Webology (ISSN: 1735-188X)
Volume 19, Number 2, 2022

Deepfakes: Criminalization And Legalization Analytical Descriptive Study

Muaath Sulaiman Al-Mulla

Associate Professor of Criminal Law - Faculty Member at Kuwait International Law School, State of Kuwait https://orcid.org/0000-0002-1043-852X

Abstract: Deepfake is an artificial intelligence application that allows users to change digital content such as photos, video clips and audio recordings to produce a new photo, clip, or recording that contradicts the truth included in the original content. The problem is reflected in that this application is available to everyone without any restrictions which affected the idea of truth and its denial due to the high accuracy of falsifying the original content. All without any discrimination, may download it through electronic stores for free. Undoubtedly, this constitutes a serious danger to the rights of others as well as an objective and procedural challenge before the criminal justice agencies. Therefore, we shed light in this research on the nature of this application, its advantages and disadvantages, identified the features of the challenge posed by this application from a criminal perspective, and reviewed the position of the American legislator until providing conclusions and recommendations. This required following the descriptive approach to present the idea and mechanism of the application of the Deepfake and the analytical approach to study its problems and clarify some of the related punitive legislations.

Keywords: Keywords: Deepfake Application - Artificial Intelligence - Crime - Punitive Legislation.

Introduction

The Fourth Industrial Revolution achieved a brilliant success in bringing about a qualitative leap in the operation of various electronic systems from being mere tools that perform automated operations to do specific tasks programmed by humans to intelligent systems that simulate the human mind and its various patterns by virtue of artificial intelligence technology and its algorithms that feed on big data so that the machine learns and trains to do it without any interference from its creator. The equation in this environment is the greater the amount of data obtained by the application, the

better the performance, the higher the quality of the content, and the more realistic the output.

A deepfake application, the so-called “Deepfake” is among the most important applications of artificial intelligence which is based on deep learning and machine learning. Reportedly, features of appearance of this application emerged in 1997 through Video Rewrite program that process digital photos and videos in a fake way[(1)]. This application had been evolving until the term "Deepfake" appeared in 2017 after this technique was used to replace the face of a celebrity with the face of a pornographic film actor, and in 2018, the application became freely available to all via the Internet.[(2)]. It has become a feature that’s used to repel the truth. We support what some have said **"Deepfake is where the truth dies... Technology can make it appear as if a person said or did anything."**[(3)]. The American National Security Agency (NSA) noted: **"Massive use of fake news could eventually put an end to the truth."**[(4)].

Therefore, the importance of this research paper is reflected in that it clarifies the nature of this application, which has recently spread among ordinary users and without distinction between them, as they are allowed to download the Deepfake program on their devices through well-known electronic stores due to the advantages that this application enjoys in some scientific fields. However, arguably, its disadvantages overwhelm those advantages because of the absence of self-censorship controls over the use of this application and the controls for its development by various technology companies. Accordingly, the problem lays in in the absence of the boundaries between

(1) Christoph Bregler, Michele Covell, Malcolm Slaney, Video Rewrite: Driving Visual Speech with Audio, Proceedings of the 24th annual conference on Computer graphics and interactive techniques - 1997, Interval Research Corporation, P1.
www.semanticscholar.org/paper/Video-Rewrite%3A-driving-visual-speech-with-audio-Bregler-Covell/3a78995510cf33edf0ee4265abe23ffdc55986cb
(2) Erik Gerstner, Face/Off: “DeepFake” Face Swaps and Privacy Laws, DEFENSE COUNSEL JOURNAL, Volume 87, No. 1. 1, P1.
www.iadclaw.org/defensecounseljournal/faceoff-deepfake-face-swaps-and-privacy-laws/
Thanh Thi Nguyen, Quoc Viet Hung Nguyen, Cuong M. Nguyen, Dung Nguyen, Duc Thanh Nguyen, Saeid Nahavandi, Fellow, IEEE, Deep Learning for Deepfakes Creation and Detection: A Survey, P1. arxiv.org/abs/1909.11573
(3) Oscar Schwartz, You thought fake news was bad? Deep fake are where truth goes to die, Technology, The Guadian, 12 Nov 2018
https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth
(4) Michael Horowitz, Paul Scharre, Gregory C. Allen, Kara Frederick, Anthony Cho and Edoardo Saravalle, Artificial Intelligence and International Security, Center for a New American Security’s series, July 2018.
www.cnas.org/publications/reports/artificial-intelligence-and-international-security

the correct or permissible use of this application and the misuse that may be subject to criminalization whenever it constitutes an attack on the rights of other people.

In this research paper, we have asked several questions: What is the concept of work of this application? What are its advantages and disadvantages? What is the impact of its misuse on the rights and interests of others? What is the attitude of the punitive legislation therefrom? In addition to other questions that may place us in front of the objectives of the study.

We considered that the descriptive and analytical approaches meet the requirements of the study. The descriptive method was used to describe the concept of work of this application in order to identify its advantages and disadvantages, and the analytical method was used to study the dimensions of these disadvantages and their impact on rights, as well as to review the attitude of punitive legislation towards their misuse, with a view to some conclusions and recommendations. This research is divided into three sections as follows:

First Section: What is Deepfake Application?

Second Section: Misuse and Consequences of the Deepfake Application.

Third Section: Efforts of Punitive Legislation in the Confronting Deepfake.

First Section

What is Deepfake?

Preface and Classification:

The idea of forgery refers to the use of information technology tools and programs to manipulate digital content such as images, video clips or audio recordings to delude the viewer or listener with the truth of what he is watching or listening to.

In our expression of the nature of this digital fake, we wonder why it is described as deepfake? What are its types? What are the fields of its application?

First: Concept of Deepfake Application

Deepfake Application operation is represented in creating fabricated digital images, video and audio using artificial intelligence "deep learning and machine learning" [(5)],

(5) Artificial Intelligence is a technology that relies on computer properties so that the machine can simulate human mental abilities and its work patterns thanks to the data processed thereby, including the ability to learn, deduct and react to situations that are not programmed into the machine. Therefore, artificial intelligence has been defined in many definitions that focus on the ability of the machine to learn and independence of performance. For more

so that the content becomes as close as the truth in which it deceives our auditory and visual senses with its nature but its content is fabricated. Photo manipulation is a very old method that appeared with the emergence of photographic techniques and this method was used by Abraham Lincoln to looks more handsome as a president. It was also used by Joseph Stalin and Mao Zedong to eliminate political opponents. The Laboratory of Federal Institute of Technology in Lausanne stated: "Today, a single image is enough for an accurate faking process."(6).

This process is considered very complex as the application uses two separate sets of algorithms working together: the first algorithm is called the (Generator) and works to produce fake content, while the second is an algorithm called the (Discriminator) because it tries to determine if the video is real or fake. Both are competing, if the second algorithm was able to report that the video is fake, the first algorithm tries again. The competition continues until the first network produces content that the second network classifies it as real. They are known as Generative Adversarial Networks (GANs).

Another technique is also reliable by using artificial intelligence via (Autoencoder). This tool is commonly used in the technique of alteration or replacement of faces in photos and videos. This is done through training the encoder using thousands of images that include facial shots of the two people targeted by the technology. This tool extracts key features and finds similarities between those images. Then, the decoder rebuilds the image and replaces faces(7).

---

details about the idea of artificial intelligence, machine learning, search algorithms and other technical concepts, refer to Dr. Mahmoud Tarek Haroun, Introduction to Artificial Intelligence, 1st ed., 2019, The Academic Science House, Cairo, p. 22 et seq. Wathiq Ali Almoussawi, Artificial Intelligence between Philosophy and Concept, Part One - 1st ed., 2019, Dar Al-Ayyam, The Hashemite Kingdom of Jordan, Amman, p. 45 et seq. See also:

Nils J. Nilsson, The Quest for Artificial Intelligence, A History of Ideas and Achievements, 2010, Cambridge University Press, NY, USA, p53. See Also: Jerry Kaplan, Artificial Intelligence: What everyone needs to know, 2016, Oxford University Press, UK, P7.

(6) Sara Ibrahim, an article published on the swissinfo.ch titled: How deepfakes are impacting our vision of reality, August 25, 2021. See the following link:
https://www.swissinfo.ch/ara/

(7) Thanh Thi Nguyen, Quoc Viet Hung Nguyen, Cuong M. Nguyen, Dung Nguyen, Duc Thanh Nguyen, Saeid Nahavandi, Fellow, IEEE, Op, cit, P4. And Robail Yasrab , Wanqi Jiang and Adnan Riaz, Article Fighting Deepfakes Using Body Language Analysis, MDPI journal/forecasting- 2021-3, Basel, Switzerland ,P306.
https://www.mdpi.com/2571-9394/3/2/20

See the following article in MIT Technology Review website: What is deepfake technology?

Accordingly, it can be said that the Deepfake is a behavior that includes tampering or manipulation of digital content (photo, video, voice recording) by a program implemented by a human or a smart machine based on artificial intelligence and machine learning, so that the features of the content changed either by adding, deletion or modification and making whoever sees or hears it believes in its reality identity to the truth.

Second: Fields of Deepfake Application

from the above, it appears that the deepfake application depends on data that is voluntarily or selectively placed by Internet users, especially social networking websites, where participants have been uploading their photos, clips and comments to allow others to view them. This content, as some describe it, is the fuel of the twenty-first century(8) and it's considered the environment in which artificial intelligence technology and its various applications operate.

Deepfake depends entirely on visual content such as photos and videos by replacing individuals faces and placing them on other individuals or manipulating their faces by modifying facial expressions such as sadness, laughter or anger, and also the possibility of lip synchronization during the conversation, so that the words match what is visible in the image or clip. The texts in the image could be manipulated so that a date or times are added to the content where it appears as if the situation or event is new. This application may depend on the audio content, i.e., audio installation, and modify it by creating an audio file added to the person's image or by controlling the tone of the voice in the clip in which it appears.

All for demonstrating the feeling of the receiver or listener that the content is real while it's originally not real, or rather manipulated content. There are many positive uses for this application in many technical fields, which we summarize as follows(9):

---

https://technologyreview.ae/technodad/%D8%A7%D9%84%D8%AA%D8%B2%D9%8A%D9%8A%D9%81-%D8%A7%D9%84%D8%B9%D9%85%D9%8A%D9%82/
See also the following link at Wikipedia:
Wikipedia, 'Deepfake',
https://en.wikipedia.org/Deepfake

(8) For more details, please see Dr. Adel Abdelsadiq, Personal Data: The Struggle for "Oil" of the Twenty-First Century, Strategic Brochures, No. 287, Vol. 27, April 2018, Al-Ahram Center for Political and Strategic Studies (ACPSS), p. 17.

(9) Rod Ghammaghami and John Villafranco, Article: Deepfake Best Practices Amid Developing Legal Landscape April 16, 2021, Law360. Kelley Drye & Warren LLP,. New York.
https://www.kelleydrye.com/News-Events/Publications/Articles/Deepfake-Best-Practices-Amid-Developing-Legal-Land

Such as using it in the field of medical applications: For example, using it to protect the identity of whistleblowers or victims, creating audio files for those who have lost their speech due to tumors and cancerous diseases, using it in the advertising and movies industry, and using the application as a virtual assistant for customer service. Also, it could be used in different businesses.

Section Two:
Misuse and Consequences of the Deepfake Application

Preface and Classification:

The Deepfake App is like other digital applications, could be utilized - as we have seen - in many technical fields, but on the other hand, there are those who exploited its capabilities in a way that poses a real threat not only to individuals; but also to the security of nations. In this section, we try to find out what is meant by the misuse of this application and to clarify its seriousness.

First: Misuse of Deepfake Application

We mean using it in a way that is inconsistent with the proper use, and human beings have been used to, since the beginning of creation, employ modern or invented means to implement their illegal aims. It's well-known that criminals have benefited a lot from information technology tools as well as the Internet for its characteristics that contributed significantly in the development of the criminal phenomenon.(10)rather, they benefited greatly from its development in the era of the Fourth Industrial Revolution in which the development of technology tools had elevated to the fact that the machine performed tasks without any interference from the human being.

Nicholas Caporusso, Deepfakes for the Good: a Beneficial Application of Contentious Artificial Intelligence Technology, International Conference on Applied Human Factors and Ergonomics AHFE 2020: Advances in Artificial Intelligence, Software and Systems Engineering, P237.
https://www.researchgate.net/publication/342691593_Deepfakes_for_the_Good_A_Beneficial_Application_of_Contentious_Artificial_Intelligence_Technology

(10) Information technology crimes have many characteristics over traditional crimes, to the extent that the latter were developed after technical systems were employed to commit them. For more details on this, see, Osama Ahmed Almanasah and Jalal Mohamed Alzoubi, Electronic Information Systems Crimes, 2nd ed., 2014, Dar Al-Thaqafa for Publishing and Distributing, Hashemite Kingdom of Jordan, Amman, p. 95 et seq. See also in foreign jurisprudence:
Jonathan Clough, Principles of Cybercrime, 2ed- 2015, Cambridge University Press, UK, P5-9.

There is nothing wrong in saying that the rapid development in this world has made us lose control and follow-up the performance of users, as the proper use controls were completely absent and the ethics of developing tools were absent with it. Even the idea of preventive measures, the so-called "Information Security" or as sometimes being referred to as "Cyber Security", has become incapable of keeping pace with the development of crime in this era.

Deepfake is a model for smart cybercrime, and the more digital content and its reproduction, the higher the level of faking. If it's now possible to detect fake digital content such as a person's color change, irregular facial movement or other that suggests inaccuracy, thanks to artificial intelligence, machine learning and the data flow from users day after day across their different devices, fake digital content will become more realistic and thus it will be more difficult to detect because it appears as a real content. Adobe's natural language processing program "VoCo" can imitates sounds accurately as well as image recognition systems "ELMO" who learns to read chaotic data labels, and it will become able to compose. Also, "Face2Face" program through which faces could be manipulated in videos, photos, and other possibilities, we do not know what the future hides for us, especially regarding artificial intelligence technology.(11).

Second: Consequences of Misuse of This Application and Abuse Models

The tools of information technology and artificial intelligence allowed many attacks to be launched, which have become a real threat, not only to individuals; but also, to states, societies and justice. Deepfake Application is one of the applications that some have used to attack by falsifying the truth by fabricating digital content. We will divide our discussion according to the following order:

1. Impact Individuals Rights and Interests: Undoubtedly, falsifying and manipulating the digital content of individuals in a way that is different from the truth will negatively affect them as this constitutes an serious assault on their personal rights, as abusers can exploit this content, either with or without the consent of the owner.(12)An example of this is the attack on the right of the image, such as changing faces and replacing them with other faces, or tampering with the video clips. In addition, this attack may affect other rights, such as the right to be forgotten by recalling the old memory or the right of reputation and dignity if the image is tampered with in a way that discredits the owner such as the use of content in pornography or other practices that put its owner in contempt of society, and raise the level of bullying or blackmail.

(11) Flynn Coleman, A Human Algorithm: How Artificial Intelligence Is Redefining Who We Are, October 2019, Counterpoint Press, USA, p154.
(12) Rebecca Delfino, Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act, Fordham Law Review Volume 88 Issue 3 Article 2- 2019. P892.

Also, manipulation of digital content may also harm the commercial, intellectual, cultural or sports interests of individuals(13).

2. Influencing Public Opinion and Causing Destabilization of the Society and the State: The falsification of digital content may negatively affect national security, public opinion and misdirect it due to the dissemination of false or misleading news or information, in other words, rumors that harm national security(14). The most famous example that can be inferred is the interference in the conduct of the 2016 US elections when a large number of people believed that something is wrong about the Vatican's support for Donald Trump(15). There is no doubt that spreading fake news undermines the trust in the electronic media. Faking and dissemination of the content may also affect stock prices and the economies of countries and companies. Among the examples we infer from, the fabricated clip of the previous US president Donald Trump when he promised to impose or raise tariffs on steel imports. This clip has affected the company's stock prices(16).

3. Impact on the Course of Justice and Obliteration of Truth: Due to the potential manipulation of the digital content, Deepfakes Application constitutes a real challenge to criminal justice agencies(17). One of the thorny issues in this aspect is the difficulty of knowing who is criminally responsible for the behavior of manipulating digital content, especially if the crime was committed by a smart machine without human intervention, as well as the difficulty of proving whether there was an actual

(13) Data mining, storage or analysis algorithms are not only limited to drawing users' personality, but also, they target their personal interests by monitoring electronic behavior and how it is used for data in various fields, especially in personal aspects. See: Dr. Haitham Elsayed Ahmed Issa, Digital Diagnosis of the Human Condition in the Era of Data Mining through Artificial Intelligence Techniques According to the General Data Protection Regulation (EU) 2016/679 (GDPR), 1st ed., 2019, Arab Renaissance Publishing House, Cairo, p. 9. See also Dr. Mamdouh Abdelhamid Abdelmuttalib, Artificial Intelligence Algorithms and Law Enforcement, Edition 1-2020, Arab Renaissance Publishing House, Cairo, p. 9.
(14) Jack Langa, Deepfakes, real consequences: Crafting Legislation to combat Threats posed by Deepfakes. Boston University Law Review. Mar2021, Vol. Mar2021, Vol. 101 Issue 2, P770.
(15) Flynn Coleman, Op, cit, p154.
(16) Henry Ajder, Why Deepfakes Pose An Unprecedented Threat To Businesses, AI Business, 5/1/2019.
https://aibusiness.com/document.asp?doc_id=760904
(17) Hin-Yan Liu & Andrew Mazibrada, Special collection on Artificial Intelligence: Artificial Intelligence Affordances: Deepfakes as Exemplars of AI Challenges to Criminal Justice Systems, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2020, Viale Maestri del Lavoro , Torino - Italy, P63.

interference from the latter or not.[18]In the future, deepfake may also affect the value of the digital evidence drawn from the crime scene before the courts, especially since the development of this application is still present. While there are devices that actually detect fake content, the development of these devices is not compatible with the development of Deepfake Application. There is an urgent need to work on better means of detecting deepfakes" Facebook Chief Technology Officer Mike Schroepfe siad.[19].

Section Three
Efforts of Punitive Legislation in the Confronting

Deepfakes

Preface and Classification:

In view of the above, what is raised by the misuse of the Deepfake Application has been the subject of discussion and controversy in some legislations of countries whose policies ranged between relying on their laws to ensure confronting the misuse of deepfake and the need to introduce special legislation to confront it. Therefore, we have devoted this section to identify the conduct of the most important punitive legislation.

First: In India:

The Indian legislator has relied on the applicable laws without any need to introduce other special laws to counter the consequences of deepfakes, and the provisions of Articles 67 and (67)A and (B) of the Information Technology Act 2000 may be applied as acts of posting or transmitting pornographic content in electronic form were criminalized, Section 66(C) if the deefakes is conducted for identity theft and Section 66(D) if the deefakes is conducted for cheating or fraud. The provisions included in the Indian Penal Code may be also applied. Provisions of Section 500 on the offense of defamation may be applied in its general sense, knowing that defamation through image using information technology is criminalized in aforementioned Section 66 (A). The provisions included in Section 468 that penalize the act of forgery, and Section 124 on

(18) Dr. Ayman Mohamed Alasiouty, Legal Aspects of the Application of Artificial Intelligence, 1st ed., 2020, Dar Misr for Publishing and Distribution, Cairo, p. 140 et seq. See also in this connection:
Gabriel Hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer; 2015th edition, P47.

(19) ARIEL DAVIS, Deepfakes Aren't Very Good. Nor Are the Tools to Detect Them The winning detection algorithm from a Facebook-led challenge could spot about two-thirds of the altered videos, highlighting the need for improvement. 06.12.2020.
https://www.wired.com/story/deepfakes-not-very-good-nor-tools-detect/

hatred, contempt or sedition, may be applied. The provisions of Section 506 on the use of fabricated content to threaten or intimidate others[(20)].

Second: In the United States of America:

At the local legislation level, some local legislation of states have encountered acts of deepfake in a special scope, i.e., in the scope of a specific incident. In 2019, in California and Texas, the first two laws related to combating deepfakes during electoral process were issued. Under California Law, Section (AB730) prohibits manipulating the content of political candidates to the detriment of reputation of the candidate or to deceive the voter into voting for or against the candidate. This law is similar to what is stated in Section (255) of Texas Law, and some have criticized them for being inconsistent with the provisions of the First Amendment to the US Constitution regulating freedom of expression[(21)]. In Virginia, a law was passed in 2019 criminalizing the activities of publishing fake pornographic content when the intent is to coerce, harass, or intimidate someone in Section (18.2-386.2). In the same context, the State of New York has regulated a new law passed in 2020, specifically in Article (A08155). However, the latter is distinguished by its reliance on protecting the right of privacy. There are great efforts by legislators in other states to confront the deepfakes. At the federal level, deepfakes had been confronted as part of the mechanism regulating in the National Defense Authorization Act (NDAA), in which restrictions are imposed on its use. The federal legislator sees deepfakes as a problem related to national security.[(22)].

Third: In China:

The Chinese government passed a law entered into force as of January 1, 2020. It criminalizes all forms in which digital content is manipulated. This law states that all fake video clips, audio content, or content created with deep learning algorithms or virtual reality technologies must be classified by application providers. This law also obligates platform operators to determine to identify, mark or independently remove unspecified content. It also prohibited production and dissemination of fake news and

(20) Purvi Nema, Are Indian Laws Equipped To Deal With Deepfakes? JULY 19, 2020, The Journal of Indian Law and Society Blog (JILSBLOGNUJS). https://jilsblognujs.wordpress.com/2020/07/19/are-indian-laws-equipped-to-deal-with-deepfakes/#_ftn26

(21) Jack Langa,Op, cit, P786. See Also Matthew Feeney, "Deepfake Laws Risk Creating More Problems Than They Solve," released by the Regulatory Transparency Project of the Federalist Society, March 1, 2021. https://regproject.org/wp-content/uploads/Paper-Deepfake-Laws-Risk-Creating-More-Problems-Than-They-Solve.pdf

(22) Jason Chipman, Matthew Ferraro, Stephen Preston, First Federal Legislation on Deepfakes Signed Into Law, December 24, 2019, WilmerHale. https://www.wilmerhale.com/en/insights/client-alerts/20191223-first-federal legislation-on-deepfakes-signed-into-law

obliged the provider to delete it as soon as it was identified. This law is passed for the handling problems relating to intellectual property rights and image rights. It is worth noting that an internet company "Tencent" introduced an Anti-Deepfake program[23].

Fourth: In the European Union:

The European Union Code of Legislation is one of the most important codes that always seeks to face the challenges raised by modern technology, especially the General Data Protection Regulation (GDPR) No. 679/2016, which regulates the mechanism of data and other documents processing ensuring that user's rights in the digital environment is protected. Countering deepfakes is carried out within the framework of applicable laws. In the English Criminal Code, the Harassment Act 1997, the Defamation Act 2013 or other laws may be applied. In the French Penal Code of 1994 and as amended, the provisions included therein regarding the criminalization of manipulation of images or video clips through production or dissemination of content without the consent of the concerned person may be applied, as well as provisions related to identity theft and provisions criminalizing harm to internal security and so on. What distinguishes German law in this aspect is that is a special act was passed in 2017, aiming to combat misinformation and impose measures that limit illegal content by reporting and determining the responsibility of social media platforms towards illegal content[24].

Conclusion

At the conclusion of this research paper, we reached some conclusions and recommendations that we ask Allah, the Almighty to be useful and motivating in confronting crime disease.

First: Results:

1. Deepfake is a global phenomenon of very serious dimensions concerning the rights and interests of individuals and states.
2. The spread of misuse of deepfakes was due to the absence of controls over usage and mechanisms for its development, and its increasing danger was due to supporting it with artificial intelligence and machine learning technologies.
3. The rapid improvement of the application of deep forgery led to matching the real reality, which naturally affects the value of evidence in proof before the criminal courts.

(23) Julia Chen, deepfakes, September 2020. https://asiasociety.org/sites/default/files/inline-files/Final%20Deepfake%20PDF.pdf

(24) M. Huijstee, P. Boheemen, D. Das, L. Nierling, J. Jahnel, M. Karaboga M. Fatun. L. Kool, J. Gerritsen. Tackling deepfakes in European policy, July 2021.Panel for the Future of Science and Technology (STOA), the Directorate-General for Parliamentary Research Services (EPRS), P45. https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2021)690039

4. Arab criminal laws in particular have not yet understood that the ability of the smart machine in committing the crime of faking a content.

Second: Recommendations:

1. There is an urgent need to address criminal laws to counter deepfake activities, and to align these laws with the developments of artificial intelligence and machine learning technology. Criminal justice systems need to use this technology to confront the crime.
2. Confronting deepfake is based on digital content, so it is necessary to find technical means to ensure the detection of the nature of fake content and to inform its users to support confidence in the digital environment.
3. It's necessary to create a clear technical and ethical charters to deal with programmers and developers regarding the processing of digital content, as well as defining their responsibilities towards that.
4. It's necessary to cooperate with technology platforms and companies to limit the spread of fake content, which enhances the implementation of cyber security strategies.

References:

First: Arabic References:

Osama Ahmed Almanasah and Jalal Mohamed Alzoubi, Electronic Information Systems Crimes, 2nd ed., 2014, Dar Al-Thaqafa for Publishing and Distributing, Hashemite Kingdom of Jordan, Amman.

Ayman Mohamed Alasiouty, Legal Aspects of the Application of Artificial Intelligence, 1st ed., 2020, Dar Misr for Publishing and Distribution, Cairo.

Adel Abdelsadiq, Personal Data: The Struggle for "Oil" of the Twenty-First Century, Strategic Brochures, No. 287, Vol. 27, April 2018, Al Ahram Center for Political and Strategic Studies (ACPSS).

Mahmoud Tarek Haroun, Introduction to Artificial Intelligence, 1st ed., 2019, The Academic Science House, Cairo.

Mamdouh Abdelhamid Abdelmuttalib, Artificial Intelligence Algorithms and Law Enforcement, Edition 1-2020, Arab Renaissance Publishing House, Cairo.

Wathiq Ali Al-Moussawi, Artificial Intelligence between Philosophy and Concept, Part One - 1st ed., 2019, Dar Al-Ayyam, The Hashemite Kingdom of Jordan, Amman.

Haitham Elsayed Ahmed Issa, Digital Diagnosis of the Human Condition in the Era of Data Mining through Artificial Intelligence Techniques According to the General Data Protection Regulation (EU) 2016/679 (GDPR), 1st ed., 2019, Arab Renaissance Publishing House, Cairo.

Second: English References:

ARIEL DAVIS, Deepfakes Aren't Very Good. Nor Are the Tools to Detect Them The winning detection algorithm from a Facebook-led challenge could spot about two-thirds of the altered videos, highlighting the need for improvement. 06.12.2020.

https://www.wired.com/story/deepfakes-not-very-good-nor-tools-detect/

Christoph Bregler, Michele Covell, Malcolm Slaney, Video Rewrite: Driving Visual Speech with Audio, Proceedings of the 24th annual conference on computer graphics and interactive techniques - 1997, Interval Research Corporation.
www.semanticscholar.org/paper/Video-Rewrite%3A-driving-visual-speech-with-audio-Bregler-Covell/3a78995510cf33edf0ee4265abe23ffdc55986cb

Erik Gerstner, Face/Off: "DeepFake" Face Swaps and Privacy Laws, DEFENSE COUNSEL JOURNAL, Volume 87, No. 1. 1.
www.iadclaw.org/defensecounseljournal/faceoff-deepfake-face-swaps-and-privacy-laws/

Flynn Coleman, A Human Algorithm: How Artificial Intelligence Is Redefining Who We Are, Ocotber 2019, Counterpoint Press, USA. Gabriel Hallevy, Liability for Crimes Involving Artificial Intelligence Systems, Springer; 2015th edition.

Henry Ajder, Why Deepfakes Pose An Unprecedented Threat To Businesses, AI Business, 5/1/2019.
https://aibusiness.com/document.asp?doc_id=760904

Hin-Yan Liu & Andrew Mazibrada, Special collection on Artificial Intelligence: Artificial Intelligence Affordances: Deepfakes as Exemplars of AI Challenges to Criminal Justice Systems, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2020, Viale Maestri del Lavoro, Torino Italy.

Jack Langa, Deepfakes, real consequences: Crafting Legislation to combat Threats posed by Deepfakes. Boston University Law Review . Mar2021, Vol. Mar2021, Vol. 101 Issue 2.

Jerry Kaplan, Artificial Intelligence: What everyone needs to know, 2016, Oxford University Press, UK.

Jonathan Clough, Principles of Cybercrime, 2ed- 2015, Cambridge University Press, UK.

Michael Horowitz, Paul Scharre, Gregory C. Allen, Kara Frederick, Anthony Cho and Edoardo Saravalle, Artificial Intelligence and International Security, Center for a New American Security's series, July 2018.
www.cnas.org/publications/reports/artificial-intelligence-and-international-security

Nicholas Caporusso, Deepfakes for the Good: a Beneficial Application of Contentious Artificial Intelligence Technology, International Conference on Applied Human Factors and Ergonomics AHFE 2020: Advances in Artificial Intelligence, Software and Systems Engineering.
https://www.researchgate.net/publication/342691593_Deepfakes_for_the_Good_A_Beneficial_Application_of_Contentious_Artificial_Intelligence_Technology

Nils J. Nilsson, The Quest for Artificial Intelligence, A History of Ideas and Achievements, 2010, Cambridge University Press, NY, USA.

Oscar Schwartz, you thought fake news was bad? Deep fake are where truth goes to die, Technology, The Guadian, 12 Nov 2018
https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth
Rebecca Delfino, Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act, Fordham Law Review Volume 88 Issue 3 Article 2-2019.
Robail Yasrab , Wanqi Jiang and Adnan Riaz, Article Fighting Deepfakes Using Body Language Analysis, MDPI journal/forecasting- 2021-3, Basel, Switzerland.
https://www.mdpi.com/2571-9394/3/2/20
Rod Ghemmaghami and John Villafranco, Article: Deepfake Best Practices Amid Developing Legal Landscape April 16, 2021, Law360. Kelley Drye & Warren LLP,. New York.
https://www.kelleydrye.com/News-Events/Publications/Articles/Deepfake-Best-Practices-Amid-Developing-Legal-Land
Thanh Thi Nguyen, Quoc Viet Hung Nguyen, Cuong M. Nguyen, Dung Nguyen, Duc Thanh Nguyen, Saeid Nahavandi, Fellow, IEEE, Deep Learning for Deepfakes Creation and Detection: A Survey.
arxiv.org/abs/1909.11573

Third: Websites

Location MIT Technology Review What is deepfake technology?
https://technologyreview.ae/technodad/%D8%A7%D9%84%D8%AA%D8%B2%D9%8A%D9%8A%D9%81-%D8%A7%D9%84%D8%B9%D9%85%D9%8A%D9%82/
Wikipedia website at the following link:
Wikipedia, 'Deepfake',
https://en.wikipedia.org/Deepfake