The Associated Challenges with the Legal Regulation of Deepfake "A "comparative analytical legal study

Saddam Faisal Kokez Al-Mihimdi
Professor of Private Law. College of Law / University of Fallujah – Iraq

DOI: https://doi.org/10.31918/twejer.2584ELI.20

Published:2/11/2025

Abstract

The technologies of deepfake have caused multiple legal problems, some of which are related to the use of these technologies, and some of which are related to the violation of the right to privacy, as few countries adopt legal legislation regulating the legal situations related to deepfake, in an attempt to overcome the risks associated with the spread of deepfake technologies. Therefore, it is necessary to clarify the legal problems and challenges associated with the use of deepfake technologies, with a focus on the role of active platforms on the network in restricting and removing fake content, and clarifying the role of legislation in addressing the negative effects of deepfake content.

***Keyword**: Deepfake, Generative Adversarial Networks, Digital Environment, Right to Privacy, Detection of Forgery.*

The Associated Challenges with the Legal Regulation of Deepfake

"A comparative analytical legal study"

Saddam Faisal Kokez Al-Mihimdi
Professor of Private Law. College of Law / University of Fallujah – Iraq
Email: saddam.faisal@uofallujah.edu.iq

1. Introduction:

Until this article is written, there is no international consensus regarding legal regulations for deepfake technology. However, discussions concerning potential global regulatory frameworks began during the Innovation Dialogue Conference organized by the United Nations Institute for Disarmament Research (UNIDIR) in 2021. At this event, participants articulated clear strategies to address the rising issue of deepfakes and explored how such technology could be harnessed positively both now and the future, (UNIDIR, 2021). There was a collective acknowledgment of the urgent need for legal measures governing deepfakes and transparency about associated content due to their implications on trust and security at both national and international levels.

The investigation into the difficulties related to the legal oversight of deepfakes begins with a fundamental inquiry: How can society address the challenges posed by technology within artificial intelligence systems, and assess whether existing legal frameworks are adequate for regulating content generated by these technologies? This encompasses both the techniques employed in creating deepfake materials and the nature of the content disseminated post-manufacturing.

Given the variety of mechanisms used in producing deepfakes, their applications have expanded considerably. The accessibility of digital tools that facilitate this production has made it increasingly challenging to identify such manipulated content and differentiate it from authentic material. Consequently, the proliferation of deceptive media over recent years has resulted in diminished trust concerning most visual or audio data circulated on internet connected platforms.

The main question of this paper is, how developed nations like the United States & United Kingdom regulate deepfakes legally. And how we will explore the appropriate legal framework in Iraq & other Arab countries may adopt for Deepfakes regulating.

To structure our research effectively, we will organize it into three main sections.

First, will focus on The Deepfake Define & its techniques.

Second, The legal issues & the challenges of the deepfake content spread:.

Third, The Legislative organization of the deepfake.

Lastly, In conclusion, recommendations aimed at enhancing approaches related to this study topic may be proposed based on our findings.

2. The Deepfake Define & its Techniques:

Deepfake refers to: the generation of artificially created content where lip movements in edited videos are synchronized with an audio track" (Shruti Agarwal et al., 2019). It represents a type of composite media, characterized by digital alterations (Brandon, J. 2018). Its applications extend beyond merely substituting one person's likeness for another (Witness Org, 2020). This technology has the potential to alter human features through advanced deep generative techniques.

Common methods used in deepfakes involve software based on Generative Adversarial Networks (GANs), which incorporate sophisticated artificial intelligence technologies (Matthew U., 2016, p. 359). One notable application supported by deep learning is that of creating synthetic images and videos that closely resemble real individuals; these outputs can be indistinguishable from authentic ones. The production process typically employs substantial amounts of image and video data to develop models that exhibit realistic characteristics. Consequently, concerns have been raised regarding the implications of deepfakes for global security due to their capacity to fabricate speeches or actions attributed to world leaders (T. Hwang, 2020).

The peculiar aspect is that, at times, fake videos gain considerable traction across various social media channels. This phenomenon appears to stem from the fact that such content entertains a significant number of users. Furthermore, this situation highlights the rapid dissemination of deepfake material and underscores the urgent need for legal measures to hold offenders accountable (Bode, L 2021).

Additionally, it should be emphasized that advancements in deepfake technology have progressed remarkably fast; consequently, ordinary viewers can no longer easily discern between genuine and fabricated visuals. Over the past decade, three distinct categories of counterfeit content have emerged (T. Ramluckan, 2024, p. 282):

1. **Face swapping**, which is replacing one person's face with another person's face, whether in a photo or video content (Siwei Lyu. 2018).

2. **Lip sync & facial expressions:** This technique involves lip syncing by making a person speak in another person's voice, so that it appears as if he is saying something that is not in the original audio or video content.

3. **Puppetry Technique:** The term "puppetry technique" describes the act of simulating movements in an artificial manner, allowing one individual's actions to align with those of another. Although some deepfake materials might have been created using traditional methods involving visual effects or computer graphics, modern technologies employ more advanced techniques. These cutting-edge methods utilize deep learning frameworks such as autoencoders and generative adversarial networks (GANs), which are widely used within the field of artificial intelligence (Ming-Yu Liu et al., 2021).

3. The legal issues & the challenges of the Deepfake content spread:

The rise of deepfake technologies presents a substantial obstacle for law enforcement agencies globally, prompting the need for diverse regulations regarding their application. This development raises multiple concerns related to the legal structures that oversee deepfakes. Consequently, this chapter will be divided into two separate parts: the first part will clarify the legal issues tied to deepfake forgery, while the second part will tackle the difficulties involved in identifying and substantiating occurrences of such fraudulent content.

3.1: Issues related to the legal regulation of Deepfake

Deepfake technology is not a new technology, although it has become difficult to detect with the naked human senses, because it uses and applies powerful digital techniques of machine learning and artificial intelligence, which can easily manipulate or create visual and audio content with the intention of deception.

Here it must be said that from a legal standpoint, democratizing deepfake technology causes many difficulties related to law enforcement, including:

Firstly: In legal contexts, both investigation and trial processes tend to extend beyond the typical duration due to defendants consistently asserting that the evidence against them is either false or fabricated. This defense strategy necessitates further inquiries and heightens reliance on witnesses and expert testimonies during court proceedings. Consequently, this

situation may result in procedural complications since it becomes evident that an individual is gathering information—an acceptable action and subsequently creating entirely counterfeit materials from it. The activities of this individual remain ambiguous, as they possess the fake content on their devices before uploading and disseminating it online through specific platforms or intermediaries, thereby making it accessible to the public.

Criminal liability can be established if this person has knowledge or should have knowledge about—their actions; however, determining legal accountability isn't always straightforward. Identifying the perpetrator typically requires collaboration with internet service providers, which poses challenges because these entities often hesitate to assist without a court order due to obligations regarding confidentiality and privacy for those who shared such material publicly. As a result, two separate lawsuits are frequently necessary: one aimed at locating and identifying the offender while another seeks prosecution against them.

Additionally, if there's a demand for removing content from various platforms or any existing copies elsewhere, supplementary lawsuits must also be initiated. Thus we could see instances where multiple cases arise concurrently, potentially leading up to third or fourth suits—which regrettably consume more time, financial resources, and energy than many individuals can afford.

Secondly, the likelihood of judges being swayed by fabricated content may rise, as they could mistake it for genuine material and regard it as original. This is particularly relevant given the increasing prevalence of fake materials in relation to authentic ones that appear credible; conversely, a judge might perceive certain evidence as potentially fraudulent when, in fact, it is legitimate. The widespread accessibility of data-driven technologies, such as deepfake technology, presents significant challenges to the existing legal framework. Currently, this framework tends to emphasize regulating these technologies after their development or distribution rather than addressing their creation and possession beforehand. As a result, many aspects remain unregulated while scrutiny predominantly focuses on content validation at a later stage (P. Korshunov & S. Marcel 2019).

Third: The possibility of harming the convicted person, as innocence cannot always be proven, which causes the judge to issue a judicial decision stating conviction, as a result of the judge being mistakenly convinced of fake content as being original.

Fourth: Unfortunately, in certain types of crimes, simply disseminating (false) information can significantly influence public sentiment and lead to widespread disapproval,

particularly concerning politically motivated offenses. This reaction can occur even without a legal verdict from the courts (Bart van der Sloot et al., 2021, pp. 3-4). From our perspective, one major factor contributing to the proliferation of deepfakes is the easy availability of software and technologies capable of generating such content. The constant connectivity provided by the internet allows individuals anywhere in the world to produce altered videos, images, and audio recordings that may seem authentic to many viewers. Additionally, these creations can be shared effortlessly with vast audiences globally. This situation presents various legal challenges related to establishing accountability for those responsible for creating this misleading content; therefore, it necessitates revisions in current legislation aimed at regulating this technology while ensuring fundamental state rights are upheld—including freedom of expression (Diakopoulos & Johnson, 2021). Many politicians have also fallen victim to deepfake manipulations.

Fifth: Any law intended to ban the use of deepfakes and mitigate their impact on political figures, candidates, or individuals in general necessitates a comprehensive examination. This should encompass a thorough revision of relevant legal texts to ensure alignment between these punitive measures and the constitutional provisions that safeguard freedom of expression within the jurisdiction where these issues arise.

Sixth: Regarding the legal ramifications of utilizing deepfakes for malicious intent, a significant issue arises due to the intricacies involved in managing deepfake content. For instance, while satirical deepfakes may be permissible, those that are harmful should face restrictions. It is essential to create a clear distinction between deepfakes used for artistic expression and those deployed with malicious aims. This differentiation is crucial for enabling effective prosecution against individuals who exploit deepfake technology for criminal activities. However, such prosecutions necessitate compelling evidence demonstrating not only the use of harmful content but also establishing proof of criminal intent.

These prerequisites present substantial challenges both for lawmakers and professionals engaged in criminal investigation and evidentiary processes; acquiring adequate proof to illustrate an individual's criminal intentions can prove difficult. Conversely, art forms like satire typically possess inherent meanings that do not align with illicit objectives (Farish, K., 2022).

The primary legal challenge associated with analyzing deepfake content lies in enforcing current laws alongside developing new legislation encompassing various regulatory measures

tailored specifically to this emerging threat. In this context, several barriers impede effective legal oversight over the realm of deepfakes.

Seventh: Some actions taken by creators of deepfake material might infringe on intellectual property rights, particularly through the unauthorized use of a specific domain name or trademark within that content. To mitigate potential legal repercussions associated with disseminating deepfake material, various online platforms like YouTube and Facebook have pledged to follow several policies. They have also implemented numerous technical solutions and established certain legal frameworks to regulate the content they distribute deemed as deepfakes.

Eighth: The possibility of problems arising from conflicts of laws, due to the cross-border nature of digital data-based technologies. The disputing parties are often subject to multiple legal systems, and thus the tendency to apply one law and leave the other is a matter of suspicion that cannot be ignored.

Ninth: The emergence of the problem of conflict of jurisdiction in disputes related to deepfakes, as it is very difficult to impose and enforce the rules of jurisdiction, fairly and appropriately, on the parties to the dispute located in other countries.

Tenth: The multiplicity of parties to the conflict, and the complexity and intertwining of relationships between them, as there is often a complex network of parties involved in it, whether in terms of production or distribution of deepfake content, where all of this can create problems in proving partial liability before the criminal judge, and even civil liability as well.

3-2: Challenges associated with detecting Deepfake content:

There are numerous challenges related to identifying counterfeit content and providing evidence of it. This encompasses the detection of private violations due to deep forgery, as well as the techniques used to expose fake content. Consequently, this section will be divided into two parts: the first will focus on detecting private violations resulting from deep forgery, while the second will explore methods for revealing fake content. As follows:

3-2-1: Detecting Deepfake Violations:

Within the framework of legal treatments for the problems that followed the emergence and spread of deepfake content, the matter has developed to a level where this content began to take on a criminal legal description, and causes many damages related to defamation of reputation and honor, as the design of deepfake technologies and programs (deepfakes) is

compatible with the possibility of being used by weak-willed people to harass, intimidate and degrade people. Threatening and blackmailing them.

Often leads to the creation and dissemination of misleading and false data and information. Creating confusion about important issues related to political financial, economic and even security fields.

First: The relative ease of circumventing legislative systems. It is often easy to circumvent the rules of a particular jurisdiction, as happens, for example, by accessing the Internet using VPN connection technology.

Second: The rapid development of technologies related to deepfakes, and therefore the special legal rules regulating the technology are quickly becoming outdated.

Third: It is challenging to ascertain which technologies involved in deep forgery are subjected to legal regulation based on the existing legislative framework. This difficulty arises because creating a precise legal definition for deep forgery technology could hinder the effective enforcement of such laws. A restrictive definition may open up significant opportunities for undesirable applications or adaptations of technologies that do not conform to this narrowly defined scope, while overly broad definitions can undermine the value and beneficial use of legitimate or constructive technologies.

Fourth: What adds complexity to the issue of deep forgery is that addressing the negative consequences associated with the misuse of these applications remains a prolonged endeavor. Furthermore, detecting such forgeries incurs significant costs, in addition to efforts required for their removal. The situation is exacerbated by the fact that deep forgery often eludes detection by unaided human observation, despite its widespread dissemination and accessibility. This presents a formidable challenge in combating deep forgery; consequently, the potential for preemptive detection poses an immense difficulty if not outright impossibility.

Fifth: The confusion caused by deepfake content. as deepfake technologies began to reveal new possibilities that contribute to the development of the video industry, which includes producing videos at a low cost, as well as creating interactive videos depicting deceased celebrities, but they soon became bad applications due to the possibility of being used to create offensive materials for children, and deepfake technology can be misused in illegal situations, including producing fake pornographic videos (S Samuel. 2019). Spreading fake news. Blackmail and financial fraud, misleading the public in order to destabilize the political

process. Or promote hate speech. and undermine governance systems in democratic countries. (T. Ramluckan, 2024, p. 282)

3-2-2: Methods for detecting fake content

What increases the problems of detecting fake content is that fake videos or images have become increasingly widespread in our world today. but the methods of detecting them are still limited. Early attempts at detecting deepfakes have relied on methods based on:

1. **Using handcrafted methods.** Which are methods based on handcrafted features. Which mostly work on detecting images generated by generative adversarial networks (GANs). The problem here is that this method cannot be generalized to detect fake materials, because GANs In constant development (X. Xuan & All, 2019) .

The image preprocessing step, using Gaussian blur and Gaussian noise. removes the low-level high-frequency evidence of the GAN images. Which increases the pixel-level statistical similarity between real and fake images. (Ying Zhang & All, 2017)

This method allows the forensic classifier to learn more intrinsic features of the images, which has the ability to generalize better than previous image forensic methods.

2. **Deep feature-based methods :**

Many appealing applications are utilized in video montage to alter faces and enhance images, including those found on identification cards. This technique is often exploited by cybercriminals to compromise identities or bypass private authentication measures for accessing secure systems. Their intention may be to gather sensitive information, unlawfully access data, or infiltrate secured areas that rely on biometric locks.

In this context, deep learning methods and generative adversarial networks (GAN) are employed to differentiate authentic facial images from fabricated ones. This approach poses greater challenges for forensic analysis as it can maintain the original pose, facial expressions, and lighting conditions of the photographs. (Chih-Chung Hsu et al., 2020)

3. **Visual effects within the video frame :**

Another approach to identifying deepfakes involves analyzing the individual frames of videos, focusing on visual artifacts present within these frames. This analysis aims to extract distinctive characteristics from the original video. These features are then processed by either

a deep or traditional classifier to differentiate between genuine and fabricated videos (K. Simonyan & A. Zisserman, 2014).

Deep classifiers often produce deepfake videos that exhibit limited features, necessitating careful adjustments in scaling, rotation, and cropping to align with the original composition. Consequently, discrepancies in resolution between the altered face and its surrounding environment can signal forgery (Kaiming He et al., 2016).

Additionally, deep learning techniques can be employed for detecting traces of facial manipulation created by algorithms associated with deepfake generation (S. Lyu, 2018; Y. Li).

4. Using block chain technology to distinguish real videos from fake ones:

Can be utilized to identify deepfakes through the application of technology such as blockchain and smart contracts, which assist users in recognizing counterfeit videos. This approach relies on a fundamental principle that asserts videos can only be deemed authentic if their sources are traceable. In technical terms, every video present within the digital landscape is associated with a smart digital contract linking it back to its original version. Each original video maintains a connection to any derivative content produced from it within a hierarchical framework. Throughout this chain, users have the ability to revert any video back to its source and confirm its validity by accessing the origin via the smart contract tied to the initial recording—this remains feasible even after multiple copies have been made. A key aspect of smart contracts is their unique fragmentation capability within file systems across digital environments; this feature facilitates secure storage for both videos and their accompanying metadata in a decentralized manner that ensures accessibility and availability of content.

5. Deep learning techniques that can detect Deepfakes :

As the spread of fake content has become faster thanks to the development of social media (A. Zubiaga. & All, 2018). it is no longer difficult to spread deepfakes to a large audience. In order to cause the intended harm. People who create deepfakes using maliciously intended materials only need to deliver them to targeted audiences. as part of their disruptive strategy without using social media. (O. Giudice & All, 2021)

It is noteworthy here that As the quality of feepfake content has increased. The performance of techniques and methods for detecting forgery has also improved. but they still

need more improvement. What is optimistic here is that what artificial intelligence breaks can be fixed by artificial intelligence as well (L. Floridi, 2018).

6. Proposed method for detecting Deepfake:

In this research, we suggest that deepfake detection techniques should be incorporated into the operational software of distribution platforms, such as social media networks. This integration aims to enhance their effectiveness in addressing the pervasive influence of deepfakes by implementing automated sorting or filtering systems utilizing reliable detection methods. Such measures could help reduce the prevalence of deepfake content on these platforms (R. Chesney & D.K. Citron, 2021).

Additionally, adjustments to the legal obligations governing technology companies responsible for these platforms may be necessary. These modifications would require prompt removal of deepfakes to lessen their impact. Furthermore, watermarking technologies could be integrated into devices used for creating digital content; this would prevent alterations through metadata manipulation and ensure proper documentation regarding authenticity details—like time and location—of multimedia materials alongside verified testimony (R. Chesney & D.K. Citron, 2021).

However, it is important to note that this proposal remains under development. While employing deepfake detection tools is vital, comprehending the underlying intentions behind users' postings also holds significance—it often outweighs concerns about the deepfake itself—and necessitates evaluating users within their specific social contexts when a deepfake emerges or is identified while considering who disseminated it and what was asserted regarding its target (M.Read., 2019).

Consequently, establishing both validity and reliability in forensic analyses of scrutinized videos or images must occur before they can serve as evidence in judicial proceedings. This process fundamentally requires meticulous documentation at every stage executed by forensic specialists along with clear explanations concerning how outcomes were derived (M Iuliani et al., 2018).

Ultimately, our study underscores a crucial aspect related to methodologies for detecting deepfakes: these approaches should not confine themselves strictly to a defined set or group but instead recognize that current techniques are still evolving towards greater efficacy.

4. The Legislative organization of the Deepfake

At the level of domestic legislation, the positions of developed countries have varied in terms of the level of legislative regulation of deepfakery, as there is no legal regulation within the framework of comprehensive legislation that regulates deepfake technologies or the content associated with them.

Accordingly, we will divide the research in this section into four branches, in which we will address the legislative position in the United States, the People's Republic of China, the United Kingdom, and the European Union, as follows:

4-1: United States

To start, it is important to note that prior to the end of 2019, there was no comprehensive federal legislation in the United States specifically governing deepfakes or addressing the associated risks posed by such technologies. The initial steps toward establishing legal frameworks at the federal level occurred in December 2019 when Congress enacted the National Defense Authorization Act (NDAA). This included Section 5709, which mandated a report from the Director of National Intelligence concerning international government usage of deepfakes, their effectiveness in disseminating misinformation, and potential implications for U.S. national security (Mabunda, SM. 2021).

A significant critique of this legislation highlights its focus on regulating threats from foreign sources while neglecting issues stemming from domestic deepfake activities. In response to these gaps, several states have initiated efforts aimed at combating deepfakes within their jurisdictions. For instance, Texas passed SB 751 and California enacted AB 730 in 2019; both laws prohibit utilizing deepfakes for electoral manipulation.

Moreover, specific regulations targeting non-consensual creation and distribution of Deepfakes were established with Georgia's enactment of Law No. 337 SB and Virginia's passage of Law No. 1736 SB in the same year.

Additionally, New York State introduced Law S6829A in 2020 that grants individuals rights to pursue legal action against unauthorized sharing of Deepfake materials.

4-2: United Kingdom

Recently, the UK has enacted legislation that addresses deepfakes, notably through the Online Safety Bill 2023. However, critiques of this framework primarily center on instances involving pornographic video deepfakes. These situations are now regulated under Section 50 of the Online Safety Act, which serves as the main legal guideline for managing deepfakes in Britain.

Prior to 2023, there were no specific laws governing deepfake technology. Consequently, prosecutors faced significant challenges in establishing that an offender had malicious intent aimed at harming or inconveniencing victims; proving such intent is a formidable obstacle necessary for classifying an act as criminal.

When criminal intent can be demonstrated successfully by prosecutors, it may lead to a two-year imprisonment sentence for offenders. Conversely, if they cannot establish this element but prove that a misleading deepfake was produced instead, penalties could result in up to six months' incarceration for those responsible for creating harmful content.

Additionally, the UK's Online Safety Bill mandates service providers associated with deepfake materials to take full responsibility for confirming user identities and ensuring any potentially harmful or illegal content can be traced back to its source. A notable issue regarding the implementation of UK law appears rooted in its predominant focus on pornography; specifically highlighted within section 13(4) of the Act concerning adult content deemed detrimental.

1. Restrict users' access to such content;

2. 'Limited' recommendation and promotion of such content (T. Ramluckan, 2024, p. 286).

In light of this, the relevant authorities in the United Kingdom are emphasizing the protection of individuals, by making amendments to the country's Internet Safety Act, in a way that imposes a ban on deepfakes used in pornographic materials.

4-3: The Arab countries

In light of the current constitutional and legislative situation under the applicable Arab laws, the concept of the "right to privacy" remains an important basis for developing rules for criminalizing deep forgery. The recognition of the protection of the right to privacy is to protect individuals in terms of their characteristics, which include the individual's likeness, image, voice, and other distinctive personal characteristics. Freedom of expression and the right to

privacy are legally recognized in the constitutions and laws of Arab countries, while the use of deep forgery appears to violate this right. Including the current Iraqi Constitution of 2005, in Articles (17 & 38) thereof.

In Iraq, there is currently no specific legal framework governing deepfakes; instead, such matters are governed by general constitutional provisions and existing laws. Consequently, any limitations on the application of these technologies or bans on certain content would contradict the constitution's affirmation of an individual's right to manage their private information. Therefore, current legislation does not support claims that producing or distributing fake images is illegal. The principle of privacy remains a fundamental right protected by the constitution, which indicates that criminal liability cannot be imposed for creating or sharing deepfake material. However, it is still permissible to apply overarching principles from other areas, particularly those related to civil liability as outlined in civil law even if this content falls outside criminal law statutes (M Akram & All, 2020).

Conversely, several Arab nations have recognized the necessity for explicit legal regulation concerning deepfakes. For instance, Egypt was one of the initial countries in the region to introduce legislation addressing cybercrimes with Law No. 175 enacted in 2018 focusing on combating information technology offenses while UAE followed suit with Law No.(34) issued in 2021 targeting rumors and cybercrimes.

In contrast to these developments elsewhere within Arab jurisdictions like Egypt and UAE where regulations exist regarding digital misconducts including electronic blackmailing practices gaining traction recently; Iraq continues without definitive legislative measures aimed at tackling either deep forgery issues directly nor broader categories encompassing cyber-crimes comprehensively yet—instead resorting when necessary--to provisions under its amended Penal Code (No:111/1969) pertaining specifically towards threats defamation slander etc., assessing severity based upon context surrounding incidents occurring therein.

Given today's technological advancements coupled alongside increasing prevalence rates observed among various forms associated particularly via cyberspace usage—it becomes imperative urgently implement new comprehensive electronic crime laws outlining punitive measures clarifying investigative protocols establishing dedicated departments overseeing cybersecurity along ensuring accountability mechanisms remain active against offenders exploiting current gaps present due lack thereof prior enactments especially critical given ongoing inability address arising challenges posed through non-existence Electronic Crimes

Act presently available frameworks merely insufficient bridging disconnect between evolving nature modern criminal acts necessitating immediate reforms now viewed essential amidst pressures faced globally across societies adapting policies reflective realities faced today following emergence profound shifts resulting from rapid digitization trends highlighting how outdated traditional approaches must evolve accordingly rather than cling onto archaic systems established over five decades ago devoid contextual relevance considering absence concepts previously nonexistent till recent times such as both "cybercrime" “deepforgery” phenomena emerged only after significant transformations occurred latter half twentieth century onward(Human Rights Watch , 2012,p. 4).

While extant texts include penalties directed toward distribution child pornography they do not sufficiently delineate clear parameters differentiating genuine pornographic imagery versus altered representations created utilizing advanced techniques hence reinforcing urgency needed catch-up counterparts leading regulatory efforts seen developed Western states notably United States United Kingdom spearheading initiatives focused around legislations encapsulating nuances inherent within utilization emerging tech-driven capabilities expanding implications surrounding trustworthiness media landscapes wherein misinformation proliferates threatens undermine societal cohesion risking escalation tensions inciting hostility potentially even violent conflict scenarios exacerbated further enabled accessibility tools facilitating dissemination fraudulent outputs amplified social ramifications experienced increasingly owing widespread reach afforded platforms capable disseminating fabricated materials rapidly throughout public sphere .

Many appealing applications are utilized in video montage to alter faces and enhance images, including those found on identification cards. This technique is often exploited by cybercriminals to compromise identities or bypass private authentication measures for accessing secure systems. Their intention may be to gather sensitive information, unlawfully access data, or infiltrate secured areas that rely on biometric locks.

In this context, deep learning methods and generative adversarial networks (GAN) are employed to differentiate authentic facial images from fabricated ones. This approach poses greater challenges for forensic analysis as it can maintain the original pose, facial expressions, and lighting conditions of the photographs. (Chih-Chung Hsu et al., 2020)

5. Conclusion:

1. Deepfake is a complex process of fabricating and falsifying digital audio or video content, using advanced technologies used to deliberately falsify the truth, with the intent to defraud, defame or harm the targeted parties.

2. The spread of the negative use of deepfake technologies causes legal, political and social problems, and these technologies are constantly evolving, to the point where it is difficult in many cases to detect it, such that real content cannot be distinguished from fake.

3. One of the solutions that can be adopted to contain the problem of the spread of deepfake materials is to integrate deepfake detection methods into the operating programs of distribution platforms, such as social media, to increase its effectiveness in dealing with the wide impact of deepfake, by adopting the method of sorting or automatic filtering using effective detection methods, which can be implemented on these platforms, to reduce the deepfake content available on them.

4. The legal system in the country must be developed, by amending legislation and adopting specific regulations that protect the right to identity, while supporting freedom of expression and publication and the right to privacy.

5. Due to deepfake, we can face countless problems at all levels, and this emphasizes the urgent need to develop a comprehensive legislation or regulatory framework that must cover all aspects of deepfake technology and its areas of use, and the legal treatment must be comprehensive, meaning that it must cover all aspects of deepfake, whether related to the technologies used in it, or the fake content produced by these technologies, which represents the harmful content published in the digital environment.

6- Recommendations:

1. We propose coordinating efforts at the international level, or at least at the Arab level, to develop a model law that would be a guiding law for the national legal regulation of deepfakes, criminalizing malicious deepfake acts, and determining the resulting criminal consequences, provided that the legal regulation aims to enhance confidence in Internet content at the international level, in a way that makes it safer and more reliable for everyone.

2. We propose adopting the best strategy for detecting, removing, and preventing the spread of deepfakes, which can be done not only through anti-deepfake technologies, but also

through direct human evaluation of the context of the digital content, which is included in the content under scrutiny, and preventing or restricting the possession of technologies and software related to deepfakes to specific entities, except with a license from a specialized official body.

3. The necessity of expediting the enactment of a law for crimes related to deep forgery in Iraq and Arab countries that have not yet adopted a special legislation to govern deep forgery, establish legal conditions in terms of criminalization and punishment, and determine through it the legal procedures related to proving and investigating it, and work to establish national agencies specialized in electronic crimes and cyber security.

7- References:

Arkaitz Zubiaga, Ahmet Aker, Kalina Bontcheva, Maria Liakata, and Rob Procter. Detection and resolution of rumours in social media: A survey. ACM Computing Surveys (CSUR), 51(2):1–36, 2018 .

Bart van der Sloot, Yvette Wagensveld and Bert-Jaap Koops, THE LEGAL CHALLENGES OF A SYNTHETIC SOCIETY. Tilburg Institute for Law, Technology, and Society. November 2021.

Bode, L. Deepfaking Keanu: YouTube Deepfakes, platform visual effects, & the complexity of reception. Convergence: The International Journal of Research into New Media Technologies 27 (4) 135485652110304-934. (2021)

Brandon, J. "Terrifying high-tech porn: Creepy 'deepfake' videos are on the rise". Fox News. Archived from the original on 15 June 2018. Retrieved 05 October 2023

Chih-Chung Hsu, Yi-Xiu Zhuang, and Chia-Yen Lee. Deepfake image detection based on pairwise learning. Applied Sciences, 10(1):370, 2020 .

Diakopoulos, N., & Johnson, D.. Anticipating and addressing the ethical implications of Deepfakes in the context of elections. New Media & Society, 23, 2072–2098. (2021)

Farish, K. Political Deepfakes: social media trend or real threat? https://www.dacbeachcroft.com/en/gb/articles/2022/september/political-Deepfakes-social-media-trend-or-genuine-threat (2022)

Human Rights Watch. All rights reserved. Printed in the United States of America, ISBN: 1-56432-913-5, Copyright © 2012. Cover design by Rafael Jimenezm, https://www.hrw.org/reports/iraq0712ar.pdf.

Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and PatternRecognition, pages 770–778, 2016 .

Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. arXiv preprint arXiv:1409.1556, 2014 .

Luciano Floridi. Artificial intelligence, Deepfakes and a future of ectypes. Philosophy & Technology, 31(3):317–321, 2018 .

M. Read. Can you spot a deepfake? Does it matter? http://nymag.com/intelligencer/2019/06/how-do-you-spot-a-deepfake-it-might-not-matter.html, June 2019 .

Mabunda, S.M. The South African Legislative Response to Cybercrime. PhD Thesis-University of the Western Cape. https://etd.uwc.ac.za/bitstream/handle /11394/8693/mabunda_m_law-2021.pdf?sequence=1&isAllowed= y .

Massimo Iuliani, Dasara Shullani, Marco Fontani, Saverio Meucci, and Alessandro Piva. A video forensic framework for the unsupervised analysis of MP4-like file containers. IEEE Transactions on Information Forensics and Security, 14(3): 635–645, 2018 .

Matthew U. Scherer, REGULATING ARTIFICIAL INTELLIGENCE SYSTEMS: RISKS, CHALLENGES, COMPETENCIES, AND STRATEGIES, Harvard Journal of Law & Technology, Vol: 29, N: 2, Spring 2016, p.358-359 .

Ming-Yu Liu, Xun Huang, Jiahui Yu, Ting-Chun Wang, and Arun Mallya. Generative adversarial networks for image and video synthesis: Algorithms and applications. Proceedings of the IEEE, 109(5):839–862, 2021 .

Mohammed Akram Younus and Taha Mohammed Hasan.Effective and fast deepfake detection method based on haar wavelet transform. In International Conference on Computer Science and Software Engineering (CSASE), pages 186 -- 190.IEEE, 2020 .

Oliver Giudice, Luca Guarnera, and Sebastiano Battiato. Fighting Deepfakes by detecting GAN DCT anomalies. arXiv preprint arXiv:2101.09781, 2021 .

Pavel Korshunov and S´ebastien Marcel. Vulnerability assessment and detection of deepfake videos. In 2019 International Conference on Biometrics (ICB), pages 1–6. IEEE, 2019 .

R. Chesney and D. K. Citron. Disinformation on steroids: The threat of Deepfakes. https://www.cfr.org/report/Deepfake-disinformation-steroids, October 2018.

S Samuel. A guy made a deepfake app to turn photos of women into nudes. It didn't go well. https://www.vox.com/2019/6/27/18761639/ai-deepfake-deepnude-app-nude-women-po .

Shruti Agarwal, Hany Farid, Yuming Gu. Mingming He, Koki Agano, and Hao Li. Protecting world leaders against Deepfakes. In Computer Vision and Pattern RecognitionWorkshops, volume 1, pages 38–45, 2019 .

Siwei Liu. Detecting 'deepfake' videos in the blink of an eye. http://theconversation.com/detecting-deepfake-videos-in-the-blink-of-an-eye- 101072, August 2018 .

T. Hwang. Deepfakes: A grounded threat assessment. Technical report, Center for Security and Emerging Technologies, Georgetown University, 2020 .

T. Ramluckan, Deepfakes: The Legal Implications, University of KwaZulu-Natal, South Africa, Proceedings of the 19th International Conference on Cyber Warfare and Security, ICCWS 2024.

United Nations Institute for Disarmament Research (UNIDIR). Innovations Dialogue on Deepfakes, Trust and International Security (Geneva 2021).

Witness Org. "Prepare, Don't Panic: Synthetic Media & Deepfakes". Archived from the original on 2 December 2020. Retrieved 05 October 2023 .

Xinsheng Xuan, Bo Peng, Wei Wang, and Jing Dong. On the generalization of GAN image forensics. In Chinese Conference on Biometric Recognition, pages 134–141. Springer, 2019 .

Ying Zhang, Lilei Zheng, and Vrizlynn L.L. Things. Automated face swapping and its detection. In The 2nd International Conference on Signal and Image processing (ICSIP), pages 15–19. IEEE, 2017 .

Yuezun Li and Siwei Lyu. Exposing deepfake videos by detecting face warping artifacts. arXiv preprint arXiv:1811.00656,2018 .