Judge. Mohamed Hassan Mekkawi

Judge at the Egyptian Council of State

The Challenges of Digital Evidence Usage in Deepfake Crimes Era

Correspondence:

Judge. Mohamed Hassan Mekkawi Judge at the Egyptian Council of State

DOI: https://doi.org/10.54873/jolets.v3i2.123

E-mail: moh.mekkawi97@gmail.com - mailto:marc.michail@bue.edu.eg

Citation:

Mohamed Hassan Mekkawi, The Challenges of Digital Evidence Usage in Deepfake Crimes Era, Conference Research Papers The Third International Conference on Legal Aspects of Digital Transformation: Opportunities and Challenges Journal of Law and Emerging Technologies, Volume 5, Issue 3, October 2023, p. 175-232

The Challenges of Digital Evidence Usage in Deepfake Crimes Era

Judge. Mr. Mohamed Hassan Mekkawi

Abstract

This research paper discusses the challenges of digital evidence usage in the deepfake crime era in both the Egyptian and US legislation. There is no doubt about the importance of keeping pace with the law with behaviors that pose a threat to fundamental interests that deserve protection, especially in an era when information technology is instantaneously accelerating towards the creation of many modern technologies that raise many concerns, since artificial intelligence algorithms have helped to think about a large number of issues that did not exist a few years ago, such as the ease of processing big data and simultaneous machine translation, and one of those algorithms is Deepfake, which was classified as the most dangerous among artificial intelligence algorithms on cyber-security threats.

With the complexity of investigations of computer-related crimes due to the obstacles in gathering the evidence, the researcher seeks, after discussing the essence of digital evidence, stating its types, forms, characteristics, sources, principles, and challenges facing its application, as well as comparing the laws regulating digital evidence nationally, internationally (Budapest Convention), and the US federal rules of digital evidence, to present and set recommendations to reduce the risks and challenges of these crimes and to assist the legislator in addressing the shortcomings in the Egyptian laws.

Keywords: Cybercrime, Digital evidence, Artificial Intelligence, Deepfake, Digital privacy, Cybersecurity

تحديات استخدام الأدلة الرقمية في عصر جرائم التزييف العميق

محمد حسن مكاوي
قاضٍ بمجلس الدولة

الملخص

تناقش هذه الورقة البحثية تحديات استخدام الأدلة الرقمية في مواجهة جرائم التزييف العميق Deepfake. خاصة في عصر تتسارع فيه تكنولوجيا المعلومات لحظيا نحو ابتكار العديد من التقنيات الحديثة التي تثير الكثير من المخاوف، في ظل ظهور عدد كبير من القضايا التي لم تكن موجودة قبل بضعة أعوام، ولعل جرائم التزييف العميق تُعد الأخطر ضمن خوارزميات الذكاء الاصطناعي على تهديدات الأمن السيبراني.

تُرتكب الجرائم اليوم في بيئة رقمية، وفي البحث عن أدلة تلك الجرائم، فإنه لا غنى عن الاستفادة بالكميات الهائلة من البيانات الضخمة المخزنة في أجهزة الاتصالات والتى تعد أدلة رقمية. ومع تعقد التحقيقات في الجرائم السيبرانية بسبب معوقات جمع الأدلة، يسعى الباحث إلى مناقشة ماهية الأدلة الرقمية وأنواعها وأشكالها وخصائصها ومصادرها ومبادئها والتحديات التي تواجه تطبيقها، ثم استعراض القوانين المنظمة للأدلة الرقمية دوليا ومحليا مثل إتفاقية بودابست بشأن الجرائم السيبرانية، والقواعد الفيدرالية الأمريكية للأدلة الرقمية.

يسعي الباحث إلى كشف وتحليل المواد المنظمة لجمع الأدلة الرقمية في قانون مكافحة جرائم تقنية المعلومات المصري ولائحته التنفيذية، بالإضافة إلى تسليط الضوء على جرائم التزييف العميق التى تنتهك الخصوصية الرقمية كجريمة اصطناع أو نشر أو حيازة أشياء أو صور خادشة للحياء العام، وجريمة انتهاك الخصوصية بنشر صور شخصية دون رضاء المجنى عليه، وجريمة معالجة البيانات الشخصية للغير، وجريمة الانتقام الإباحي عبر تقنية التزييف العميق. وبناء علي مقارنة التشريعات الدولية مع نظيرتها المصرية يستخلص الباحث بعض النتائج والمقترحات للمشرع المصري بهدف معالجة أوجه القصور، والحد من المخاطر والتحديات لجمع الأدلة الرقمية فى جرائم التزييف العميق.

الكلمات المفتاحية: (الجرائم السيبرانية – الأدلة الرقمية – الذكاء الاصطناعى – التزييف العميق – الخصوصية الرقمية – الأمن السيبراني).

Introduction

As of January 2023, there were 5.16 billion internet users worldwide, which is about 64.4% of the global population. Of this total, 4.76 billion, or 59.4% of the world's population, were social media users(1). This increment in users of social networking sites is a direct result of the tremendous development in the treatment of collectibles and personal photos of others and the infringement of the sanctity of others' private lives by using sensitive data or fabricated content, which could lead the victim to commit suicide as a result of the social and psychological pressure.

Crimes today are committed in a digital environment, whether we like it or not. Not everyone has a firearm, but almost everyone has a computer, smartphone, or any other digital device that carries data and leaves traces. In the search for the truth in a cyber-investigation, it is indispensable today to make use of the data that communication devices leave behind. There is an enormous amount of data automatically generated by digital devices, such as internet browsing history, other computers, or the network to which the device has been connected. All of this information is digital evidence(2).

Cybercrimes (including pure cybercrimes, by which technology can be the target of the crime, such as «hacking, DDoS attacks, malware, or cyber-enabled crimes, by which technology can be the means or to assist in committing the crime, such as «online fraud, deepfakes») and other crimes involving digital evidence badly affect the right to privacy of millions of people whose personal data is stolen due to being volatile and fragile. Since it attacks their dignity and integrity and is considered a threat to freedom of expression and public security.

(1) Ani petrosyan, Worldwide digital population 2023, Statista,2023, available at: https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Worldwide%20digital%20population%202023&text=As%20of%20January%202023%2C%20there,percent%20of%20the%20global%20population. Accessed on 23-3-2023.

(2) Piotr Lewulis, Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law, Criminal Law Law Forum33, Springer, 2022. P. 39–62, available at: https://rdcu.be/c8hLQ Accessed on 23-3-2023.

Research Purpose

The researcher aims to determine the essence of digital evidence by studying its notion, characteristics, principles, sources, advantages, and the main technical and legal challenges in its usage. The research's main purpose is to detect and analyze the weak areas in the Egyptian Anti-Cyber and Information Technology Crimes Law, which is considered the only law that governs cybercrime. Additionally, the researcher seeks to highlight the deepfake crimes to improve the national law. This shall be done after analyzing the Budapest Convention on Cybercrime and the US Federal Rules on Digital Evidence and comparing them to the national law to suggest some recommendations to the Egyptian legislator.

Research Problem

Research done on the challenges of digital evidence usage has not covered all its aspects, which has led to weak outcomes. While many scholars have written about artificial intelligence threats, there have been few studies specifically on deepfake crimes. That's why the researcher aims to determine the legal challenges of digital evidence usage, especially in new forms of crime such as deepfake crimes, which might suggest legislative recommendations based on the research findings.

Research Methodology

The researcher used the critical comprehensive analysis study with the International Budapest convention on cybercrime as it is the most important convention regulating cybercrime, however Egypt still not joining the convention, and the US Federal Rules. Therefore it was important to show the strengthen points to help the legislator with alternatives to improve the national law.

Research Questions

Accordingly, the research will answer all the above-mentioned information in terms of solving certain questions:

- Where can digital evidence be found? To what extent is digital evidence admissible in court?
- What are the legal and technical challenges facing digital evidence?
- To what extent was the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 in Egypt appropriate to cope with the challenges of digital evidence in comparison to the Budapest Convention and US federal rules?
- What is the Deepfake algorithm, what are the arising crimes from it, how important is the digital evidence to deepfake crimes, and to what extent does Egyptian legislation regulate the possible crimes? What are the provisions of criminal liability for publishing the fake sexual clip on social media?

1. The Essence and Challenges of Digital Evidence

In this part, digital evidence will be defined from theoretical and legal perspectives, highlighting its characteristics, sources, advantages, and principles according to which it could be admissible to courts, answering the question of the extension of accepting evidence obtained through illegal means, and then discussing in detail the legal and technical challenges facing digital evidence.

1.1 The Definition of Digital Evidence

Evidence can be defined as any of the material items or assertions of fact that may be submitted to a competent tribunal as a means of ascertaining the truth of any alleged matter of fact under investigation before it[1].

(1) Jerry Norton, evidence meaning, The Editors of Encyclopaedia Britannica, 2023, available at: https://www.britannica.com/topic/evidence-law Accessed on 23-3-2023.

There is no internationally accepted definition of digital evidence. However, in all countries, there are regulations containing precepts that, in some way, refer to it.

From a legal perspective, the «Council of Europe Guide» defined digital evidence as any information generated, stored, or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings(1). However, the Anti-Cyber and Information Technology Crimes Law No. 175 of 2018 in Egypt defines digital evidence in Article (1) as «any electronic data with a probative force or value stored, transferred, extracted, or taken from computers, information networks, or equivalent thereof. Such information can be collected and analyzed using special devices, programs, or applications».

From the above, it became easy to define digital evidence as data stored within digital devices or systems that can be recovered by digital forensic experts and can be used as admissible evidence in court(2).

1.2 The Characteristics of Digital Evidence

Digital evidence is considered evidence of a technical nature because it is intangible, that is, it is not physical or material evidence, as it is a group of electric or magnetic fields. Therefore, translating the digital evidence and producing it in a tangible physical form does not mean that this assembly is considered evidence, but rather that this process is nothing more than a process of transferring those domains from their digital nature to the form in which a specific piece of information can be inferred(3).

(1) E-evidence - cross-border access to electronic evidence improving cross-border access to electronic evidence, available at: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en Accessed on 23-3-2023.

(2) Larry E. Daniel and Lars E. Daniel, Digital Forensics for Legal Professionals, Understanding Digital Evidence From The Warrant To The Courtroom, 1st edition, Syngress, 2012, P. 124.

(3) Khaled Mamdouh Ibrahim, Informational Crimes, 1st edition, Alexandria: University Thought House, 2009, P. 191.

- Digital evidence is a type of machine evidence; the scientific evidence must not deviate from what the digital evidence has reached, otherwise its meaning will be lost. It must be taken into account that digital science is a very developed science, but rather, it proves itself in its great ability for continuous self-development.
- Understanding the content of digital evidence depends on the use of specific devices for collecting and analyzing its content. Therefore, everything that cannot be identified and analyzed by those devices cannot be considered digital evidence because it cannot be inferred from a specific piece of information, which is of no value in proving the crime and its attribution to the criminal(1).

It became clear that digital evidence shares most properties with traditional forms of evidence but also possesses some unique characteristics, such as(2):

1. It is invisible to the untrained eye.
2. It is highly volatile.
3. It may be altered or destroyed through normal use.
4. It can be copied without degradation.

1.3 The Sources of Digital Evidence

Most people immediately think of computers, cell phones, and the Internet as the only sources for digital evidence, but any piece of technology that processes information can be used in a criminal way. For example, hand-held games can carry encoded messages between criminals, and even newer household appliances, such as a refrigerator with a built-in TV, could be used to store, view, and share illegal images. The important thing to know is that

(1) Abdel Fattah Bayoumi Hijazi, Digital Evidence and Forgery in Computer and Internet Crimes, An In-depth Study of Computer and Internet Crimes, Bahjat for Printing and Binding, 2009, P. 142.
(2) Dawn Lomer, 15 Types of Evidence and How to Use Them, I SIGHT, 2016, available at: https://www.i-sight.com/resources/15-types-of-evidence-and-how-to-use-them-in-investigation/ accessed on 22-3-2023.

responders need to be able to recognize and properly seize potential digital evidence(1).

Cyber-Investigators should always consider the possibility that any digital devices or equipment encountered during the investigation can yield digital evidence, as the Cyber-investigators should always consider the possibility that any digital devices or equipment encountered during the investigation can yield digital evidence, as the variation in devices containing digital evidence increases almost daily, such as in the following examples(2):

1. Dead Box: refers to equipment that has been found during the search that has been turned off. The dead box devices will be removed from the scene and examined later at a law enforcement or digital forensic laboratory.
2. Live Data: Forensics is likely to be necessary when a crime scene has computers and digital devices switched on. In the early years of computer forensics, whenever the cyber-investigator found a running system during the search and seizure process, the advice was to «pull the plug.» This means that the volatile data will be lost to the investigation as the remote connections will drop and the open files may be locked and encrypted. Such data and information can be of high evidential value. Live data forensics require a much higher level of technical knowledge and expertise, specific training, and hands-on practical experience.
3. Data held by third parties: such as data stored by large Internet service providers, Such as tracing a suspect Facebook profile to obtain necessary data that requires cooperation with the private sector, such as Facebook.
4. Internet Data: There are many sources of online information available

(1) David Mugisha, Digital Forensics: Digital Evidence In Judicial System, International Journal of Cyber Criminology, 2019, P. 1.
(2) Don Mason, Digital Evidence and Computer Forensics, National Center for Justice and the Rule of Law, 2013, P.8.

that might be useful to an investigation, such as OSINT (open source intelligence tools)[1].

From the above, The researcher noted that Digital evidence could be found anywhere in computer system[2], computer data[3], or traffic data[4], such as in Hard Disk Drives (HDD) the Main storage devices, Solid State Disks (SSD), Computer Disk, Digital Video Disk (DVD), Memory Cards, Universal Serial Bus (USB), Digital Cameras in a forms of thousands of pixels, it may be able to prove which camera took a specific photo because a certain metadata are often stored with the image in the camera's memory card, Digital Audio, Closed Circuit Television (CCTV), iPods or MP3, Video Games PlayStation, Network Attached Storage, Routers, Network switch, Server, Firewall, Wireless access point, Bit coin address, QR Codes, Finger prints, Eye prints and other Biometric Data. With the increment of the «Internet of Things, everything is or will be connected to the Internet, so there is no imagination about the impact of this on the importance of digital evidence.

1.4 The Principles of Digital Evidence

There are five main principles that should be respected to achieve an admissible presentation or digital evidence in court, which will be discussed as follows[5]:

1. Data Integrity: When handling digital devices and data, they must not be altered, either in relation to hardware or software. There are

(1) Mohamed El-Guindy, Applying Digital Forensics Methodology to Open Source Investigations in Counterterrorism. Journal of Law and Emerging Technologies, 1(1), 2021, P. 11–64.

(2) Budapest conv. Defined «computer system» as any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

(3) Budapest conv. Defined «computer data» as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

(4) Budapest conv. Defined «Traffic data» as any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

(5) Piotr Lewulis, Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law, Criminal Law Law Forum 33, 2022, P. 39–62, Springer, available at: https://rdcu.be/c8hLQ Accessed on 23-3-2023.

circumstances where a decision will be made to access the data on a «live» computer system to avoid the loss of potential evidence. This must be undertaken in a manner that causes the least impact on the data and by a person qualified to do so.

2. Audit Trail: all activities related to the search, seizure, access, storage, or transfer of digital evidence shall be fully recorded and available for review.

3. Specialist support: In cyber-investigations involving the search and seizure of digital evidence, it is always desirable to involve digital evidence specialists. All such specialists, either from within the organization or external contractors, should have the appropriate and objectively verifiable knowledge to deal with digital evidence properly.

4. Appropriate Training: In circumstances where no specialist is available, the first responder searching, seizing and/or accessing original data held on an electronic device or digital storage media must be trained to do so according to legally sanctioned procedures and must be able to explain and justify the relevance and implications of his/her actions: the chain of custody has to be respected at all times!

5. Legality: All the above shall be done in respect of the rule of law, and that shall be done by knowing and applying the law, respecting the conditions and safeguards, and ensuring the rights of defense and human rights.

1.5 The Advantages of Digital Evidence

Digital evidence is developed by nature: it is of a dynamic nature with high speed and the ability to move from one place to another through communication networks, not restricting the boundaries of time or space[1].

(1) Emad Sayed Haidar, Primary Investigation of Computer Crimes, Ph.D. Thesis, Faculty of Law, Cairo University, 2018, P.137.

The special technical nature of the digital evidence enables it to be subjected to some applications or programs to see if it has been subjected to tampering or distortion(1). The offender's attempt to erase or destroy the digital evidence is in itself evidence against him, as his actions are recorded in the device's memory by his digital footprints, which are something that can be retrieved or extracted and used as evidence against him.

1.6 The extent of acceptance of evidence obtained through illegal means

We can distinguish between three directions in this regard; some of them argued that the illegal evidence has complete authority in the proof, and some also argued that the illegal evidence has no authority, while others went to the distinction between the evidence of guilt and the evidence of innocence, as the latter is the one that could be used. The Anglo-Saxon systems, such as the United Kingdom and the United States of America, belong to what is known as the system of legal evidence, which exclusively identifies the evidence that the judge may resort to in proof; however, the Latin regimes prevail in the system of free evidence, in which the criminal judge enjoys absolute freedom in proving the facts before him(2). More details will be discussed in the next chapter.

1.7 The challenges of Digital Evidence

The criminal judge has discretionary power to assess the evidence, presumptions, and facts or indications they elicit by weighing the elements of the case, understanding its facts, and ascertaining their verification. Digital evidence shall be dealt with seriousness and great care to keep its integrity. Therefore, any cyber-investigator who encounters some challenges will be described in detail as follows:

(1) Mamdouh Abd al-Hamid Abd al-Muttalib, a proposed model for the rules for adopting digital evidence of evidence in computer crimes, published within the proceedings of the banking and electronic business conference organized by the Faculty of Sharia and Law at the United Arab Emirates University and the Dubai Chamber of Commerce and Industry, in the period from 10-12/5/2003 vol. Fifth, 2003, P. 2237.

(2) Ahmed Awad Bilal, The Rule of Excluding Illegally Obtained Evidence in Comparative Criminal Procedures, 3rd Edition Dar Al-Nahda Al-Arabia, 2013, P. 324.

1.7.1 Volatility

Volatile data makes digital evidence vulnerable to being destroyed, changed, manipulated, modified, and distorted easily. Due to the digital fingerprints left by each program on the computer, as well as rewriting on the data, this can ruin the evidence and affect its integrity. Thus, cyber-investigators shall use other technologies besides forensic tools to block the rewriting of these programs(1). Also, volatility includes all the data that can easily fade away, whether by shutting down the computing device or after a certain time has elapsed. This data is saved on a non-volatile memory, such as a random access memory. It can only be available when the computer is turned on and running, as there is no possibility of moving the device or changing the place of investigation. So, the forensic investigator will not be able to work on a forensic image on a different device and will have to work on the same device using live forensic techniques.

1.7.2 Encryption

Encryption is the process of scrambling information that can only be decoded and read by someone who has the correct decoding key. It is used to hide or make the evidence unreadable on the compromised system. Cybercriminals use many different encryption methods, and in order to make the data usable, sometimes the encrypted data cannot be decrypted(2). There are two kinds of encryption: symmetric and asymmetric encryption. In symmetric encryption, the same key of encryption is used to encrypt and decrypt the content; however, in asymmetric encryption, there are two keys for encryption and decryption, and they are both connected mathematically. This can disrupt the whole investigation process as investigators will have to

(1) Xandra E. Kramer, Challenges of Electronic Taking of Evidence: Old Problems in a New Guise and New Problems in Disguise Il Conferencia Internacional & XXVI Jornadas Iberoamericanas de Derecho Procesal IIDP & IAPL, La Prueba en el Proceso / Evidence in the process Atelier 2018, P. 391-410.

(2) Jean-Philippe Aumasson, serious Cryptography A Practical Introduction to Modern Encryption, San Francisco, 2018, P. 18.

have the decryption key, and many screening tools cannot open the encrypted documents(1).

1.7.3 Steganography

It is an encryption technique that can be used along with cryptography as an extra-secure method to protect data(2).

Steganography is a technique that is used to hide any information inside a file without modifying its outward appearance. Cybercriminals use this steganography to hide their hidden data (payloads) inside the compromised system. When investigating computer crimes, the cyber-investigator has to identify this hidden data in order to reveal the information for further reference.

Modern steganography uses technical procedures to insert contents inside other contents using the same idea of microdots or invisible ink. Steganography is about hiding confidential data or messages inside non-confidential content. Most commonly, the technique of steganography is used to conceal secret data in images. This changes the binary number and metadata of the image; however, this does not change anything in its appearance, and the image still looks the same. This also changes the volume of the hosting file, so if someone inserts a video of 100 MB inside an image of 30 MB, the volume of the image will be 130 MB in total. Accordingly, it could only be visible if someone used to insert a large volume of data inside a text or an image that was not as large as the inserted content, which might raise some doubts(3). The processes for the uprooting of data must be robust to ensure the restoration and validity of all information and data. Thus, these processes must also be legitimate to secure the originality of the evidence without any manipulation, deletion, or addition of data in any way(4).

(1) S.Suguna, V.Dhanakoti, and R.Manjupriya, A Study on Symmetric and Asymmetric key encryption algorithms, International Research Journal of Engineering and Technology (IRJET), 2016, P. 27.

(2) Rashad Rasras, Ziad Alqadi, and Mutaz Rasmi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, Engineering technology and applied science researches, 2019, P. 3681-3684.

(3) Mazen Abbas, Destroying Digital Evidence: Technical and Legal Dimensions, Master thesis, Cybercrime investigations professional master, Faculty of Law, British University in Egypt, 2022, P. 33.

(4) Zachary Roush, Digital Forensics: Data Recovery and Steps You Can Take to Assist in the Recovery Effort, JDSPURA, 2022, available at: https://www.jdsupra.com/legalnews/digital-forensics-data-recovery-and-6642070/ Accessed on 23-3-2023.

1.7.4 Data hiding in storage space

Cybercriminals hide some data inside storage areas and make them invisible to the usual system commands and programs. It makes the investigation more complex and time-consuming and sometimes data can be corrupted too. Rootkits are one of the most popular techniques used to hide data in storage space(1).

1.7.5 Residual Data wiping

When the cybercriminal uses a computer for his target, a few hidden processes are running without the cybercriminal's knowledge. But an intelligent attacker can avoid this risk by wiping out the tracks that were made by his process and making the system work as if it had not been used for such a purpose.

1.7.6 Resource Challenges

The cyber-investigator has to go through all the collected data in order to gather evidence. It may take more time for the investigation. Since time is a limiting factor, it becomes another major challenge in the field of digital forensics(2).

1.7.7 Preservation challenges

Preservation of digital evidence is the process of proving that the evidence is in fact what its proponents claim. One of the major issues with digital evidence authentication often involves identifying the author of digital contents. For example, the prosecutor will need to show evidence that an email allegedly written by the defendant to the victim was actually drafted by the defendant(3).

(1) David Mugisha, Digital Forensics: Digital Evidence in Judicial System, International Journal of Cyber Criminology, 2019, P. 4.

(2) Sabika Tasneem & Sidra Jabeen, How to Overcome Major Problems in Handling Digital Evidence?, VIDIZMO, 2022, available at: https://blog.vidizmo.com/6-major-problems-in-handling-digital-evidence Accessed on 23-3-2023.

(3) Martin Novak, Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration, Journal of Digital Forensics Security and Law, Volume 14, Number 4, 2020, P. 8.

1.7.8 Accidental Incidents

Although some obstacles may occur during the investigation that may disrupt the case and increase the difficulty and enormous pressure on the forensic expert, These obstacles include data breaches or cyber-attacks, especially in sensitive cases related to a state's critical infrastructure. The forensic expert will be under pressure to get a quick response, with less time to deal with a data breach or cyber-attack and keep data safe on devices. Most of the cases will require work in silence to identify a certain criminal, and if a data breach incident takes place, it could give him the signal to flee, which may affect the case negatively.

On the other hand, a cyber-attack may result in deleting or encrypting the digital documents required for investigation or may stop the device itself from working properly, disrupting the whole investigation process. Also, the variety of data types and digital devices will require the investigator to have multiple tasks to deal with each type. For example, if the only evidence on the device can be obtained from a volatile memory, this will require the investigator to work on active systems. So, he will work on the same device at the same time promptly and efficiently to prevent data loss, which is called live forensics. Conversely, the data saved on a local hard disk can be investigated and analysed on the same device or on other devices, but forensically specialized programs must be used for extracting an original image of the data found on the system without any changes and for restoring any deleted or hidden content. Moreover, the bigger the volume of data on the devices, the longer it takes to extract and analyse it[1].

1.7.9 Cross border Jurisdiction and the principle of territoriality

Globally, courts in most legal systems are not interfering in cases outside

(1) Eoghan Casey, Focused Digital Evidence Analysis & Forensic Distinguishers 18 Digital Investigation, 2016, P. 23.

their scope of jurisdiction due to the respect of the principle of territoriality. While in cybercrimes, the place of jurisdiction of the criminal might not be the same one for the storage of data, so, digital evidence must be equivalent to the rules and regulations of the state of jurisdiction to be admissible. This is what makes it difficult since the actions that might be considered a crime in one state might not be considered a crime in another state, making the digital evidence without value in some cases, as well as the fact that there is no obligatory legislation (just ethical) to oblige the state or the company to support and give the data needed to another state. This issue will be discussed later in this research.

Law enforcement officers often find that requested information is held by service providers located outside the country or internationally. An ISP may refuse to comply, particularly for fear of liability under the Electronic Communications Privacy Act. Law enforcement officers have the option in some cases. A trial or summons before a grand jury may be more effective in inducing compliance, and international cooperation and exchange between states is the best solution(1).

1.8 Summary for Chapter 1

From the above, the researcher noted that:

Physical/Material or testimonial evidence is more direct, generally easier to maintain, store, demonstrate, interpret and confront. However digital evidence is volatile by nature, soft, generally has a date stamp, is vast in volume, is more difficult to store than traditional evidence, and requires specialized knowledge. It's hard to prove its origin and demonstrate its authenticity and integrity.

(1) Gavin manes, Elizabeth Downing, Lance Watson and Christopher Thrutchley, New Federal Rules and Digital Evidence, Annual ADFSL conference on digital forencsics, security and Law, 2007, available at: https://core.ac.uk/download/pdf/217157581.pdf Accessed on 25-3-2023.

Digital evidence could be found anywhere in computer system, computer data, or traffic data, since the increment of «Internet of things» everything is or will be connected to Internet, so there is no imagination about the impact of this on the importance of digital evidence with unlimited examples.

The admissibility of digital evidence based on two major keys:

1. Authenticity: evidence must establish facts in a way that could not be disputed and its representative of its original state.
2. Completeness: the analysis of/or any opinion based on the evidence must tell the whole story and not be tailored to match a more favorable or desired perspective.

International Cooperation became a must in collecting and using digital evidence, as cybercrime is global crime, so the state shall join international agreements and conventions to ensure the (Legal obligation) support from other states.

2. International and national rules regulating digital evidence

The continuously increasing of online content due to the proliferation of digital technologies in socio-economic life, gave more importance of digital evidence. In this chapter the researcher describes the legal shortcomings of Egyptian legislation in the context of digital evidence after comparing with the Budapest convention on cybercrime and American federal rules regulating digital evidence as follows:

2.1 Budapest Convention on cybercrime

This part reviews the scope of the different procedural provisions under Budapest convention and the relevant conditions & safeguards as follows:

Article 16(1) regulates the Expedited preservation of stored computer data,

(1) Article 16 – Expedited preservation of stored computer data https://www.coe.int/en/web/cybercrime/the-budapest-convention Accessed on 12-8-2023.

as it set necessary measures to enable its competent authorities to obtain the expeditious preservation of specified computer data, the researcher can summarize it by the following:

1. Preservation may be ordered through judicial order, administrative order, search, and seizure; each country has the flexibility to determine how to implement the preservations.
2. Preservation means ensuring that data exists in a protected form and is safe from modification or deletion.
3. Power extends to all computer data, including business, personal, and even traffic data.
4. Preservation does not impose a general data retention obligation. Data sought to be preserved must already exist and have been collected and stored in a computer system.
5. For preservation to be exercised, there must be grounds that the computer data is particularly vulnerable to loss or modification, such as a data deletion policy, a limited retention policy, insecure data storage, or an untrustworthy custodian.
6. A person who is subject to a preservation order's control does not include the technical ability to access remotely stored data without legitimate control.
7. The maximum time period for a preservation order is 90 days.
8. Suspects are unaware of the investigation, which is why the right to privacy shall always be protected and prevents other persons from deleting or accessing the data.

Article 17(1) regulates the expedited preservation and partial disclosure

(1) Article 17 – Expedited preservation and partial disclosure of traffic data.

of traffic data, as it sets necessary measures to ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication and to ensure the expeditious disclosure to the competent authority of a sufficient amount of traffic data to enable the party to identify the service providers and the path through which the communication was transmitted.

Article 18(1) regulates the production order, and it can be summarized by the following:

- Any person in his territory including the service provider.
- Order must specify the computer data.
- Data shall be stored only on computers and be related to services offered in the territory.
- The service provider can have possession; control does not include technical ability.
- The service provider does not have to be located in the territory as long as it is «offering its services» in the territory.

From the above, it is noted that the production order allows law enforcement to order individuals and service providers to produce stored computer data and (domestic and foreign) service providers offering services in territory to produce subscriber information, as well as being less onerous for service providers than seizure.

Article 19(2) regulates the search and seizure of stored computer data, and it can be summarized by the following points:

- The term «search» means to seek, read, review, examine, or inspect.

(1) Article 18 – Production order.
(2) Article 19 – Search and seizure of stored computer data.

- The term «seize» means to take away the physical medium upon which data or information is recorded or to make and retain a copy of such information.
- The term «similarly accessible» is technology-neutral language that enables inspecting intangible data that can be in electromagnetic form.
- The term «similarly secure» is technology-neutral language that would enable recording, rendering inaccessible, or retaining a copy of intangible data that can be in electromagnetic form.
- Power to search or similarly can access: computer system, or part of it, Computer data stored in a computer system, computer-data storage medium with computer data stored within territory
- Power to extend search or similar access to another computer system or part of it if: the grounds to believe that data required is in that computer system or part of it; and the other computer system or part of it is also in the territory; or the data that is subject of extension is lawfully accessible from the initial computer system.
- All the measures shall be lawful, documented, done with high integrity by professionals, and not unreasonably threaten the right to privacy.

Article 20(1) stipulates the real-time collection of traffic data and it can be summarized by the following points:

- The competent authority has the power to directly collect or record traffic data, to compel a service provider to do so, or to cooperate with and assist the competent authority.
- Power must be exercised in relation to specified communications, as exercising this power for general or indiscriminate surveillance or the collection of large amounts of traffic data is not permitted.

(1) Article 20 – Real-time collection of traffic data.

- All communication measures shall be in the party's territory.
- It is important that the service providers be compelled to keep confidential the exercise of any powers.

From the above, it is noted that the real-time collection of traffic data allows live investigations, has an intrusive measure, requires conditions and safeguards, allows law enforcement authorities to collect or record, through technical means, data in real time, and allows the compulsion of service providers to collect or record data from their customers in real time.

Article 21(1) stipulates the interception of content data, and it is considered very important; therefore, it shall be summarized by the following:

- This power may only be exercised in relation to serious offenses, and the term «serious offenses» shall be determined by the party's domestic law.
- The competent authority has the power to directly collect or record traffic data, to compel a service provider to do so, or to cooperate with and assist the competent authority.
- Content data refers to the communication content of the communication, as well as the power that must be exercised in relation to specified communications, as exercising this power for general or indiscriminate surveillance or collection of large amounts of traffic data is not permitted, and all the communication measures shall be in the party's territory.

From the above; it is noted that interception of content data is very powerful investigative tool, but also very intrusive, it allows live collection of content data, it is only allowed in relation to a range of serious offences to be determined by national laws, Adequate safeguards need to be putted in place.

(1) Article 21 – Interception of content data.

Article 15(1) stipulates the conditions and safeguards needed in digital evidence, and it can be summarized by the following points:

- Modalities for the implementation of conditions and safeguards are left up to the party's domestic law.
- Parties are required to implement conditions and safeguards to protect human rights and liberties pursuant to obligations under applicable human rights instruments to ensure a balance between the requirements of law enforcement and the protection of human rights and liberties.
- Always respect the concept of proportionality. As the power or procedure must be proportional to the nature and circumstances of the offense, the domestic law must provide limitations on the breadth of production orders and reasonableness requirements for searches and seizures. The parties are required to implement the principle of proportionality in accordance with domestic law.
- Safeguards shall include judicial supervision and other independent supervision, Grounds justifying the application of procedural powers: limitation of scope of powers; limitation of duration of powers
- The need to balance the public interest with the rights, responsibilities, and legitimate interests of third parties the considerations should include minimizing disruption to consumer services, protecting from liability for disclosure or facilitating disclosure, and protecting proprietary interests.

2.2 US Federal rules on digital evidence

The Federal Rules of Procedure strive to accommodate the daunting challenges of the digital era of modern litigation. It gives general guidelines as to the discussion and handling of digital documents in modern litigation.

(1) Article 15 – Conditions and safeguards.

US Courts imposed high standards for the collection and analysis of digital evidence to ensure its authenticity under Rule 901[1]. Establishing authenticity of digital evidence often hinges on the testimony of digital forensic experts, whose opinions must pass the scrupulous reliability test imposed by Rule 702[2]. The researcher will briefly highlight key components of these rules and other basic digital evidence issues, such as authentication of digital evidence, expert testimony, and the best evidence rule, by the following:

1- Authentication of digital evidence

Authentication of digital evidence requires sufficient evidence to support a finding that the matter in question is what its proponent claims[3].The jury decides the authenticity of the evidence after determining the power given to the evidence after it has been subjected to vigorous cross-examination, the presentation of contrary evidence, and instructions from the judge on the burden of proof[4]. As there are many challenges in digital evidence that differ from material evidence, proving the authentication of digital evidence requires the use of digital forensics experts who have the skill, knowledge, and experience to use and apply a set of complex methods and tools for information security[5].

2- Expert Testimony

An expert may provide opinion testimony under Rule 702 if it is based on «scientific knowledge» that will help the jurors «understand or determine a fact in an expert may provide opinion testimony under Rule 702 if it is based

(1) Rule 901 – Authenticating or Identifying Evidence, available at: https://www.rulesofevidence.org/article-ix/rule-901/#:~:text=(a)%20In%20General.,the%20proponent%20claims%20it%20is. Accessed on 25-3-2023.
(2) Rule 702. Testimony by Expert Witnesses, available at: https://www.law.cornell.edu/rules/fre/rule_702 Accessed on 25-3-2023.
(3) The committee on the judiciary house of representatives, Federal Rules of Evidence, 2014, available at: https://www.uscourts.gov/sites/default/files/Rules%20of%20Evidence. Accessed on 25-3-2023.
(4) Gavin W. Manes, Elizabeth Downing, Lance Watson and Christopher Thrutchley, New Federal Rules and Digital Evidence, Annual ADFSL Conference on Digital Forensics, Security and Law. 3, 2007, P. 32.
(5) Hosmer, Chet, Proving the Integrity of Digital Evidence with Time, 1st Int'l J. Of Digital Evidence, 2002, P. 153.

on «scientific knowledge»[1] that will help the jurors «understand or determine a fact in issue». With regard to digital evidence, the fact usually at issue is whether the electronic information can be relied on as unadulterated and pure.

3- Best Evidence Rule

An issue created by digital documents is whether a paper copy of the original digital version satisfies the best evidence rule when the digital document contains metadata. Metadata is embedded information stored in electronically created materials that is not visible when the digital document is printed. As for email, metadata will tell you who was blind-copied or when it was read, while the paper printout will not reveal such nuggets. In some cases, metadata can be hugely relevant. In others, it may have no value, and its paper counterpart will suffice[2].

Once sources of potentially relevant electronic information have been identified, thought must be given to the proper process for collecting, transporting, preserving, analyzing, and producing it in a fashion that will not destroy its potential admissibility. The most cautious approach would entail retaining a digital forensic expert to assist with the process and the authentication of the evidence, as needed[3].

The best digital evidence shall contain a photo of the crime scene, a copy of the signed contract, a file recovered from the hard drive, and a bit-for-bit snapshot of a network transaction.

2.3 Egyptian Anti-Cyber and Information Technology Crimes Law No. 175 of 2018

(1) The committee on the judiciary house of representatives, Federal Rules of Evidence, 2014, available at: https://www.uscourts.gov/sites/default/files/Rules%20of%20Evidence. Accessed on 25-3-2023.

(2) William Y. Arms, Christophe Blanchi and Edward A. Overly, An Architecture for Information in Digital Libraries, D-Lib Magazine, February 1997, available at: http://www.dlib.org/dlib/february97/cnri/02arms1.html Accessed on 11-1-2022.

(3) Gavin manes, Elizabeth Downing, Lance Watson and Christopher Thrutchley, New Federal Rules and Digital Evidence, Annual ADFSL conference on digital forensics, security and Law, 2007.

The Law regulated the digital evidence through Articles 2, 6, and 11 of the Law, as well as Article 9 of the Executive Regulations issued by Prime Minister Resolution No. 1699 of 2020, which will be analyzed as follows by discussing five main points: Data retentions, temporary judicial injunctions, the conditions of digital evidence to be admissible in courts, the parties responsible for collecting digital evidence, and samples of recent judicial rulings applying digital evidence.

2.3.1 Data retentions

Article (2) regulates the concept of Data retention(1). The researcher finds advantages and disadvantages in the article: The advantage is that the service provider is obliged to maintain data for 180 days, which enriches the availability of digital evidence and helps in cyber-investigations, but on the other side, the article obliges the service provider to transfer all the data «upon the request of national security agencies and according to their needs», The criteria are vague and broad, which might invade the right to privacy if misused, and they

(1) Article 2.

«First: Without prejudice to the provisions of this law and Telecommunication Regulation Law as promulgated by Law No. 10 of 2003, the Service Providers shall: 1. Preserve and store the Information System Registry or any means of information technology for one hundred and eighty days on end. Data to be saved and stored shall be as follows: (A) Data enabling identification of the service user. (B) Data related to the content of the Information System dealt with whenever such data are under the control of the Service Provider. (C) Traffic-related data. (D)Data related to communication terminals. (E) Any other data for which a resolution is passed by the Board of the Authority. 2. Maintain the confidentiality of preserved and stored data, and shall not reveal or disclose such data without a substantiated order of a competent judicial body, including the personal data for any user of the service, or any data or information related to the websites and private accounts to which these users, or the persons and bodies with which they communicate, have an access. 3. Secure the data and information marinating its confidentiality, and shall not disclose or damage it.

Second: Without prejudice to the provisions of the Law on Consumer Protection, the Service Provider shall, in convenient, direct and ongoing manner and way, provide the users of its services and any competent governmental body with the following data and information: 1. Name and address of the Service Provider. 2. Contact information related to the Service Provider, including the email address. 3. Data of license to identify the Service Provider and the competent body by which the Service Provider is supervised. 4. Any other information whose value is deemed by the Authority as important for protecting the service users, and for its determination a resolution is passed by the Competent Minister.

Third: Subject to observing the privacy guaranteed by the Constitution, the Service Providers and their respective members shall, upon the request of National Security Agencies and according to their needs, provide all technical capabilities that permit such agencies to exercise its competences according to the Law.

Fourth: The Service Providers of Information Technology, and their agents and distributors that are entrusted with marketing such services, shall obtain the users data. It shall be prohibited for any person other than the foregoing to do the same».

are also against one of the most popular principle precedents of the Egyptian constitutional court, which sentence «What is meant by the ambiguity of the penal article is that the legislator is ignorant of the actions that he approved, so their statement is not clear, nor is their definition conclusive or their understanding straight, but rather vague and hidden among the people, because the enforcement of this article is linked to personal criteria that refer to the assessment of those in charge of its application of the truth of its content and the subrogation of their own understanding. Which means that the application of these texts by those in charge of their implementation should be a selective act, defined in the light of their personal whims and fancies, thus crystallizing their choices. Which they hunt whomever they want, so it is nothing but a trap with which no one is safe, and there is no warner for them».

Therefore, the researcher recommends amending this article and determining the criteria for data retention in a way that ensures more balance between national security and basic human rights such as the right to privacy.

2.3.2 Temporary judicial injunctions

Article (6) regulates the concept of Temporary judicial injunctions(1). The researcher commends the legislator in this article, as the maximum period of temporary judicial injunctions is 60 days, and they shall be reasoned

(1) Article (6)

«The investigation body concerned may, as the case may be, issue a substantiated writ to the competent law enforcement officer in respect of one or more of the following matters, for a period not exceeding thirty days renewable for one time, if this will help reveal the truth about the perpetration of an offence punishable under this law:

Control, withdrawal, collection, or seizure of data and information or information systems, or tracking them in any place, system, program, electronic support or computer in which they are existing. Its digital evidence shall be delivered to the body issuing the order, provided that it shall not affect the continuity of the system and provision of the service, if so required.

Searching, inspecting, accessing and signing in the computer programs, databases and other devices and information systems in implementation of the seizure purpose.

The concerned investigation body may order the Service Provider to submit the data or information related to an information system or a technical device under the control of or stored by the Service Provider, as well as the data of the users of its service and the connection traffic made in that system or the technical system.

In all circumstances, the writ issued by the investigation entity must be substantiated. The aforesaid writs shall be appealed before the criminal court concerned, as held in the deliberation room on the dates and according to the procedures stipulated in the criminal procedural law».

for plausible and serious reasons. This period is less than the Budapest Convention, which stipulates the maximum period of 90 days.

2.3.3 The conditions for digital evidence to be admissible in courts

Article 11 stipulates «The evidence derived or taken from devices, equipment, media, electronic supports, information system, software, or any means of information technology shall have the same value and force of criminal material evidence in criminal evidence where the technical conditions set out in the executive regulations of this Law are met».

The executive regulations of the Anti-cyber and Information Technology Crimes Law, issued by the Prime Minister's Resolution No. 1699 of 2020, specified in Article 9 of them five conditions for digital evidence to be admissible in courts; all five of these conditions shall be met in an accurate and correct way.

1. The process of collecting, obtaining, extracting, or eliciting digital evidence at the scene of the incident should be done using techniques that guarantee no change, update, erasure, or distortion of writing, data, or information, or any change, update, or damage to devices, equipment, data, information, information systems, software, electronic supports, and others. In particular, Write Blocker, Digital Image Hash, and other similar technologies
2. The digital evidence shall be related to the incident and within the framework of the subject matter required to be proven or disproved, according to the scope of the decision of the investigation authority or the competent court.
3. The digital evidence must be collected, extracted, preserved, and kept by the judicial officers, who are authorized to deal with this type of evidence, or by the experts or specialists assigned by the investigation

or trial authorities, provided that the type and specifications of the programs, tools, devices, and equipment are indicated in the control reports or technical reports that have been used. The hash algorithm code resulting from the extraction of similar and identical copies of the digital evidence must be documented in the control report or the technical examination report while ensuring that the original is still preserved without tampering with it.

4. In the event that the copy of the digital evidence cannot be examined and the devices under examination cannot be kept for any reason, the original shall be examined, and all of this shall be recorded in the seizure report or the examination and analysis report.

5. Digital evidence must be documented in a record of procedures by the specialist before the examination and analysis of it, as well as documenting the place where it was seized, the place where it is kept, the place of dealing with it, and its specifications.

The digital evidence must be verified by the expert or competent employee by printing it or taking pictures of it by any digital or visual means. The following information must be mentioned:

- The date and time of printing and photocopying;
- The name and signature of the person who did the printing and photocopying;
- The name or type of the operating system and its version number;
- The name of the program and the type of version or commands used to prepare copies;
- Data and information related to the contents of the exact evidence;
- Data on hardware, equipment, software, and tools used.

After analyzing the previous articles, the researcher noted the following:

- The executive regulations did not stipulate the controls related to the procedures related to the process of collecting and documenting the evidence at the various stages.
- The executive regulations did not provide for controls related to cases of evidence being damaged at any stage of the investigation or trial.
- The executive regulations did not stipulate how to decrypt the digital evidence, if it was encrypted.

2.3.4 The parties responsible for collecting digital evidence

The procedures were limited to two parties: the judicial control officer and specialized experts.

1. Judicial officers: the executive regulations have indicated that they must be authorized to deal with this type of evidence. Which means that with the exception of the specialized law enforcement officers or those who have been issued a decision of judicial accuracy in the crimes stipulated in the Information Technology Crimes Law, no officer has the right to gather, extract, preserve, or seize digital evidence and then issue seizure reports related to the evidence.
2. Specialized experts: the law gave specialized experts the right to collect, extract, preserve, and seize digital evidence and to edit technical reports related to these procedures. From investigation or trial authorities only.

2.3.5 Samples of recent judicial rulings applying digital evidence

The Supreme Administrative Court established an important legal principle and a precedent that is the first of its kind in the history of the administrative judiciary in 2021, to protect citizens from impersonation on Facebook pages, stating that it is not permissible to prosecute citizens for Facebook crimes

except with digital evidence from the Internet investigations, through the General Administration of Information Technology, And that adhering to justice requires not punishing the innocent, and that digital evidence must be proven for all information technology crimes on all means of communication and social communication, and that there are 24 criminal offenses with severe penalties to preserve the entity of the state and its national security, preserve family principles and values in Egyptian society, and sanctify the private life of citizens And that a page not in the name of the appellant on Facebook accuses the head of the Tax Authority of using corrupt and Brotherhood elements as chiefs of missions, and the origin of innocence prevails because there is no digital evidence of his ownership of the page(1).

The Supreme Administrative Court ruled to reject the tax authority's appeal, to cancel the decision of that authority to deduct fifteen days' wages from the salary of the respondent, the Shubra Al-Khaimah tax chief, for insulting the leaders of the tax authority on a page that is not in his name on Facebook, and to acquit him of the accusation leveled against him. Because of the serious failure of the investigation due to its lack of digital evidence in accordance with the provisions of the Anti-Cyber and Information Technology Crimes Law, the appealed decision is in violation of the principles of a just and fair trial and requires the judiciary to invalidate the investigation and invalidate the contested penalty decision as a consequence of that defect(2).

2.4 Summary for Chapter 2

Digital evidence is here to stay and indispensable to the investigation of virtually any kind of crime. The handling of digital evidence is embedded in the Budapest Convention and is directly linked to the procedural powers and safeguards provided by the Convention.

(1) Supreme Administrative Court ruling, June 7, 2021

Supreme Administrative Court ruling, June 27, 2021 (٢)

Budapest Convention can be applied anytime, because any crime can have a digital evidence even if it is not a cybercrime.

The Egyptian Law, tries to fit the digital environment, but there are many articles needed to be discussed more and amended, the lake of international cooperation is still considered as a weakness point in the Law, also there is a need to remember that digital evidence is often massive, highly privacy-sensitive and linked to far-reaching procedural powers; it is therefore crucial that digital evidence is handled in a controlled and proportionate manner, in accordance with the rule of law and human rights standards.

The researcher noted that the judge can have his belief in any form and to everything that enters into his reassurance, and this means that if the digital evidence is not taken as evidence, it will be used as a presumption, and if the presumptions are gathered, evidence can be emerged from them. As the judge can have his belief in any form and to everything that enters into his reassurance, and this means that if the digital evidence is not taken as evidence, it will be used as a presumption, and if the presumptions are gathered, evidence can be emerged from them. This trend was applied by the Egyptian and French judiciary, as Article 336 of the Criminal Procedure code stipulates that «if it is decided that any procedure is invalid, it deals with all the effects that directly result from it, and it is necessary to return it whenever possible.»

After comparing between Budapest convention and the law no.175 of 2018, it shall be noted that the later did not regulate all the safeguards that Budapest convention had, as it did not regulate the judicial supervision, and other independent authority supervision, however it regulated the grounds justifying application of procedural powers, Limitation of scope of powers, Limitation of duration of powers.

3. Deepfake Crimes

This part reviews the definition of artificial intelligence, forgery, and the difference between forgery and deepfake as one of the algorithms of artificial intelligence, shows how the deepfake video clip is made, determines the main pillars of deepfake crimes, and then highlights how US legislation regulates deepfake. Finally, analyzing the types of fake crimes and to what extent the Egyptian legislation is appropriate to cope with them.

3.1 Definition of Deepfake crimes

Forgery is defined as «the reproduction or re-presentation of a work in an illegal manner and is mainly represented in the accurate reproduction of an original product or its distinctive signs, as these distinctive signs relate to the external aspects of the product»(1). However, artificial intelligence (AI) is defined as one of the modern digital sciences that searches for innovative and advanced methods to carry out work and analyze the similarity of human intelligence(2).

While deepfake is one of the algorithms of artificial intelligence and machine learning, as it is done through the algorithms of artificial intelligence systems AI, using the machine learning network ML, these systems to achieve deepfake rely on the use of three main techniques, which are the Face Swap technology, the Expression Replacement Technology Swap, and Generative Adversarial Networks (GANs)(3).

The first deepfake videos appeared in 2017 on Reddit(4), where celebrities' faces were used instead of the real faces of porn actors, and since then, deepfakes have gone viral and have been so convincing that it is difficult to tell the difference between the truth and the fake(5).

(1) Delphine Baize, De la contrefaçon à l'imitation, revue française de gestion, juin-juillet-aout 1999, P. 76-78.
(2) Brett Lantz, Machine Learning with R, Packt Publishing Limited; 2 edition (31 July 2015), P. 178-198.
(3) Yuezun Li and Siwei Lyu, Exposing DeepFake Videos by Detecting Face Warping Artifacts (presentation, CVPR 2019: Computer Vision and Pattern Recognition, Long Beach, CA, June 2019), available at: https://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Li_Exposing_DeepFake_Videos_By_Detecting_Face_Warping_Artifacts_CVPRW_2019_paper.pdf Accessed on 27-3-2023.
(4) Great Learning Team, All You Need to Know About Deepfake AI, GreatLearning, November 2022, available at: https://www.policechiefmagazine.org/law-enforcement-era-deepfakes/ Accessed on 27-3-2023.
(5) Mika Westerlund, The emergence of Deepfake Technology: A Review, Technology Innovation Management Review 9, no. 11 (November 2019): P. 39–52.

Using deepfakes differs between positive and negative, as deepfakes can be used legitimately in artistic and media use, such as filming scenes of cinematic deceptions in a way that appears to be closer to the truth without danger; they are also used in the health sector to increase the clarity of rays to detect cancerous tumors; and they are used in the educational sector, such as bringing historical figures back to life for students to watch and tell them historical facts(1). While deepfake can be used illegally, such as in fourth-generation wars to overthrow countries from within without armed confrontation by falsifying the awareness of citizens, it is also used to produce revenge porn, which we will present later(2).

The deepfake video of Ukrainian President «Zelinsky» was spread on social media in March 2022, ordering his soldiers to lay down their arms and surrender completely in the fight against the state of Russia(3). This algorithm did not stop at public figures alone but extended to ordinary individuals, as In one incident, 243,000 dollars were transferred to a bank account in Hungary in 2019, where the CEO of an energy company branch of a UK-based believed that the person on the other end of the line was his boss, the CEO of the headquarter company, as the scammer asked the CEO of the company Sub to send money to him promptly by using deepfakes. According to statistical figures, the deepfake content industry is increasing at a rate of 900% every year, so the number of deepfake clips online jumped from 14,678 clips in 2019 to 145,277 clips by June 2020(4).

(1) Betül Çolak, Legal Issues of Deepfakes, The institute of Internet & the just society, January 2021, available at: https://www.internetjustsociety.org/legal-issues-of-deepfakes Accessed on 27-3-2023.

(2) Ashley Dean, Deepfakes, Pose Detection, and the Death of «Seeing is Believing», Law and Technology Today, 2020, available at https://www.lawtechnologytoday.org/2020/08/deepfakes-pose-detection-and-the-death-of-seeing-is-believing/ Accessed on 27-3-2023.

(3) Deepfake video of Volodymyr Zelensky surrendering surfaces on social media, available at: https://www.youtube.com/watch?v=X17yrEV5sl4 Accessed on 27-3-2023.

(4) John Letzing, How to tell reality from a deepfake, World Economic Forum, 2021, available at: https://www.weforum.org/agenda/2021/04/are-we-at-a-tipping-point-on-the-use-of-deepfakes/
Accessed on 27-3-2023.

3.2 Main pillars of Deepfake crimes

Deepfakes have three pillars: the duality of criminal behavior, publicity, and global crime.

1. The duality of criminal behavior: Where the material element in deepfake crimes consists of two basic behaviors: the first behavior is the collection and monitoring of pictures, video clips and audio recordings of the victim, and this behavior in itself is legal if the personal data that you obtain relates to public figures or people who willingly gave up their data on various Internet applications, such as «Public Account», But if he obtained that personal data illegally, then he would have violated the victim's privacy and fall under the penalty of the Anti-Cyber and Information Technology Crimes Law no. 175 of 2018(1). The second behavior is misrepresenting and manipulating the personal data you obtain to create the fake video. The two behaviors must be sequential in chronological order(2).

2. Publicity: It means making the fake video available to the public through any of the means of publication (digital or normal), whereas publicity does not mean synchronization or contemporaneity between it and the creation of the fake video. Rather, publicity is achieved by publishing at any time, even after the production of the fake video.

3. The global nature of the crime: Where doubts arise in identifying the perpetrator of the crime between the person who created the original clip, the one who used artificial intelligence algorithms to carry out deep falsification, the person who published it on the Internet, or the service provider who knew about the existence of the illegal content,

(1) Unauthorized Access Offences Article (14).
Crime on Infringement of surpassing the Right of Access Article (15).
(2) Mahmoud Salama Al-Sherif (2022) revenge porn crime through deep falsification and criminal responsibility for it, Journal of the Faculty of Law for Legal and Economic Research, Faculty of Law, Alexandria University, P. 382.

Then, the difficulty arises in prosecuting the perpetrators due to the global nature of the crime and the fact that it crosses borders, and then there must be international cooperation to avoid impunity.

From the foregoing, the researcher believes that the expansion of the risks of deepfake is due to four main factors:

1. Digitizing personal data that has become available on social media, including images and clips that can be used in deepfake content.
2. Availability of deepfake applications so that they become accessible to everyone without being monopolized by anyone, which facilitates their use in several crimes.
3. Specialization is not required to be used, as these applications address the common people and do not need specialists to use them.
4. The availability of multiple methods that allow perpetrators of crimes via the Internet to hide their identity, including the Doxing feature.

3.3 US rules on regulating deepfakes

As of this writing, only three US states have enacted different laws to combat deepfakes:

In 2019, the state of California added provisions prohibiting any person or entity from producing, distributing, publishing, or broadcasting, in bad faith, false election campaign materials that contain a picture or voice of a person or persons nominated through deep fake technology within 60 days of the election. It criminalizes the act, but it gives the injured party the right to file a lawsuit, according to which he deserves compensation in return for the damage he suffered and the lost earnings.

The state of Virginia(1) has imposed criminal penalties on fake pornography through technologies designed for that, including deepfakes, if the purpose is to coerce, harass, or intimidate the victim. The law comes into force on July 1, 2019, making the fabrication, sale, or distribution of fabricated pornographic images and videos a first-degree misdemeanor punishable by up to a year in prison and a $2,500 fine.

In 2019, the state of Texas(2) criminalized the creation or distribution of fake videos by introducing an amendment to its election law, adding a new text that criminalizes this act if it is intended to harm a specific candidate or influence the election result if it is published and distributed within 30 days of the elections, and considered this act A misdemeanor of the first degree is punishable by one year in prison in a state prison and a fine of up to $4,000.

The aforementioned laws in the states of Texas and Virginia considered deepfake technology merely a means to achieve the criminal purpose of violating the integrity of the electoral process or influencing a candidate.

By extrapolating these three previous legislations, it becomes clear that deepfake technology is not criminalized in itself, but rather for a criminal purpose, what the offender intended, and then does not exceed in its legal adaptation just the means or tool used by the offender to commit his crime, and according to the general rule, the criminal legislator does not consider the means, but rather By assaulting the criminally protected interest, whatever the means of this infringement, however, the legislator in exceptional cases may deviate from this principle to give the means by which the crime was committed an important role in criminalizing the act or intensifying the punishment for it, as if he made the means one of the components of the

(1) Code of Virginia, § 18.2-386.2. Unlawful dissemination or sale of images of another; penalty. Available at https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-386.2/#:~:text=Morals%20and%20Decency-,%C2%A7%2018.2%2D386.2.,of%20images%20of%20another%3B%20penalty. Accessed on 27-3-2023.

(2) Texas-2019-SB751-Introduced.html available at: https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm Accessed on 27-3-2023.

crime, especially crimes related to influence on the integrity of the electoral process or revenge porn through deepfakes.

3.4 Types of Deepfake crimes

This part reviews the most important types of crimes committed through deepfake algorithms by the following:

3.4.1 Manufacturing, publishing, or possessing things or pictures that are offensive to public decency crime

The Egyptian penal code stipulates in (Article 178) «Whoever makes or holds, for the purpose of trade, distribution, leasing, pasting or displaying printed matter, manuscripts, drawings, advertisements, carved or engraved pictures, manual or photographic drawings, symbolic signs, or other objects or pictures in general, if they are against public morals, shall be punished with detention for a period not exceeding two years and a fine of not less than five thousand pounds and not exceeding ten thousand pounds or either penalty».

This part discusses the material and moral pillars of the crime, as well as the validity of this article to face the threats of deepfake, by the following:

3.4.1.1 The Material pillar of the crime

The criminal behavior of the crime is publishing, manufacturing, and possession.

- Publishing: is achieved by making what has been published available to everyone without discrimination by any means, and it is not required that others have actually seen what has been published; it is sufficient for the offender to have made this subject available by publishing it even if no one has actually seen it.
- Manufacturing: is achieved by every act of the offender to process an object or a group of things by means of a device or manually, such

as modifications that occur to images through photo or video editing programs through «Photo-Video Editor» or Photoshop» programs.

- Possession: is achieved by the offender's control over the images or other things and with the powers that derive from this control, such as using the object, modifying its form, and disposing of it, which means that the presence of the object in the hands of the person without having any material powers over it does not make him possess it in the sense referred to[1].

It becomes clear that the object of criminal behavior is anything that is suitable to be published, possessed, or manufactured as long as it is offensive to public modesty, that is, it would prejudice the sentiment of modesty among people, and it is also according to the collective view of individuals within the society in which the behavior occurred and not according to the self-view of those who witnessed this behavior of people[2].

3.4.1.2 The Moral pillar of the crime

General MENS REA is needed by making, publishing, or possessing something of what is mentioned in the article with the intention of trading, distributing, trading, sticking, or displaying, and he knows what it entails to insult public modesty, whether with or without payment. The criminal will not be punished under this article if he or she made or possessed sexual images for the purpose of personal pleasure and without the three objects of the crime[3].

3.4.1.3 The validity of the article to face the threats of deepfake

The article expands on defining the types of criminal behavior that may

(1) Tarik Sorour, Explanation of the Penal Code Special Section, Crimes of Persons and Money, second edition, Dar Al-Nahda Al-Arabiya, Cairo, 2010, P. 309.
(2) Ramses Benham, The General Theory of Criminal Law, Alexandria, Origin of Knowledge publishing, 1971, P. 697.
(3) Ahmed Fathy Sorour, The Mediator in Penal Law, General Section, Sixth Edition, Cairo, Dar Al-Nahda Al-Arabiya, 2015, P. 875.

occur by any means, as it punishes possession, publication, and manufacture, and it includes forgery, and thus it is considered one of the articles that help in punishing deepfake crimes. Despite this, the researcher believes that this article punishes the crime contained therein with discretionary penalties that are not commensurate with the seriousness of deep forgery crimes, nor did it add any aggravating circumstances to punishment, and it did not take into account, for example, the case in which the victim is a minor or in other cases. Others to protect national unity and the country's reputation.

3.4.2 Invasion of privacy by publishing personal photos without the consent of the victim crime

The Anti-Cyber and Information Technology Crimes Law stipulates in Article (25) «Anyone who infringes a family principle or value of the Egyptian society, encroaches on privacy, sends many emails to a certain person without obtaining his/her consent, provides personal data to an e-system or website for promoting commodities or services without getting the approval thereof, or publishes, via the information network or by any means of information technology, information, news, images or the like, which infringes the privacy of any person involuntarily, whether the published information is true or false, shall be punishable by imprisonment for no less than six months and a fine of no less than fifty thousand Egyptian Pounds and no more than one hundred thousand Egyptian Pounds, or by one of these two penalties».

This part discusses the material and moral pillars of the crime, the penalty prescribed for it, and its suitability for deepfake crimes:

3.4.2.1 The Material pillar of the crime

Criminal behavior is achieved through publication. That is the transfer of knowledge of the image to others, and publication is achieved once it reaches

one person[1], so there is no specific number of views needed in order for publication to be achieved, but rather it is sufficient for the perpetrator to publish it even if no one has seen it. All that is required is that this image be available for viewing through any digital means. The publication shall be without the consent of the victim, as the consent focuses on the publication, not on the method of obtaining the image subject of publication, and therefore the image taken with the consent of the person it represents can be the subject of the crime of publishing, as the owner of the image may agree to the capture but not to the publication, just as it is not required that the culprit in the crime of publishing be the same person who took the victim's photo.

3.4.2.2 The Moral pillar of the crime

General MENS REA is needed and shall be represented with the availability of the elements of awareness and intention. The intention of the offender must be directed toward violating the article by publishing digitally, and he must be aware that he is publishing a picture of others that violates the privacy of this third person without his consent.

3.4.2.3 The Crime's penalty

The penalty is imprisonment for no less than six months and a fine of no less than fifty thousand Egyptian pounds and no more than one hundred thousand Egyptian pounds, or one of these two penalties.

The Egyptian legislator has tightened the penalty for the publishing crime mentioned in Article 25 in certain cases, such as Article 34 of the same law, where the penalty for the crime is imprisonment, which could reach 15 years if it is committed for the purpose of disturbing public order, endangering the safety and security of society, or harming the country's national security. Article 40 stipulates that the punishment for attempting to commit this crime must not exceed half of the maximum penalty.

(1) Gamil Abdel-Baki Al-Saghir, Procedural aspects related to the Internet, Dar Al-Nahda Al-Arabiya, 2001, P.325.

3.4.2.4 The Article suitability to deepfake crimes

Although the article punishes publishing an image that violates a person's privacy, whether it is true or incorrect, this article is only concerned with publishing the image, which makes the scope of its application in the matter of deepfake limited to publishing fake images and does not include the fake itself. In addition to that, it does not It is applied unless the publication is through one of the means of information technology, and thus outside the scope of its application is the publication by any other means, in addition to the ambiguity that surrounds the meaning that the legislator wanted for the image that violates the privacy of the person.

The researcher recommends that this article punish cases of unintentional publication or disclosure of the image that is the subject of criminal behavior, as the damage that could result from publishing or violating the privacy of the victim

3.4.3 Processing the personal data of others crime

The Anti-Cyber and Information Technology Crimes Law stipulates in Article (26) «Anyone who deliberately uses an information program or information technology in processing personal data of a third party to connect such data with an abusive content or to display the same in a way detrimental to the reputation of such third party shall be punishable by imprisonment for no less than two years and a fine of no less than one hundred thousand Egyptian Pounds and no more than three hundred thousand Egyptian Pounds, or by one of these two penalties».

This part discusses the material and moral pillars of the crime, the penalty prescribed for it, and its suitability for deepfake crimes:

3.4.3.1 The Material pillar of the crime

The crime does not require a specific result, but it is sufficient for the

perpetrator, through processing the personal data of the victim, to make changes in the images, audio, or video, and he can delete some elements from them, record them, and merge the images, audio recordings, or clips with each other in one fake video. In all cases, the fake video must be contrary to public morals or show it in a way that would prejudice the consideration or honor of the victim, and honor has a personal nature related to the moral side of the victim.

Linking criminal offenses to broad terms that are not precisely defined is contrary to the rules of the Supreme Constitutional Court. The phrase «public morals» has a social perspective that changes with the change of place and time, just as not everything that contradicts a religious rule is considered contrary to public morals(1). As the criteria for identifying the truth of the content and the extent to which it contradicts public morals are what the judge reassures him of, this content contradicts the aforementioned values and considerations(2).

3.4.3.2 The Moral pillar of the crime

The general MENS REA is needed and shall be represented by the criminal intention to process the personal data of the victim and link it to content contrary to public morals or to show it in a way that would prejudice the honor and consideration of the victim by using information technology programs and having his awareness of all of the above.

3.4.3.3 The Crime's penalty

The penalty is imprisonment for a period of not less than two years, and not exceeding five years and a fine of not less than one hundred thousand pounds and not exceeding three hundred thousand pounds, or one of these two penalties.

(1) Mohamed Hassan Mekkawi, Digital Privacy in International Law and International conventions, Journal of Media Research and Studies, Issue Twenty, 2022, P. 840.
(2) Criminal Cassation of. 118 of Judicial Year 51 in 10/10/2000.

3.4.3.4 The Article suitability to deepfake crimes

After analyzing the article, the researcher found the following:

- The article is considered a good step to address the risks of deepfakes, especially because it criminalizes mere illegal processing and does not require that the perpetrator publish the image that has undergone processing in order to be punished. Simply sending, for example, a «fake» porn video to the victim on a private messaging application is considered a crime.
- The article is an optional punishment that is not appropriate to address deepfake crimes in cases where the court may suffice with the penalty of a fine, and therefore the researcher recommends the necessity to add a paragraph in this article that stresses the punishment for the intentional publication of the processed content.
- The article does not apply to anyone who produces a fake video clip of himself without publishing it, such as someone who makes a fake sexual video clip of himself with an artist. Rather, he is subject to accountability according to Article 1 and Article 14 of the Anti-Prostitution Law No. 10 of 1961, which are old penalties. The researcher recommends the massive need to reconsider such articles.

3.4.4 Deepfake Revenge Porn Crime

This part discusses the definition of revenge porn and the differences between cyber blackmail, revenge porn, and deepfake revenge porn crimes, also the material and moral pillars of the deepfake revenge porn crime and the penalty prescribed for it.

3.4.4.1 Definition and Differences

Revenge porn is a compound term for revenge, which is taking revenge on a person as a response to what he did in terms of harming the other financially

or morally, and porn means revealing the chastity of the same person(1). Therefore, revenge porn is a form of sexual harassment via the Internet, and it is always followed by one of two things: either on the occasion of a previous intimate relationship with the consent of both parties, whether it was legal or illegal; by publishing pictures or video clips recorded without the knowledge of the other party; or by targeting a person's data. By penetrating his mobile phone, computer, or e-mail to steal pornographic videos and then publish them on the Internet(2).

Deepfake revenge porn means broadcasting and sharing sexual videos that were created or produced through deepfake technology without the consent of the victim, male or female, and for the purpose of taking revenge on him.

This type differs from revenge porn because the latter is a real porn incident that actually occurred and the perpetrator published or broadcasted it in retaliation against the victim, but in deepfake revenge porn, the porn incident is fake and artificial, which makes it more dangerous than the crime of pure revenge porn(3).

Deepfake revenge porn differs from cyber blackmail in that the latter involves the threat to publish pictures or clips associated with a specific request. In deepfake revenge porn, the threat is not required to be associated with a request. Cyber blackmail uses information technology. As for deepfake revenge porn, it uses artificial intelligence algorithms represented in the deepfake technique, as in cyber blackmail, the purpose is to harm the victim materially or morally, but in deepfake revenge porn, the purpose is pure revenge against the person using a pornographic clip.

(1) Ahmed Abdel-Mawgoud Zakir, The crime of deep pornographic counterfeiting, a comparative study, The Legal Journal, Cairo University Faculty of Law, Khartoum Branch, Volume 11, Issue 7, 2022, P. 2229.

(2) Mohamed Hassan Mekkawi, Cyber blackmail between threats and protection: A study of the Egyptian and American Legislation, Journal of Law and Emerging Technology (JOLETS), Volume 2, Issue 2, 2022, P.14. Available at: https://jolets.org/ojs/index.php/jolets/article/view/71 Accessed on 12-9-2023.

(3) Mahmoud Salama Al-Sherif, revenge porn crime through deep falsification and criminal responsibility for it, Journal of the Faculty of Law for Legal and Economic Research, Faculty of Law, Alexandria University, 2022, P. 403.

3.4.4.2 The Material pillar of the crime

Criminal behavior is a sequence of actions that passes through stages, each of which is considered an independent crime or an attempt to commit a crime. Firstly, collecting and withdrawing the victim's personal data, legally or illegally, second: creating and fabricating a video clip through personal data through artificial intelligence algorithms by installing images, audio, and video clips to produce a deepfake porn clip for the victim, whose counterfeiting is difficult to detect.

3.4.4.3 The Moral pillar of the crime

General MENS REA is needed and shall be represented by the criminal intention by the use of deepfake algorithms of personal data in order to create a fake porn video with the offender's intention to do such behavior.

3.4.4.4 The Crime's penalty

The Egyptian legislator did not stipulate a separate penalty for this crime, but rather it is punishable as part of the crime of processing the personal data of others, that is, according to the aforementioned Article 26.

The researcher recommends the necessity of stipulating a separate punishment for that crime and is not satisfied with the text of Article 26 alone. It is also clear that the legislator did not intensify the punishment if the purpose of the crime was pornographic revenge for the victim, although the law intensified the punishment in other cases in Article 34, such as disturbing public order or harming the country's national security. Therefore, it would have been better for the legislator to pay attention to the real risks that result from artificial intelligence algorithms and to provide deterrent criminal protection for them.

There is question arises about the provisions of criminal liability in publishing the fake sexual clip on social media?

One of two scenarios can be assumed to answer this question:

- First, if the user copies the fake sexual video to publish it through his social media account, he will be considered an original perpetrator for the crime of publishing.
- Or the user republishes (shares) the fake sexual video from another account; therefore, he will be considered an accessory contributor to the crime of illegal informational content.
- Whoever reacts to the fake sex video post is considered an affiliate contributor.

3.4.5 Summary for chapter 3

The researcher believes that the wide spread of deepfake techniques and their widespread use among all at a cheap cost sound a warning bell for the possibility of their illegal use endangering security and public peace. There is still no legal text to confront the illegal use of deepfake techniques, as it is one of the emerging issues that has not been addressed by the Egyptian legislator. However, a legal umbrella can be formed to counter this by using a set of laws that apply to the criminal acts perceived have been committed during this illegal exploitation. In addition, the fight against information technology crimes must be a comprehensive societal action in which all governmental and non-governmental agencies and civil society organizations join hands, not forgetting the role of the family, which is the first source from which a person draws his information and knowledge and builds his conscious awareness.

Based on the above, the researcher suggests some recommendations:

1. The need to add provisions in the Penal Code that criminalize the illegal use of artificial intelligence algorithms, such as deepfake illegal actions.
2. The need to tighten the text of Article 178 of the Penal Code, especially since it is a voluntary penalty, the fine does not exceed thirty thousand

pounds, and it is not commensurate with reparation for the material and moral damage that occurs as a result of the crime.

3. There is a need to add a paragraph to Article 26 of the Information Technology Crimes Law that tightens the punishment for the intentional publication of the processed content because it is only applied in intentional cases, but the penalties must be regulated in the event of the crime occurring by mistake as a result of negligence, recklessness, or others.

4. The need to add the purpose of «revenge porn» within the cases of severe punishment in Article 34 of the Anti-Cyber and Information Technology Crimes Law.

4. Conclusion

This paper has presented a critical and comprehensive analysis of the challenges of digital evidence usage in deepfake crimes. The paper extends our understanding of digital evidence challenges. The paper has attempted to go through the Budapest Convention on Cybercrime and US federal rules, in addition to the developments in Egyptian legislation.

The research proved that the Anti-cyber and Information Technology Crimes Law No. 175 of 2018 needs to be amended by adding new articles in order to regulate the AI illegal use acts, as well as that the current criminal procedure in Egypt lacks specific legal tools for online digital material acquisition in a trans-border context, so there is no exception to the principle of territoriality. Which is a logical result due to the refusal to join international agreements combating cybercrimes, so there is no obligatory order (just ethical) for states or companies to support Egypt with any data if needed.

4.1 Findings

1. The increment of using the internet led to criminals going online, and for

many reasons, such as having more criminal opportunities, a low risk of being arrested, crime becoming global and not committed in a certain territory or being obliged to a certain law, and targeting and collecting individual's personal data, they gained a lot of economic benefits.

2. Digital evidence usage is a must, as it has become the most important aspect of tracing criminals because any crime can have digital evidence, even if it is not a cybercrime.

3. The applicable rules of evidence in Egypt need to be developed to fit with the advent and challenges of the digital era. Conventional evidence-gathering means known to Egyptian law, such as ''search and seizure'', do not stand the test of time; they are insufficient to mitigate modern challenges associated with digital evidence.

4. The researcher noted that the judge can have his belief in any form and in everything that enters into his reassurance, and this means that if the digital evidence is not taken as evidence, it will be used as a presumption, and if the presumptions are gathered, evidence can emerge from them.

5. The law no. 175 of 2018 did not regulate all the safeguards that the Budapest Convention had, such as judicial supervision and other independent authority supervision; however, it regulated the grounds justifying the application of procedural powers, the limitation of the scope of powers, and the limitation of the duration of powers.

6. The executive regulation no. 1699 of 2020 of the law no. 175 of 2018 did not provide for controls related to cases of evidence being damaged at any stage of the investigation or trial, nor did it stipulate how to decrypt the digital evidence if it was encrypted.

7. The expansion of the risks of deepfake is due to digitizing personal data that can be used in deepfake content. Availability of applications and

methods that, without specialization, allow perpetrators of crimes via the Internet to hide their identities.

8. US laws do not criminalize deepfake in itself, as it is just a tool or means used by the offender to commit his crime; however, in exceptional cases, the legislator may criminalize it, especially crimes related to influence on the integrity of the electoral process or revenge porn through deepfakes.

9. There is still no legal text to confront the illegal use of deepfake techniques, as it is one of the emerging issues that has not been addressed by the Egyptian legislator. However, a legal umbrella can be formed to counter this by using a set of laws that apply to the criminal acts perceived to have been committed during this illegal exploitation.

4.2 Recommendations

1. Digital evidence usage requires a higher level of technical knowledge and expertise, specific training, and hands-on practical experience; therefore, the countries should conduct many technical and legal workshops delivered by international professionals to achieve such requirements.

2. The researcher suggests the need to impose a minimum amount of funds allocated in each ministry or institution for digital protection systems to fend off potential cyber-attacks.

3. The increment of the «internet of things» shows a great impact of how digital evidence is extremely important and highlights the massive need for legislation to fit it.

4. Reconsidering the formulation of the principle of legality of evidence to be more appropriate with the new digital era crimes, including deepfakes, as the articles shall be more appropriate and acceptable

for proof in light of the massive and wide development in information technology and digital transformation, and justice will not remain restricted because it is not proven.

5. Egypt shall join the Budapest Convention on Cybercrime, as it guarantees great international cooperation provisions, such as the 24/7 Office, which helps with urgent collection of evidence and expedited preservation, and ensures a balance between the requirements of law enforcement and the protection of human rights and liberties.

6. The Egyptian penal code (Article 178) punishes the crime contained therein with discretionary penalties that are not commensurate with the seriousness of deep forgery crimes, nor did it add any aggravating circumstances to punishment, and it did not take into account, for example, the case in which the victim is a minor or in other cases. Others to protect national unity and the country's reputation; therefore, the article shall be amended to include such cases.

7. The Law No. 175 of 2018 shall be amended in some articles, such as: Article 2, a better way to determine the criteria of data retention in a way that ensures more balance between national security and basic human rights such as the right to privacy. Article 25 shall punish cases of unintentional publication or disclosure of the image that is the subject of criminal behaviour as well as the damage that could result from publishing or violating the privacy of the victim. Article 26 shall not be an optional punishment, as it is not appropriate to address deepfake crimes in cases where the court may suffice with the penalty of a fine, and therefore the researcher recommends the necessity to add a paragraph in this article that stresses the punishment for the intentional publication of the processed content.

8. The executive regulation no. 1699 of 2020 of the law no. 175 of 2018

shall regulate how to decrypt the digital evidence if it was encrypted.

9. The researcher recommends the necessity of stipulating a separate punishment for the deepfake revenge porn crime.

4.3 List of references

Legislations

1. Convention on Cybercrime, Budapest, 23.XI.2001
2. Code of Virginia, § 18.2-386.2.
3. Texas-2019-SB751.
4. California Election Code § 20010
5. The Egyptian constitution 2014 amended in 2019
6. The Penal code no 58 of 1937
7. Anti-Cyber and Information Technology Crimes Law No. 175 of 2018

Books and Articles

1. Abdel Fattah Bayoumi Hijazi, Digital Evidence and Forgery in Computer and Internet Crimes, An In-depth Study of Computer and Internet Crimes, Bahjat for Printing and Binding, 2009.
2. Ahmed Abdel-Mawgoud Zakir, The crime of deep pornographic counterfeiting, a comparative study, The Legal Journal, Cairo University Faculty of Law, Khartoum Branch, Volume 11, Issue 7, 2022.
3. Ahmed Awad Bilal, The Rule of Excluding Illegally Obtained Evidence in Comparative Criminal Procedures, 3rd Edition Dar Al-Nahda Al-Arabia, 2013.
4. Ahmed Fathy Sorour, The Mediator in Penal Law, General Section, Sixth Edition, Cairo, Dar Al-Nahda Al-Arabiya, 2015.

5. Aju D, Anil Kumar Kakelli and Kishore Rajendiran, A Comprehensive Perspective on Mobile Forensics: Process, Tools, and Future Trends, Confluence of AI, Machine, and Deep Learning in Cyber Forensics, premiere reference resource, 2021.

6. Andrii Skrypnyk and Ivan Titko, Use of Information from Electronic Media in Criminal Proceeding of Several European States: Comparative Legal Research SOCRATES University Faculty of Law Electronic Scientific Journal of Law 3(15), 2019.

7. Ani petrosyan, Worldwide digital population 2023, Statista, 2023.

8. Anna-Maria Osula and Mark Zoetekouw, The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives. 11 Masaryk University Journal of Law and Technology, 2017.

9. Ashley Dean, Deepfakes, Pose Detection, and the Death of «Seeing is Believing», Law and Technology Today, 2022.

10. Betül Çolak, Legal Issues of Deepfakes, The institute of Internet & the just society, 2021.

11. Brett Lantz, Machine Learning with R, Packt Publishing Limited; 2 edition, 2015.

12. Chet Hosmer, Proving the Integrity of Digital Evidence with Time, 1st Int'l J. Of Digital Evidence, 2002.

13. Cybercrime Convention committee (T-CY) Guidance Note, Critical information infrastructure attacks, adopted by the 9th plenary of the T-CY 2013.

14. David Mugisha, Digital Forensics: Digital Evidence In Judicial System, International Journal of Cyber Criminology, 2019.

15. Dawn Lomer, 15 Types of Evidence and How to Use Them, I SIGHT, 2016.

16. Delphine Baize, De la contrefaçon à l'imitation, revue française de gestion, juin-juillet-aout, 1999.

17. Don Mason, Digital Evidence and Computer Forensics, National Center for Justice and the Rule of Law, 2013.

18. Emad Sayed Haidar, Primary Investigation of Computer Crimes, Ph.D. Thesis, Faculty of Law, Cairo University, 2018.

19. Eoghan Casey, Focused Digital Evidence Analysis And Forensic Distinguishers 18 Digital Investigation, 2016.

20. Gamil Abdel-Baki Al-Saghir, Procedural aspects related to the Internet, Dar Al-Nahda Al-Arabiya, 2001.

21. Gavin manes, Elizabeth Downing, Lance Watson and Christopher Thrutchley, New Federal Rules and Digital Evidence, Annual ADFSL conference on digital forencsics, security and Law, 2007.

22. Jean-Philippe Aumasson, serious Cryptography A Practical Introduction to Modern Encryption, San Francisco, 2018.

23. Jerry Norton, evidence meaning, The Editors of Encyclopaedia Britannica

24. John Letzing, How to tell reality from a deepfake, World Economic Forum, 2021.

25. Khaled Mamdouh Ibrahim, Informational Crimes, 1st edition, Alexandria: University Thought House, 2009.

26. Larry E. Daniel and Lars E. Daniel, Digital Forensics for Legal Professionals, Understanding Digital Evidence From The Warrant To The Courtroom, 1st edition, Syngress, 2012.

27. Mahmoud Salama Al-Sherif, revenge porn crime through deep falsification and criminal responsibility for it, Journal of the Faculty of Law for Legal and Economic Research, Faculty of Law, Alexandria University, 2022.

28. Mamdouh Abd al-Hamid Abd al-Muttalib, a proposed model for the rules for adopting digital evidence of evidence in computer crimes, published within the proceedings of the banking and electronic business conference organized by the Faculty of Sharia and Law at the United Arab Emirates University and the Dubai Chamber of Commerce and Industry, 2003.

29. Martin Novak, Digital Evidence in Criminal Cases before the U.S. Courts of Appeal: Trends and Issues for Consideration, Journal of Digital Forensics Security and Law, Volume 14 Number 4, 2020.

30. Mazen Abbas, Destroying Digital Evidence: Technical and Legal Dimensions, Master thesis, Cybercrime investigations professional master, Faculty of Law, British University in Egypt, 2022.

31. Mika Westerlund, The Emergence of Deepfake Technology: A Review, Technology Innovation Management Review 9, no. 11, 2019.

32. Mohamed El-Guindy, Applying Digital Forensics Methodology to Open Source Investigations in Counterterrorism. Journal of Law and Emerging Technologies, 1(1), 2021.

33. Mohamed Hassan Mekkawi, Digital Privacy in International Law and International conventions, Journal of Media Research and Studies, Issue Twenty, 2022.

34. Mohamed Hassan Mekkawi, Cyber blackmail between threats and protection: A study of the Egyptian and American Legislation, Journal of Law and Emerging Technology (JOLETS), Volume 2, Issue 2, 2022.

35. Piotr Lewulis, Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law, Criminal Law Law Forum33, Springer, 2022.

36. Ramses Benham, The General Theory of Criminal Law, Alexandria, Origin of Knowledge publishing, 1971.

37. Rashad Rasras, Ziad Alkadi, and Mutaz Rasmi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, Engineering technology and applied science researches, 2019.

38. Roman Dremliuga and Alexander Korobeev, A Fight against the Dissemination of Deepfakes in Other Countries: Criminal and Criminological Aspects, July 2021 Russian Journal of Criminology 15(3) 2021.

39. S.Suguna, V.Dhanakoti, and R.Manjupriya, A Study on Symmetric and Asymmetric key encryption algorithms, International Research Journal of Engineering and Technology (IRJET), 2016.

40. Sabika Tasneem & Sidra Jabeen, How to Overcome Major Problems in Handling Digital Evidence?, Vidizmo, 2022.

41. Standard opereating procedures for the collection, analysis and presentation of electronic evidence.

42. Tarik Sorour, Explanation of the Penal Code Special Section, Crimes of Persons and Money, second edition, Dar Al-Nahda Al-Arabiya, 2010.

43. The committee on the judiciary house of representatives, Federal Rules of Evidence, 2014.

44. William Y. Arms, Christophe Blanchi and Edward A. Overly, An Architecture for Information in Digital Libraries, D-Lib Magazine,

1997.

45. Xandra E. Kramer, Challenges of Electronic Taking of Evidence: Old Problems in a New Guise and New Problems in Disguise Il Conferencia Internacional & XXVI Jornadas Iberoamericanas de Derecho Procesal IIDP & IAPL, La Prueba en el Proceso / Evidence in the process Atelier 2018.

46. Yuezun Li and Siwei Lyu, Exposing DeepFake Videos by Detecting Face Warping Artifacts, 2019.

47. Zachary Roush, Digital Forensics: Data Recovery and Steps You Can Take to Assist in the Recovery Effort, JDSPURA, 2022.