SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 11, No. 4, (2025), pp. 3311-3320
Open Access. Online & Print

DOI: 10.5281/zenodo.11425149

CRIMINAL PROSECUTION OF CRIMES INVOLVING MANIPULATION OF ELECTRONIC CONTENT USING DEEPFAKE APPLICATIONS

Mohannad Walid Al-Haddad[1]

[1]Associate Professor of Criminal Law, Department of Public Law, Faculty of Law, Jerash University, Jordan.
ORCID iD: https://orcid.org/0009-0005-1085-2252, Email: m11haddad@yahoo.com

Received: 25/07/2025
Accepted: 28/11/2025

Corresponding Author: Mohannad Walid Al-Haddad (m11haddad@yahoo.com)

ABSTRACT

In recent years, the world has witnessed a remarkable rise in the use of artificial intelligence and deep learning to create hyper-realistic images, videos, and audio clips. Artificial intelligence technology, known as "deep fakes," take real image and audio data and replace or modify its main details, manipulating the content by modifying facial features, speech, and movement with such realism that it is often impossible to distinguish it from the real content. The problem of the study emerged in clarifying the threats that deep fake applications can pose by researching the effectiveness of Jordanian law and comparative texts in addressing deep fake crimes, such as sexual exploitation, defamation, fabrication of crimes, blackmail, and dissemination of misinformation. Therefore, through this study, we will work to answer several questions, the most important of which are: What are deep fake applications? Does the illegal use of these applications entail criminal liability under the law? What crimes can be committed using them? What are the ways to counter this type of abuse? Our study requires following an analytical and descriptive approach based on gathering information from various academic and non-academic sources, in addition to using a comparative approach with some developed countries in developing their legislation in this regard, with the aim of answering the research question.

KEYWORDS: Deep Fakes, Cybercrime, Artificial Intelligence, Digital Content.

1. INTRODUCTION

Deep fake applications are defined as a subset of "synthetic media" or "synthetic content," a type of artificial intelligence that, as the name suggests, is used to create fake content, such as images, audio, and video. Artificial intelligence applications, especially deep fakes, have a positive side in that they have a number of useful applications in creativity, entertainment, education, media, and other fields.

On the other hand, there is a dark side, as this application can be used as a criminal tool in the commission of many cybercrimes (Mughaier, Alaa El-Din, 2023). Cybercrime is poised to take a quantum leap forward, especially with the use of deep fake applications-videos, images, and audio clips created using artificial intelligence to appear real-which are the latest medium for cybercrime (Vassist & Krishnan, 2022). There are many social applications and social networking sites that have enabled individuals to produce digital content and even manipulate its visual and audio content. Despite this, modern digital media, such as visual and audio recordings, are still trusted by many users, as the content circulating in audio and video form refers definitively to its owner, and there is no doubt that this visual or audio content not reflected the truth and reality (Hancock & Bailenson, 2021).

Experts in this field have pointed to the inevitability of the spread of deep fake applications in the near future, as it is now possible to produce fake content using a mobile phone through the Reface application or other applications that have become widespread and accessible to everyone (Magharia, Alaa El-Din, 2023).

This study will be divided into two sections, in the first section, we will examine the forms of attacks using deep fakes and their components, in the second section, we will examine how to combat deep fake crimes, as follows:

SECTION 1: FORMS OF ATTACKS USING DEEP FAKES AND THEIR COMPONENTS

With the development of artificial intelligence tools capable of creating images and videos on a large scale, such as DALLE-3 and Sora, a new phenomenon has emerged: deep fake, which are images or recordings that have been convincingly altered and manipulated to distort someone's image as doing or saying something that was not actually done or said. Although deep fake have opened up creative possibilities, particularly in the fields of marketing and entertainment, they can be misused for harmful purposes that affect individuals and private and public institutions.

1. Forms of Deep Fake Attacks (Deep Fake Crimes)

There are many types and forms of deep fake crimes, which can be divided into two categories: those targeting individuals and private institutions, and those targeting public institutions.

1.1. Deep Fake Attacks Against Individuals and Private Institutions

There are certainly acceptable uses for deep fake technology, such as its use in satirical simulations of economic, social, and political situations, etc., or its use in historical entertainment to animate old photos and paintings or to recreate historical events. etc., or for historical entertainment, such as animating old photos and paintings, or recreating historical events. However, if deep fake violate a person's privacy or intellectual property rights, then a crime has been committed, the most prominent deep fake crimes include the following:

1.1.1. Deep Sexual Blackmail

This crime is committed against individuals, not institutions. Deep sexual blackmail refers to threatening or coercing someone to share nude or sexual images that have been altered using artificial intelligence applications, exploiting the victim's lack of technical skills to force them to comply with certain demands, such as paying a ransom, sharing sexual (intimate) images, or engaging in unwanted acts. Sexual blackmail occurs in a variety of forms (Blancaflor, Eric. et al, 2024), including cyber bullying, real-life sex, cybersex, online dating, sex trafficking, online sexual exploitation of minors, and computer hacking (Abdul Moneim, Mahmoud, 2022). Sexual blackmail can cause serious harm, and reporting it and seeking help remain very low due to shame and fear of the perpetrator threatening to publish the video or images with false content (Alana, Ray & Nicola, Henry 2024).

In accordance with this, the Jordanian Court of Cassation ruled that: "... The complainant remained in contact with the defendant on his phone number for a week., he will help her with recruitment and sent her photos of a person in military uniform, he asked her for a personal photo and personal documents and requested 500 dinars for recruitment purposes..,.then the defendant told her that he had hacked into her device and taken photos of her, and threatened her with them, saying that the person was demanding money to stop the threats, the complainant refused to give him the money, he then asked her to message him on Facebook and created an account under her name,

she communicated with him from that account, and he told her that he would send her private photos and videos. He sent her photos and videos fabricated with artificial intelligence in indecent positions, he threatened to publish these photos and videos if she did not give him 500 or have sex with him, and threatened to publish them on the group or company where she works and on her family's group..." (Decision No. 3421/2022, Zarqa Court of First Instance in its capacity as an appellate court).

1.1.2. Deep Fraud

This crime affects individuals and institutions, as traditional systems based on conventional rules are no longer sufficient to defend against deep fraud, which involves deceiving customers into agreeing to fraudulent transactions. Fraudsters are already using artificial intelligence (GenAI) for more complex fraud, especially when criminal human expertise is combined with artificial intelligence.

With the proliferation of banking applications on smartphones, the risk of deep fake fraud has increased, although banks implement effective, multi-layered security measures to protect their applications from various cyber-attacks, fraudsters have managed to circumvent these defenses by sending modified images using deep fake technology using artificial intelligence, thereby breaching the banking institution's multi-layered security system. Attackers have been able to acquire the victim's digital identity through various illicit channels, such as malware, social media, and the dark web. They have manipulated the image on the ID-changing features such as clothing and hairstyle—and used the fake image to bypass the banking institution's verification systems (Huang, Yuan, 2025).

Cybercriminals can use deep fake technologies to impersonate senior executives during phone calls or video conferences (sometimes called "voice phishing"), convincing others of their authority. They can then obtain confidential information or even persuade individuals to transfer large sums of money, insurance companies may be targeted with deep fake-generated images attached to claims. For example, in early 2020, voice deep fake technology was famously used in a 35$ million bank fraud in Hong Kong, a bank manager received a call and several emails from a company manager he had apparently spoken with previously. The manager claimed that his company was about to be acquired and needed a 35 $ million transfer to complete the transaction. The bank manager recognized the man's voice, believed everything was in order, and complied with the payment, of course, the person who called the bank manager and sent the emails was not the one who claimed to be the fraudster (https://www.kyriba.com/blog/fraud).

1.1.3. Deep Fake

Fake videos or audio recordings can spread inauthentic, false, or defamatory information about individuals and organizations, potentially damaging the trust of stakeholders and the wider public. In the age of social media, such content can spread rapidly (Al-Hakim, Rabab, 2025). For example, by circulating fake clips of executives announcing a company's financial status, upcoming mergers, product launches, and marketing materials, or making derogatory remarks or inaccurate political statements, criminals can capitalize on subsequent fluctuations in stock prices, in addition to damaging a company's reputation.

These tactics can also be used by competitors to cause stock price volatility and deter investors, as well as by other countries to undermine the economy. Similarly, malicious actors may attempt to damage a company's reputation by spreading fake clips about environmental damage, poor labor practices, defective or dangerous products, or inappropriate behavior by executives (https://kpmg.com/xx/en/our-insights)

1.1.4. Digital Identity Management

With the increasing realism of AI-generated audio, video, and images, cybercriminals are exploiting these technologies to impersonate individuals, falsify authentication systems, and access sensitive information without authorization. This growing threat is forcing individuals and organizations to reconsider how they verify a user's digital identity and secure their systems. Deep fake threats to identity and access management. AI-generated fake content has the potential to manipulate trust, destabilize the privacy of individuals and organizations, and deprive them of their rights (Al-Hakim, Rabab, 2025). For example, a manipulated video of a CEO or privileged user, created by artificial intelergence , could grant access to secure systems, highlighting the imminent threat to secure identity environments. Identity and Access Management (IAM) systems rely on trust models that authenticate users based on unique identifiers, such as facial or voice recognition. These deep fake undermine trust, weaken confidence in authentication systems, and expose organizations to increased risks of fraud and unauthorized access (https://identitymanagementinstitute.org/).

This is why deep fake-based digital impersonation poses a particular problem for identity and access management (IAM) professionals. Traditional

security controls that rely on static identifiers, such as passwords, are ineffective against these advanced attacks. Advanced identity and access management solutions must include multi-factor authentication (MFA) and real-time behavior analysis to distinguish authentic users from impostors.

1.2. Deep Fake Attacks Against Public Organizations

Deep fake crimes are not limited to attacks on private individuals and institutions; they also pose a threat to public institutions. This is what we will now explore in this article about the most significant deep fake crimes against public institutions.

1.2.1. Political Deep Fake

Deep fake and other synthetic media are used for a variety of purposes, from entertainment and education to fraud, however, politically oriented deep fake are a particularly worrisome use (Tulga, Ahmet, 2025). Recent examples include the use of deep fake to criticize political figures such as Donald Trump, Joe Biden, Emmanuel Macron, Nancy Pelosi, Vladimir Putin, and Volodymyr Zelenskyy, accusing politicians of sexual scandals (Walker, Christina, et al., 2024). Deep fake have also been used to influence voter turnout and even influence geopolitical events such as war in Gaza. A prominent example of this is that a doctored video depicting an explosion at the Pentagon caused a sharp decline in the US stock market (Sorkin, A., R. et al. 2023).

Thus, political content can be used to produce fake events that incite real political divisions within society, potentially fostering democratic decline, undermining trust in media and government institutions, fostering widespread uncertainty, inciting intolerance and violence, undermining public health, and providing new tools for disinformation campaigns (Walker, Christina, et al. 2024).

1.2.2. Deep Fake Against Journalism and The Media

Deep fake technology poses a serious challenge to media integrity, creating an environment where it is difficult to distinguish between real and fake content (Fitzgerald, Laura, 2025). The ability to produce highly convincing, albeit entirely fake, images, videos, and audio clips undermines public trust in the media, leading to widespread skepticism about the credibility of the content they view. Social media has undoubtedly become one of the primary sources people turn to for news of all kinds, and thus has become the primary means used by deep fake criminals to broadcast and disseminate fake content (Al-Mugharih, Alaa El-Din, 2023). This naturally threatens the integrity of the media and journalism, by increasingly undermining trust in news organizations and established media sources, as well as spreading misleading and disinformation (Hendrickson, Lauren, 2025).

A real-life example of deep fake in the media is a fake White House tweet in 2013. A fabricated tweet from a hacked Associated Press (AP) Twitter account (Steven C. Johnson, 2013) falsely reported explosions at the White House and claimed that President Obama had been injured. This misinformation led to widespread panic and a drop in trading in the US stock market (Lu Wang, et al., 2013). Although the truth was quickly revealed, the event highlighted the devastating impact that even a single piece of fabricated information can have on public confidence and financial markets.

1.2.3. Deep Fake Against the Criminal Justice System

Deep fakes technology users can be divided into two groups: the malicious group, which seeks to deceive the court by presenting forged evidence, and the justice group, which seeks to expose this deception and identify the forged evidence and exclude it from the evidence or disproven evidence of a crime.

During litigation, courts must consider how to evaluate and accept digital evidence that may have been influenced by deep fake. This evidence-which often includes video footage, audio recordings, or images—plays a crucial role in trials by influencing judges' decisions. The increasing sophistication of technology has led to the emergence of deep fake that are difficult to distinguish from genuine material (AlMazrouei, Noor 2024).

In application of this, the Jordanian Magistrates' Court ruled: ". After examining all the documents in this case, the court finds that the facts of this complaint are summarized as follows: The defendant posted on his personal Facebook page that anyone wishing to obtain travel visas to a country... could contact him via his Messenger. Several individuals of different nationalities contacted him, and he sent photos of a visa for a country... certified by an embassy... in Jordan. In addition,... he also sent photos of conversation between himself and the ambassador of a country... in Jordan. This was done by placing a photo of the ambassador on his phone and creating a fake conversation between him and the ambassador. It was found that all of these documents and photos were forged and false, in order to attract the largest number of people to obtain the visa..." (Decision No. 2113/2023, East Amman Magistrates' Court).

Therefore, it can be said that manipulated media can be used to create convincing but false narratives, which may exonerate the guilty or convict the innocent. These effects are particularly worrisome in the context of cyber-evidence-based crime proof, as they may create convincing false narratives that can be used to falsify evidence. Indeed, the mere possibility of their existence may cast doubt on the validity of legitimate evidence.

1.2.3. Deep Fake Against State Security

Deep fake pose a threat not only to specific individuals or entities, but also have the potential to harm state security both internally and externally. The threats posed by deep fake are systemic dimensions, they may include distorting democratic discourse on important political issues; manipulating with elections; eroding trust in important public and private institutions; deepening and exploiting social divisions; harming specific military or intelligence operations or capabilities; and threatening the economy, and harming international relations. For example, fake videos may show government officials receiving bribes, displaying racism, or meeting with spies or criminals, inciting public outrage. A fake audio clip may promote a candidate's criminal behavior on the eve of an election. A fake video may depict emergency officials "announcing" an imminent missile strike on the homeland or an emergency pandemic in a city, causing panic among citizens (Bobby & Danielle, 2019).

2. Elements of Deep Fake Crimes

In addition to the legal element, the crime of deep fake must also have a material and a mental element, these two elements are the subject of our current study.

2.1. The Material Element

Forgery crimes require tangible, positive actions and behaviors. The deep faker must engage in actions and movements that create a tangible external impact on the victim's psyche, assets, or reputation, or cause widespread harm to public and private institutions, for a deep fake crime to be considered material, the following elements must be present:

2.1.1. Criminal Behavior

This is represented by the external physical activity that constitutes the crime, represented by the perpetrator's full willful use of a deep fake application to design and produce fake content after having collected the necessary information and data to produce the content, then provides the deep fake applications with this information and issues electronic commands to produce the content. He then proceeds to send and circulate the content via social media or various websites on the internet, or use it to obtain a material or moral benefit in an illegal manner - as previously stated - especially since it is inconceivable that this type of crime would occur through negative behavior, such as the legally responsible person's failure to perform his duties (Al-Najjar, Sahar, 2024).

It is noted that the nature of criminal behavior in this type of crime may take several forms, as follows: The crime may take the form of a temporary criminal behavior that begins and ends immediately, such as deep fraud crimes, where the perpetrator uses fake content to trap the victim and obtain money, the crime may also take the form of an ongoing crime, beginning with the creation of the fake content and continuing to circulate it online. In these cases, the perpetrator's behavior continues for a long time, as they require negotiations with the victim, such as blackmail, porn revenge, or defamation of reputation, in addition to the material damage and loss of trust in public institutions, which may continue for a period of time in deep fake crimes against the state (Al-Hakim, Rabab, 2025).

2.1.2. Criminal Consequences

There is no doubt that the consequences of criminal behavior in deep forgery are serious and dangerous, in crimes targeting people's reputations, the victim suffers psychological distress and anger as a result of the act of deep fake. He may also lose his money through blackmail or fraud using deep fake, in particular, deep fake may lead to the deterioration of relationships and trust between individuals and private or public institutions, or to material losses, causing serious damage to state functions and disrupting public order and security in the state and confidence in its institutions (Al-Mughira, Alaa El-Din, 2023).

It is noted that deep fake crimes result in both public and private harm, public harm refers to harm to the state's interests and the undermining of confidence in its various institutions, such as harming members of the legislative, judicial, or executive authority, thereby jeopardizing state security, private harm refers to the harm that directly affects the victim and the indirect harm that befalls the victim and their family as a result of the suffering incurred by the dissemination of fake content (Al-Hakim, Rabab, 2025).

2.2. The Moral Element

The second element of deep fake crimes is the

moral element, which is based on demonstrating the criminal intent to commit the crime with intent, to achieve this, two elements must be established: knowledge and will.

2.2.1. The Element of Knowledge

Knowledge in criminal intent means that the perpetrator must be fully aware that the act they are committing is a crime punishable by law and be aware of the nature of their words and actions at the time of committing it, as it is legally unacceptable to use ignorance of the law as an excuse. Therefore, in order for criminal liability to be established, the person must be aware of what he is doing, that his action is against the law, and that he is heading towards committing a deep fake crime. The perpetrator must be aware that what he is doing is a fake using one of the deep fake technology applications of a person's images and voices with the aim of generating the fake clip without the consent of the owner of the original content or the person whose identity is being faked (Maktouf; Ashour, 2025).

2.2.2. The Element of Will

Will with criminal intent means that the individual perpetrator's intention is directed, voluntarily and freely, towards committing the act of deep fake to create a fake image or video without obtaining the content owner's permission. This is regardless of whether the act is intended to achieve financial gain, take revenge on the victim, or achieve personal goals (Al-Mughira, Alaa El-Din, 2023).

SECTION TWO: CONFRONTING DEEP FAKE CRIMES

Many countries find themselves in a race against time to issue legislation and regulations specific to deep fake to prevent or limit its negative uses, undoubtedly, combating d fake deep fake crimes is a joint effort that requires the concerted efforts of governments, the companies producing and developing this technology, and the role of society. Accordingly, the confrontation will be examined from a legal and technical perspective (the use of artificial intelligence technologies).

1. Legal Confrontation

Most countries around the world have primarily relied on issuing specific laws to combat deep fake, such as the Cybercrime Law and the Deep fake Law.

1.1. Legal Confrontation Through Cybercrime Law

Most countries around the world have issued specific laws to criminalize cybercrimes. For example, the UAE legislator issued Law No. 34 of 2021 to Combat Rumors and Cybercrimes. It is noteworthy that it did not explicitly mention deep fakes, but it did mention them indirectly in Article (16), which states: "Anyone who possesses, acquires, prepares, designs, produces, imports, makes available, or uses any information program, information technology device, passwords, symbols, or uses encryption with the intent to commit any of the crimes stipulated in this decree shall be punished." Articles (23 and 24) also indirectly mention deep fakes if the subject of the attack is crimes of incitement that affect state security or promote sedition and harm national unity. It is also inferred from the context of Article (42) of the same law that extortionist acts involving deep fakes are criminalized. Finally, Article (44/5) of the same law criminalizes misinformation crimes resulting from deep fakes.

As is the case in Jordan, Cybercrime Law No. 17 of 2023 was issued, It is noteworthy that the Jordanian legislator indirectly referred to one of the deep fake crimes in Article 2/20 of this law, stating: "Anyone who uses an information network, information technology, an information system, a website, or a social media platform to compile, modify, or process a recording, image, scene, or video that a person is keen to preserve and not show to the public, with the intent to defame, offend, or gain a benefit from it, shall be punished." An analysis of the text reveals that the legislator criminalized and punished some forms of deep fake crimes, such as extortion and deep pornographic revenge, but did not criminalize other attacks, such as deep fakes, deep fraud, and others. It goes without saying that while the advanced texts can be used to criminalize some forms of deepfake crimes, they fall short of providing comprehensive texts that address all aspects of the illegal use of deep fake applications. Furthermore, the advanced laws do not address criminalizing companies that produce deep fake technology or service providers, nor do they address the circulation or re-dissemination of fake content.

1.2. Legal Confrontation Through a Special Law on Deep Fake

Some countries have not only issued a cybercrime law to combat certain deep fake attacks, but have also issued a specific law to combat deep fake attacks. For example, the People's Republic of China is among the first countries to issue a number of laws regulating artificial intelligence in general, and deep fake technology in particular. In 2023, the Information Security Administration, in cooperation with the

Ministry of Industry and Technology and the Ministry of Public Security of China, issued a 25-article system called the "Deep fake Internet Information Services Management Regulations." One of the most prominent provisions of this system prohibits any organization or individual from using deep fake services to produce, copy, publish, or transmit information prohibited by laws and administrative regulations, such as endangering national security and interests, harming the nation's image, violating the public interest, disrupting the economic and social order, violating the legal rights and interests of others, or spreading false news (Article 6 of the system).

The system also stipulates a number of obligations for deep fake service providers, the most important of which is the responsibility of the deep fake service provider to ensure the security and integrity of users' information and data, register them under their real names, and prevent fraud (Article 7 of the system). The system also requires the service provider to verify the identity of deep fake users (Article 9 of the system). Furthermore, the service provider is required to take immediate measures in the event of discovering fake content that violates Chinese law, including refuting the content, keeping a record of that content, and reporting it to the competent authorities (Article 11 of the system).

It is noteworthy that despite the comprehensiveness, objectives, and quality of the formulation of this system in protecting against deep fake, it faces problems related to its implementation mechanism and difficulty in interpreting it, which exposes it to criticism.

2. Confrontation Using Artificial Intelligence Applications and Electronic Platforms

2.1. Confronting Deep Fake Applications with Artificial Intelligence

There is an ongoing race between deep fake applications and deep fake detection applications. This means that AI-based detection methods must improve to control sophisticated malicious deep fake applications. Deep fake applications involve a combination of advanced generation techniques, strategic content manipulation, and sophisticated training methods to create increasingly difficult-to-detect deep fake applications (Babaei, Reza, et al. 2025).

The solution has therefore been to use hybrid applications for deep fake detection, combining deep learning applications, such as CNNs and RNNs, with traditional signal processing applications. CNNs are used to capture spatial features in images, while RNNs focus on the temporal aspects of videos. These are all coupled with AI applications that detect inconsistencies in lighting, shadows, and other physical cues (Rana, M. et al. 2022).

It is worth noting that there are several AI-powered hybrid applications that can be used to detect deep fake, for example, an attention-based facial manipulation detection model combines spatial domain features from semantic facial segmentation with frequency domain features via discrete Fourier transform to enhance generalization (Chen, Z; Yang, H. 2020). Another model based on multimodal detection analyzes visual and audio components to identify inconsistencies, such as mismatches in lip movements and speech (Mittal, T; et al. 2020).

However, hybrid applications may not be sufficient, as attackers can continually update deep fake techniques based on the latest detection methods and combine different evasion techniques, ensuring their content remains undetectable, such as adversarial attacks, which involve subtle modification of input data, such as images or videos, to deceive detection algorithms (Juefei-Xu, F; et al. 2022).

In conclusion, the rapid advancement of deep fake applications is constantly outpacing detection applications, as new methods emerge, the effectiveness of current detection algorithms is decreasing, with the quality of deep fake videos approaching a level where they are almost indistinguishable from real videos, this requires concerted efforts to combat deep fake by developing technical and legal regulatory frameworks.

2.2. Countering Deep Fake Actions by Online Platforms

Deep fake applications have become a real and growing threat to organizations and individuals, from impersonating executives to fake product advertisements, they can cost organizations millions of dollars in fraud, reputational damage, and legal repercussions. Cybercriminals have long attempted, using phishing and "fake boss" scams, to trick users into revealing sensitive information. These scams are often carried out using fake email accounts, which are sometimes easy to detect. However, with deep fake applications, cybercriminals now have the ability to deceive even the most cautious and discerning organizations.

Therefore, online platforms on which fake content is disseminated must remove it. On May 19, 2025, President Trump signed the bipartisan "Tools to Address Known Exploitation Through the Installation of Technical Deep Fakes on Websites and Networks" Act. The Act defined the term "covered platforms" as including public websites, online

services, and mobile applications that (i) primarily provide a forum for user-generated content, or (ii) are primarily designed to disseminate non-consensual intimate visual imagery, covered platforms do not include broadband internet service providers, email services, online services, or websites that offer pre-screened content where the content is not user-generated but is curated by the provider (Stuart D. Levi Mana Ghaemmaghami, 2025).

Covered platforms must establish a clear and accessible mechanism for individuals to notify the platform of intimate visual depictions or deep fakes and request their removal. Article 4 of the above law stipulates: "Any person who (a) shares deep fake videos, or (b) shares or threatens to share real intimate visual depictions of an adult, shall be punished by fines (which, under the Anti-Unfair Trade Practices Act, may include civil fines, injunctive relief, and consumer damages) and imprisonment for up to two years. Anyone who intentionally threatens to share deep fake videos shall be punished by fines and imprisonment for up to 18 months." Article 5 of the same law also stipulates: "Any person who (a) shares deepfake videos, or (b) shares or threatens to share real intimate images of a minor, shall be punished by fines and imprisonment for up to three years. Anyone who intentionally threatens to share deep fake videos of a minor, shall be punished by fines and imprisonment for up to 30 months." We note that the US legislature did not exempt online platforms from criminal liability for deep fake applications, and the penalties imposed were somewhat deterrent.

2. CONCLUSION

In conclusion, we affirm that deep fake applications can open new and innovative horizons in the world of communication, but at the same time, they pose serious threats, their use has rapidly increased, necessitating the development of comprehensive legislation and standards to regulate these applications. In the absence of such legislation, their misuse could expose individuals, institutions, and financial systems to grave risk and undermine trust in digital environments. Therefore, this study reached several conclusions and recommendations, the most important of which are summarized below.

First: Results

1. The illegal use of artificial intelligence in deep fake applications is a criminal phenomenon that has caused significant harm to individuals, institutions, and countries.
2. The Cybercrime Law does not specify all the illegal uses resulting from the use of deep fake applications, although the legislature did include some of them in an implicit text. We hoped that our legislature would learn from the Chinese and American experiences in this regard.
3. The existence of tools to combat the illegal use of deep fake content, based on legal text, and the ability of online platforms to confront this type of attack.

Second: Recommendations

1. 1.We recommend that the Jordanian legislature explicitly criminalize deep fake content that threatens the security of national security, financial institutions, and individuals.
2. We also recommend that online platforms be held accountable for not placing a digital watermark on a fake video, image, or audio, indicating that the content is fabricated, consequently, failing to do so constitutes a crime punishable by law with imprisonment, a fine, or both.
3. Require technology companies that produce deep fake applications to include, among their application features, information about the criminal and civil liability stipulated in the law in the event of an attack on others.
4. This study demonstrates that the Chinese legislature has not limited itself to traditional or electronic laws to combat the deep fake phenomenon, believing that these laws are inadequate to effectively combat a technology that could be used negatively in an unprecedented manner. Chinese law plays a significant role in preventing the production of deep fakes for criminal purposes by activating the role of service providers and obligating producers to take the necessary measures to detect fake content. We, in turn, urge the national legislature to draft a specific law on the use of this technology, specifying the penalties that could result from its negative use, and imposing obligations on producers and service providers to prevent and remove fake content.

REFERENCES

Alana, Ray & Nicola, Henry (2024). Sextortion: A Scoping Review, Author information, 2024 Sep 25;26(1):138–155. 10.1177/15248380241277271.

AlMazrouei, Noor (2024) Deepfake Dilemmas: Navigating the Realism of AI-Generated Media. https://trendsresearch.org/insight/deepfake-dilemmas-navigating-the-realism-of-ai-generated-media/ 19.9.2025 تاريخ الدخول.

Babaei, Reza, et al. (2025) Generative Artificial Intelligence and the Evolving Challenge of Deepfake Detection: A Systematic Analysis. *J. Sens. Actuator Netw.* 2025, *14* (1), 17; https://doi.org/10.3390/jsan14010017

Blancaflor, Eric. et al, (2024) Deepfake Blackmailing on the Rise: The Burgeoning Posterity of Revenge Pornography in the Philippines

Bobby Chesney & Danielle Citron, (2019), Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, California Law Review, Volume 107.

Chen, Z.; Yang, H. Manipulated face detector: Joint spatial and frequency domain attention network. *arXiv* 2020, arXiv:2005.02958. [Google Scholar]

Deepfake Risks to Identity and Access Management, https://identitymanagementinstitute.org/. 2.9.2025.

Deepfake threats to companies, https://kpmg.com/xx/en/our-insights/risk-and-regulation/deepfake-threats.html ,13.8.2025.

Fitzgerald, Laura,(2025) The Impact of Deepfakes on Journalism, https://www.pindrop.com/article/impact-deepfakes-journalism/.17.9.2025 تاريخ الدخول

Hancock & Bailenson. The Social Impact of Deepfakes. Cyberpsychol Behav Soc Netw 2021 Mar;24(3) pp: 149-152. DOI: 10.1089/cyber.2021.29208.jth

Hendrickson, Lauren. (2025) How Do Deepfakes Affect Media Authenticity? https://www.identity.com/deepfake-ai-how-verified-credentials-enhance-media-authenticity/ تاريخ الدخول 17.9.2025

Huang, Yuan (2025) Deepfake Fraud: How AI is Deceiving Biometric Security in Financial Institutions, https://www.group-ib.com/blog/deepfake-fraud/ 11.8.2025.

Juefei-Xu, F; et al. Countering malicious deepfakes: Survey, battleground, and horizon. *Int. J. Comput. Vis.* 2022, *130*, 1678–1734. [Google Scholar] [CrossRef]

Lu Wang, et al (2013), Fake Post Erasing $136 Billion Shows Markets Need Humans. https://www.bloomberg.com/news/articles/2013-04-23/fake-report-erasing-136-billion-shows-market-s-fragility.17.9.2025 تاريخ الدخول

Mittal, T; et al. (2020) Emotions don't lie: An audio-visual deepfake detection method using affective cues. In Proceedings of the 28th ACM International Conference on Multimedia, Seattle, WA, USA, 12–16 October 2020; pp. 2823–2832. [Google Scholar]

Rana, M. et al. 2022. Deepfake detection: A systematic literature review. *IEEE Access* 2022, *10*, 25494–25513. [Google Scholar] [CrossRef]

Sorkin,A,R. et al. [2023]. An A.I.-Generated Spoof Rattles the Markets.*The New York Times*.

Steven C. Johnson. (2013) False White House tweet exposes instant trading dangers, April 24, 2013. https://www.reuters.com/article/us-usa-markets-tweet-idUSBRE93M1FD20130423/

Stuart D. Levi Mana Ghaemmaghami 2025, 'Take It Down Act' Requires Online Platforms To Remove Unauthorized Intimate Images and Deepfakes When Notified. https://www.skadden.com/insights/publications/2025/06/take-it-down-act تاريخ الدخول 22/9/2025.

The Threat of Deep fake Frauds in Payment, https://www.kyriba.com/blog/fraud-evolution-and-the-threat-of-deepfakes/ 12.8.2025.

Tulga ,Ahmet,(2025) The Malicious Exploitation of Deepfake Technology: Political Manipulation, Disinformation, and Privacy Violations in Taiwan ,Global Taiwan Brief Vol. 10, Issue 9 https://globaltaiwan.org/wp-content/uploads/2025/05/GTB-10.9-PDF.pdf

Vasist, P., & Krishnan, S. (2022). Deep fakes: An Integrative Review of the Literature and an Agenda for Future Research. Communications of the Association for Information Systems, 51, pp-pp. https://doi.org/10.17705/1CAIS.05126

Walker, Christina, et al,2024, Merging AI Incidents Research with Political Misinformation Research: Introducing the Political Deepfakes Incidents Database, arXiv:2409.15319v1 [cs.CY] 05 Sep 2024https://arxiv.org/html/2409.15319v1

Al-Hakim, Rabab Mustafa, Legal Aspects of Deepfake, Journal of Jurisprudential and Legal Research, Al-Azhar University/Damanhour, Volume 48, Issue 48, pp. 2669-2742. 10.21608/jlr.2025.346070.1598

Abdel-Hakim, Rabab Abdel-Moneim, Legal Aspects of Deepfake, Journal of Jurisprudential and Legal Research, Damanhour University, Issue 48, pp. 2678-2742.

Abdel-Moneim, Mahmoud Salama, (2022) The Crime of Revenge Pornography Using Deepfake Technology and Criminal Liability Therefor, Journal of Law for Legal and Economic Research, Alexandria University, Volume 2, Issue 1, pp. 366-485. 10.21608/LALEXU.2022.266089.

Mughayra, Alaa El-Din, (2023), "Artificial Intelligence Crimes and Ways to Confront Them: Deepfake Crimes as a Model," International Journal of Law, Qatar University, Volume 13, Issue 2, pp. 127-162.

Maktouf, Sabreen; Ashour, Amil (2025), "Substantive Provisions of the Crime of Deepfake and Its Legal Treatment: A Comparative Study," Ashur Journal of Legal and Political Sciences, Volume 2, Issue 2, pp. 79-119.

Al-Najjar, Sahar (2024), "Criminal Response to Crimes Resulting from the Use of Deepfake Technology," Journal of Legal Sciences, University of Baghdad, Volume 39, Issue 2, pp. 575-633. DOI: https://doi.org/10.35246/9sjgyd13