. 869.

[22] Emil Jabbar Ashour, Sabreen Jassim Maktoof, The Legal Adaptation of the Crime of Deliberate Forgery (A Comparative Study), Maysan Journal of Comparative Legal Studies, Volume (1), Issue (13). pp.(514-540),2025, p.535.

[23] Sahar Fouad Majeed Al- Najar, previous source, p.583.

[24] Safaa Ayad, The Cybercrime Law in Iraq: Suspended Until Further Notice?, Digital Safety helpdesk (SMES),Iraqi Cybercrime Draft Law: In Suspension. Article published in 14/1/2022.https://smex.org/ar/%d9%82%d8%a7%d9%86%d9%88%d9%86%d8%ac%d8%b1%d8%a7%d8%a6%d9%85%d8%a7%d9%84%d9%85%d8%b9%d9%84%d9%88%d9%85%d8%a7%d8%aa%d9%8a%d8%a9%d8%a7%d9%84%d8%b9%d8%b1%d8%a7%d9%82-%d9%85%d8%b9%d9%84%d9%82/ last visit 5/11/2025.

[25] Suleiman Qataf, and Abdul Halim Bougrine, The Objective Legal Mechanisms for Combating Cyber Crimes under the Budapest Convention and Algerian Legislation, Academic Journal of Legal and Political Research, Volume (6), Issue (1), pp. (334-358), 2022, p.339.

[26] Sahar Fouad Majeed Al- Najar, previous source, p.600.

[27] Mahmoud Hussein Sayed Abu Seif, previous source, p.1676.

[28] Sahar Fouad Majeed Al- Najar, previous source, p.599.

[29] Sahar Fouad Majeed Al- Najar, previous source, p.596.

[30] Reda Ibrahim Abdullah Al-Bayoumi, previous source, p. 853.

[31] The Cybercrimes Law of 2023, article (20/2).

[32] Sahar Fouad Majeed Al- Najar, previous source, p.583.

[33] Reda Ibrahim Abdullah Al-Bayoumi, previous source, p. 855.

[34] Alaeldin Mansour Maghaireh, Artificial Intelligence Crimes and Ways to Combat Them: Deepfakes as a Model, International Journal of Law, Qatar University, Volume (13), Issue (2), pp. (127-167), 2024, p.145.

[35] Azzedine Ritab, and Nabila Sadrati, The legal nature of the act of cyber defamation via artificial intelligence tools. Algerian Journal of Law and Political Science, Volume (9). Issue (1), pp. (933-952), 2024, p. 47.
[36] Alaeldin Mansour Maghaireh, Previous source, p.146.
[37] Sahar Fouad Majeed Al- Najar, previous source, p.585.
[38] Mona Mohamed Al-Atris Al-Desouki, Crimes of Artificial Intelligence Technologies and the Independent Electronic Legal Personality (A Comparative Study), Journal of Legal and Economic Research, Issue (81), pp.(1141-1222), 2022, p.1191.
[39] Ahmed Ali Ahmed Al-Najm, Criminal liability for artificial intelligence crimes, Journal of the College of Heritage University, Issue (39), Special Issue, 2024, p.151.
[40] Mona Mohamed Al-Atris Al-Desouki, Previous source, p.1168.
[41] Ahmed Ali Ahmed Al-Najm, previous source, p. 149.
[42] Haskar Mourad Ben Aouda, The Problem of Applying the Provisions of Criminal Liability to Artificial Intelligence Crimes, Journal of Law and Humanities, Volume (15). Issue (1). pp. (187-205), 2022, p.198.
[43] Muhammad Salama Abdel Moneim Al-Sharif, previous source,p.367.
[44] Mohammed Wahhab Abbood, USING AI TOOLS TO VERIFY DEEPFAKES IN MEDIA CONTENT, Proceedings of the Ninth Scientific Conference (Third International) of Media Colleges - Iraqi Universities, entitled: Artificial Intelligence in the Horizons of Innovation and the Challenges of Cultural Dialogue, from 23-24/4/2025, (Special Issue), pp.(171-179), 2025, p.575.
[45] Yazid Saleh Al-Muhamid, Cybercrimes in Criminal Law, The Legal Journal, Volume (25), Issue (3), pp. (2201-2256), 2025, p.2247.
[46] Sahar Fouad Majeed Al- Najar, previous source, p.582.
[47] Emile Jabbar Ashour, Sabreen Jassim Maktoof, previous source, p.856.
[48] Ali Mawloud Fadel, and Saif Abbas Adnan, previous source, p. 33.
[49] Ali Mawloud Fadel, and Saif Abbas Adnan, previous source, p. 65.
[50] Emile Jabbar Ashour, Sabreen Jassim Maktoof, previous source, p. 858.
[51] Mohamed Mohamed Abdel Zaher Mosa, The evidentiary value of digital evidence and the controls of the criminal judge's conviction, Journal of Legal and Economic Research, Volume (36), Issue (2), pp. (226-336), 2024, p. 296.
[52] Alaeldin Mansour Maghaireh, Previous source,p.142.
[53] Ali Mawloud Fadel, and Saif Abbas Adnan, previous source, p.44.
[54] Reda Ibrahim Abdullah Al-Bayoumi, previous source, p.835.
[55] Ali Mawloud Fadel, and Saif Abbas Adnan, previous source, p.55.
[56] Mohamed Abdulrahman Abdulhamed, and Asaad Noori Hashim, A Survey on Detecting Deep Fakes Using Advanced AI-Based Approaches, Iraqi Journal of Science, Volume (65). Issue (9). pp. (5254-5269), 2024, p.5260.
[57] Mohamed Mohamed Abdel Zaher Mosa, Previous source, p.304.
[58] Ali Mawloud Fadel, and Saif Abbas Adnan, previous source, p.54.
[59] Hussein Muhammad Assaf , The Legality and Admissibility of Digital Evidence in Criminal Procedures: A Comparative Analytical Study. Comprehensive Electronic Journal. Issue (82). pp. (1-35), 2025, p.28.
[60] Emil Jabbar Ashour, Sabreen Jassim Maktoof, previous source, p.858.
[61] Hussein Muhammad Assaf , previous source, p.29.
[62] Articles (6 & 9) of the Penal Code No. (111) of 1969, as amended.
[63] Articles (69 & 70) of the Code of Criminal Procedure No. (23) of 1971, as amended.
[64] Articles (51 & 52) of the Code of Criminal Procedure No. (23) of 1971, as amended.
[65] Articles (153 - 155) of the Code of Criminal Procedure No. (23) of 1971, as amended.
[66] Chapter Nine of the Anti-Money Laundering and Counter-Terrorism Financing Law No. (39) of 2015, comprising Articles (27-33).
[67] Entities or individuals who contribute to the dissemination of counterfeit content or facilitate its circulation may be subject to the provisions of criminal complicity stipulated in Articles (47& 48, and 49) of the Iraqi Penal Code No. (111) of 1969, as amended.
[68] Article (99) of the Code of Criminal Procedure No. (23) of 1971, as amended.

References

Frist: Books

Ali Mawloud Fadel, and Saif Abbas Adnan, Deepfakes: The Language of Artificial Intelligence in Cyber Media Wars, Amjad Publishing and Distribution House, Amman, 2021.

Second: Articles

Gauri Jaiswal et al., Deepfake Technology: The Threat of AI-Generated Misinformation. International Journal of Research Publication and Reviews. Volume (6). Issue (3). pp.(930-934), 2025.

Nik Hynek et al., Risks and benefits of artificial intelligence deepfakes: Systematic review and comparison of public attitudes in seven European Countries. Journal of Innovation & Knowledge, Volume (10), Issue (5), pp.(1-19), 2025.

Reda Ibrahim Abdullah Al-Bayoumi, Legal Protection from the Risks of Deep faking Applications in Islamic Jurisprudence and Positive Law: A Comparative Analytical Study, The Spirit of Laws Journal, Faculty of Law-Tanta University, Special Issue for the Eighth International Scientific Conference (Technology and Law for the period (7-8/5/2023), pp.(815-878), 2023.

Mohamed Abdulrahman Abdulhamed, and Asaad Noori Hashim, A Survey on Detecting Deep Fakes Using Advanced AI-Based Approaches. Iraqi Journal of Science. Volume (65), Issue (9). pp. (5254-5269), 2024.

Muhammad Salama Abdel Moneim Al-Sharif, The crime of revenge porn through deepfake technology and criminal liability for it. Journal of Law for Legal and Economic Research. Volume (2). Issue (1). pp. (366-485), 2022.

Sahar Fouad Majeed Al- Najar, Criminal Response to Crimes Stemming from the Use of Deepfake Technology. *Journal of Legal Science*. Volume (39). Issue(2). pp.(575-633), 2024.

Mahmoud Hussein Sayed Abu Seif, The Legal Regulation of Deepfake in the European Union Artificial Intelligence Act, Journal of Legal and Economic Sciences, Issue (1), Year (67), pp. (1642- 1741), 2025.

Abigail Olson, "The Double-side of Deepfakes: Obstacles and Assets in the Fight Against Child Pornography," Georgia Law Review, Volume (56), Issue (2), pp.(856-892), 2022.

Emil Jabbar Ashour, and Sabreen Jassim Maktoof, The Legal Adaptation of the Crime of Deliberate Forgery (A Comparative Study), Maysan Journal of Comparative Legal Studies, Volume (1), Issue (13), pp.(514-540), 2025.

Mohamed Mohamed Abdel Zaher Mosa, The evidentiary value of digital evidence and the controls of the criminal judge's conviction, Journal of Legal and Economic Research, Volume (36), Issue (2), pp. (226-336), 2024.

Alaeldin Mansour Maghaireh, Artificial Intelligence Crimes and Ways to Combat Them: Deepfakes as a Model. International Journal of Law, Qatar University, Volume (13), Issue (2).pp. (127-167), 2024.

Azzedine Ritab, and Nabila Sadrati, The legal nature of the act of cyber defamation via artificial intelligence tools, Algerian Journal of Law and Political Science, Volume (9), Issue (1), pp. (933-952), 2024.

Mona Mohamed Al-Atris Al-Desouki, Crimes of Artificial Intelligence Technologies and the Independent Electronic Legal Personality (A Comparative Study), Journal of Legal and Economic Research, Issue (81), pp.(1141-1222), 2022.

Ahmed Ali Ahmed Al-Najm, Criminal liability for artificial intelligence crimes. Journal of the College of Heritage University. Issue (39), pp.(145-154), 2024.

Haskar Mourad Ben Aouda, The Problem of Applying the Provisions of Criminal Liability to Artificial Intelligence Crimes, Journal of Law and Humanities, Volume (15), Issue (1), pp. (187-205), 2022.

Mohammed Wahhab Abbood, Using Ai Tools To Verify Deepfakes in Media Content. Journal of Media Studies and Research (Masar), Special Issue, pp. (171-197), 2025.

Yazid Saleh Al-Muhamid, Cybercrimes in Criminal Law, The Legal Journal, Volume (25), Issue (3), pp. (2201-2256), 2025.

Hussein Muhammad Assaf, The Legality and Admissibility of Digital Evidence in Criminal Procedures: A Comparative Analytical Study, Comprehensive Electronic Journal, Issue (82), pp. (1-35), 2025.

Suleiman Qataf, and Abdul Halim Bougrine, The Objective Legal Mechanisms for Combating Cyber Crimes under the Budapest Convention and Algerian Legislation, Academic Journal of Legal and Political Research, Volume (6), Issue (1).pp. (334-358), 2022.

Third: Legislations

Iraqi Penal Code No. (111) of 1969, as amended.

The Code of Criminal Procedure No. (23) of 1971, as amended

Budapest Convention on Cybercrime of 2001.

Iraqi draft cybercrime law of 2011.

The Anti-Money Laundering and Counter-Terrorism Financing Law No. (39) of 2015

The General Data Protection Regulation (GDPR) of 2016.

Egyptian Anti-Cyber and Information Technology Crimes No (175) of 2018.

Texas Election Interference Law 2019.

European Union's Digital Services Oversight and Safety Act of 2022 .

Jordanian Cybercrime Law No. (17) of 2023.

European Union's The Artificial Intelligence Act of 2023.

Forth: Electronic articles

Laura Carvajal, and Andrew Iliadis, Deepfakes: A preliminary Systematic Review of The Literature. AOIR Selected Papers of Internet Research, 2020,https://spir.aoir.org/ojs/index.php/spir/article/view/11190/9860 ,last visit 7/11/2025.

Safaa Ayad, The Cybercrime Law in Iraq: Suspended Until Further Notice?, Digital Safety helpdesk (SMES),Iraqi Cybercrime Draft Law: In Suspension, Article published in 14/1/2022, https://smex.org/ar/%d9%82%d8%a7%d9%86%d9%88%d9%86%d8%ac%d8%b1%d8%a7%d8%a6%d9%85%d8%a7%d9%84%d9%85%d8%b9%d9%84%d9%88%d9%85%d8%a7%d8%aa%d9%8a%d8%a9%d8%a7%d9%84%d8%b9%d8%b1%d8%a7%d9%82%d9%85%d8%b9%d9%84%d9%82/, last visit 5/11/2025.