Revenge Porn in the Digital Space: A Study on Criminalization and Legal Accountability

الإنتقام الإباحي في الفضاء الرقمي: دراسة في التجريم والمساءلة القانونية

Chikhi Nebia*, laboratory of land law and the environment, University of Mostaganem

nebia.chikhi@univ-mosta.dz

Received: *28/08 /2025* ***Accepted***: *29/10 /2025* ***Published***: *29/11 /2025*

Abstract:

Revenge porn stands as a prominent emerging cybercrime associated with digital transformation and the proliferation of social media. Its threat lies in publishing—or threatening to publish—a victim's intimate content without consent, for defamation or revenge. This act constitutes a direct violation of the right to privacy and human dignity, causing severe psychological and social consequences. Despite this crime's seriousness, practical experience reveals shortcomings in legal frameworks addressing it, as existing provisions often handle privacy protection broadly without explicitly criminalizing revenge porn. Therefore, studying this phenomenon is crucial to propose more precise legislative solutions and to benefit from comparative experiences in establishing an integrated legal framework that ensures effective victim protection and enhances digital and societal security.

Key words: Revenge Porn; Social Media; Digital Transformation; Criminalization; Legal Confrontation.

Introduction

The use of the Internet has expanded widely, becoming indispensable in various aspects of daily life. However, this tremendous utility is paralleled by a darker side, as the digital space has turned into a fertile environment for committing diverse crimes, particularly with the emergence of novel forms of cybercrime that were previously unknown. These crimes are becoming increasingly dangerous and complex due to the rapid technological advancements used in their commission. Among such emerging crimes stands out « revenge porn », which is considered one of the gravest cybercrimes because of the psychological, social, and legal harms it causes, and the complex challenges it poses to national legislations in the realm of criminalization and punishment.

In this context, it is worth noting that the wide spread of social media platforms has directly contributed to the aggravation of this crime, through the sharing of intimate photos, video clips, or live recordings without the consent of their owners, for the purpose of revenge or defamation. These platforms have thus become tools for violating privacy and circulating personal data without authorization, undermining the legal protection of the right to privacy and human dignity. Furthermore, practical experience has revealed the inadequacy of some traditional criminal provisions in confronting this crime, as they were often drafted to protect private life or personal data in general, without making explicit reference to the act of publishing intimate content for purposes of revenge[1].

Accordingly, the following central research problem arises: To what extent has the legal system been able to respond to the seriousness of revenge porn, in terms of its legal qualification,

*CorrespondingAuthor

criminalization, and punishment of perpetrators? What shortcomings hinder legal frameworks in addressing this act, and how can broader legal protection for victims be achieved?

Methodology: To address this problem, the research relies on the descriptive-analytical method by describing the crime of revenge porn and clarifying its forms and elements, followed by an analysis of relevant legal provisions to assess their sufficiency in confronting it. The study also employs the comparative method: drawing on the Egyptian legal experience, which has taken relatively advanced steps in this field, thereby allowing for recommendations to strengthen the Algerian legal system.

Significance and Objectives of the Study:

The importance of this study stems from the novelty of revenge porn as a crime and its direct link to a fundamental right—privacy and human dignity—alongside the growing number of victims due to the massive spread of social media. The study aims to:

Clarify the legal nature of revenge porn and highlight shortcomings in existing legal provisions.

Provide proposals and recommendations that contribute to strengthening victim protection under Algerian legislation.

The study is divided into two main parts:

1. The legal nature of revenge porn.
2. The legal confrontation of revenge porn.

1- Part One: The Legal Nature of Revenge Porn

Although harmful lies are not new, the ability to distort reality has surpassed all previous comparisons thanks to modern technology. Today's tools are capable of producing altered or fully fabricated images and videos that appear more convincing, realistic, and harder to detect than ever before.[2] These are designed to psychologically influence people through the notion of "perceptual manipulation",[3]by deceiving them with voices and videos of real individuals appearing to do or say things they never actually did. This practice is commonly referred to as revenge porn.

1.1-First: The Concept of Revenge Porn

Defining a comprehensive and precise legal concept of "revenge porn"—which is also referred to as deepfake pornography—does not in itself prevent its development or limit its spread. Most research confirms the expectation that such misuse will become increasingly widespread in the near future. Nevertheless, establishing a clear and comprehensive definition is considered an essential step toward understanding this phenomenon and formulating legal solutions capable of mitigating its risks.[4]

1.1.1. Definition of Revenge Porn

Revenge porn, or « deep fake pornography », is a modern form of visual and audio manipulation. It enables the production of realistic simulations of a person's face, voice, or movements in a way that makes it appear as though they said or did something they never actually did. This phenomenon is one of the most notable developments in the field of Artificial Intelligence[5] (AI) and synthetic media generation. These technologies allow the creation of realistic yet fabricated representations of people engaging in acts they never committed, as well as the creation of fictional images, objects, or even entirely fabricated events.

The term deep fake is composed of two parts:

Deep: referring to Deep Learning Models, an advanced data processing approach based on artificial neural networks.

Fake: meaning falsification or distortion of reality.

Some experts argue that the term refers to the illicit use of deep learning technology to create fabricated content[6].

Scholars have defined it in different ways:

A video produced using deep learning algorithms through easily accessible programs with high capabilities for creating manipulated content, such as by placing a targeted person's face on another person's body in a manner difficult to distinguish from reality[7]

Digitally altered audio or video recordings using machine learning algorithms, aimed at creating fictional scenes or events that never occurred, but appear convincingly real[8]

From these definitions, it is evident that most emphasize the technical characteristics of the practice. Therefore, a legal definition must also be established to reflect its nature. In this regard, deep fake revenge porn may be defined as:

"An application of artificial intelligence that allows the creation of digital content—audio, visual, or both—that imitates reality but contradicts the truth, with the intent of harming the targeted person or serving other unlawful purposes."

1.1.2. Forms of Revenge Porn:

Revenge porn is a crime that involves publishing or sharing sexually explicit or private images and videos of an individual without their consent, with the intent of revenge or defamation. Such acts often occur after the end of an intimate relationship or a dispute between two parties, where the offender exploits images or videos obtained during the relationship to harm the victim. This crime generally manifests in two main forms:

A. Deep fake Revenge Porn

Deep fake revenge porn is a defamatory practice that represents a new era of digital forgery. It uses advanced and complex software technologies that often make it impossible to distinguish between truth and fabrication.[9]Unlike ordinary manipulation, this form goes beyond simple tampering to represent a highly deceptive use of artificial intelligence (AI) in digital processing. It allows for altering content and manipulating images, voices, and gestures in ways that mimic reality with extreme accuracy.[10]

Article 26 of Egypt's Cybercrime Law No. 175 of 2018[11]defines "digital or electronic processing" as:

"Any technical operation or procedure carried out, wholly or partially, for the purpose of writing, collecting, saving, recording, storing, merging, displaying, receiving, transmitting, circulating, deleting, modifying, publishing, retrieving, or extracting electronic data and information, by using any electronic, magnetic, optical, or other modern technological means."

In Algerian law, digital or electronic processing denotes any systematic operation performed on personal data, regardless of whether it is conducted through automated digital systems or manual methods. This includes a wide range of actions, such as the collection, organization, storage, modification, consultation, transmission, encryption, or deletion of data. Law No. 18-07 of 2018[12] laid down this general definition, while Law No. 25-11 of 2025[13] further refined the concept by introducing modern elements—such as biometric data, pseudonymization, profiling, and data breaches—and by imposing stricter compliance obligations like appointing a Data Protection Officer (DPO), maintaining processing records, and conducting data protection impact assessments.

The term "deep fake revenge porn" emerged around 2017 when users of the platform Reddit applied AI algorithms to insert celebrities' faces into fabricated pornographic videos. This was done by altering visual content to appear authentic. In May 2019, Samsung developed a system capable of generating fake videos of individuals based on a single image, by mapping the facial geometry of the targeted person and overlaying it onto another person's face in a video.[14]

This type of crime essentially involves attributing statements or actions to a person that they never made, using advanced technological means.[15]At its core, deep fake revenge porn relies on cloning a voice, altering an image, or generating false text with the deliberate intent of misinformation, forgery, and reputation damage.

With the rapid advancement of computer software, especially image-editing programs like Photoshop, it has become possible to cut parts of people's photos and insert them into indecent or offensive images, then publish them on social media platforms such as Instagram, YouTube, or Facebook. Such acts constitute cybercrimes punishable by law, as they violate privacy, defame individuals, and harm their social standing.[16]

According to a 2019 report by the Dutch cybersecurity firm Startup Deep Trace, there were 14,698 fabricated videos uploaded to the Internet in just 10 months, 96% of which were pornographic.[17]

This crime has occurred in practice. In Egypt, a tragic case involved a young woman named Basant Khaled, who committed suicide after fabricated pornographic content falsely attributed to her was spread online. The perpetrators had used her personal photos, originally posted innocently on Facebook, to create fake sexual material. The Egyptian judiciary sentenced one of the offenders to six years in prison, in addition to confiscating devices and deleting all fake content.[18]

B. Conventional Revenge Porn

According to the United Nations Economic and Social Commission for Western Asia (ESCWA), conventional revenge porn is the deliberate distribution of sexually explicit materials without the subject's consent, most often online. Typically, the perpetrator is a former partner who misuses photos or videos obtained during a past relationship to humiliate or take revenge on the victim.

In other cases, hackers steal personal data from victims' phones or cloud accounts, then publish intimate images on social media platforms. In such cases, the offender may have had no prior personal relationship with the victim.

This crime is criminalized in Article 25 of Egypt's Cybercrime Law No. 175 of 2018, which states:

"Anyone who deliberately publishes, via an information network or any means of information technology, news, images, or similar material relating to a person's privacy without their consent—whether true or false—shall be punished by imprisonment for not less than six months and a fine of not less than fifty thousand Egyptian pounds and not exceeding one hundred thousand Egyptian pounds, or by either penalty."[19]

Therefore, the distinction between deep fake revenge porn and conventional revenge porn lies in their degree of criminal severity. Deep fake revenge porn represents a more advanced and deceptive form, since it does not merely involve leaking actual private material but rather fabricating entirely false content attributed to the victim using AI-driven data manipulation.

1.2-Second: The Elements of the Crime of Revenge Porn

Revenge porn is among the most dangerous crimes affecting both individuals and society, as it represents a blatant violation of privacy and causes severe psychological and social harm to victims. This crime relies on the use of technology to publish—or threaten to publish—private or sensitive content with the aim of defamation or revenge. To fully understand its legal nature, it is necessary to analyze its constitutive elements, which establish the occurrence of the crime and determine the offender's criminal liability.

1.2.1. The Material Element (actus reus)

The criminal conduct in this offense lies in the perpetrator's act of publishing digital content or using an information program to process another person's personal data with the purpose of associating it with material contrary to public morals.

Personal data refers to any information that makes it possible to identify a natural person, including any piece of information, image, or sound that relates to them, whether directly identifiable or indirectly.[20]

Revenge porn is classified as a successive act crime, meaning it typically unfolds in several stages, each of which may constitute a standalone crime or an attempt at committing it. These stages are as follows:[21]

Stage One: Data collection

(a) Publicly available data: The offender collects data voluntarily shared by the victim on social media platforms or websites. This behavior is criminalized under Article 2 of Law No. 151 of 2020 on the Protection of Personal Data (Egypt).[22]

It is observed that Algerian law does not expressly criminalize the act of collecting data voluntarily disclosed by individuals in the digital public sphere. However, the Algerian legislator has indirectly addressed this issue through Articles 394 bis to 394 bis 2 of the Penal[23]Code, which criminalize unlawful access, manipulation, or fraudulent exploitation of data, thereby broadening the scope of criminal protection to cover the misuse of personal information.

(b) Unauthorized access (hacking): The offender steals encrypted or protected personal data stored on the victim's phone, computer, or email, by unlawfully breaching accounts or devices. This constitutes the offense of illegal access under Article 14 of Law No. 175 of 2018 on Combating Cybercrimes.[24]

The act of seizing encrypted or protected data stored by the victim on their phone, computer, or email account through hacking constitutes a form of unlawful access criminalized by Algerian law. The Algerian legislator, through Articles 394 bis to 394 bis 2 of the Penal Code[25], has addressed this by criminalizing fraudulent access to information systems and the unlawful manipulation of digital data, including the possession or use of information obtained through illegal means.

Stage Two: Processing personal data

The offender processes the collected data through mixing operations and artificial intelligence techniques to fabricate images of the victim without their consent (e.g., placing the victim's face in compromising or immoral scenes).[26]

This may also include merging photos, voices, and videos to create false pornographic material attributed to the victim, or generating a fabricated sexual narrative under their name. Such acts require advanced technical skill in digital editing and content manipulation.[27]

For liability to be established, Article 25 of Egypt's Cybercrime Law No. 175 of 2018 requires that the processed data belongs to a third party (the victim). Thus, a person manipulating their own data, even if in an indecent manner, does not fall under this provision unless the content is shared with others. The offense is complete once the falsified content is linked to immoral or defamatory material, and its exposure to even one person suffices, including sending it only to the victim.[28]

Importantly, the legislator deliberately used the term "disclosure" rather than "publication", thereby broadening liability to cover private communications via email or social media messages. In such cases, the crime exists even in the absence of public dissemination.[29]

Similarly, the Algerian legislator, under Articles 394 bis to 394 bis 2 of the Penal Code[30], required for punishment of unlawful access or seizure of protected data that the act involves accessing an information system or electronic account without the owner's authorization. Accordingly, a person processing their own personal data is not considered to have committed the offense, even if the content involves sensitive or reputation-damaging information, unless it is made available or transmitted to others. An exception applies when another person's data is incorporated into the falsified content. Moreover, the Algerian legislator did not require the offense to reach a certain number of individuals; it is deemed committed even if only one person views the data, which reflects the orientation of Algerian law towards broad protection of digital information. Thus, it becomes clear that the Algerian legislator, similar to the Egyptian legislator,

sought to narrow the scope of criminal liability while ensuring the protection of personal data against any unlawful intrusion.

1.2.2. The Moral Element (mens rea)

The Egyptian and Algerian legislators require the presence of general criminal intent for liability to arise. This entails that the perpetrator deliberately employs algorithms or digital programs to manipulate images, voices, or videos, with full awareness that such conduct amounts to fabrication, falsification, and distortion of reality. This behavior materializes through the exploitation of another person's personal data to create false pornographic content attributed to the victim. In this regard, the Algerian legislator, under Articles 394 bis to 394 bis 2 of the Penal Code, explicitly criminalizes unlawful access to information systems and the seizure or manipulation of personal data, thereby safeguarding the right to privacy and human dignity.

2.Part Two: The Legislative Treatment of the Crime of Revenge

2.1. Porn: Between Criminalization and Shortcomings

Legal confrontation primarily relies on employing existing laws to effectively combat crimes, or enacting new laws to address emerging phenomena when existing provisions prove insufficient. At the beginning of the 21st century, for example, traditional laws were shown to be inadequate in addressing cybercrimes, which pushed legislators in most countries to adopt new laws tailored to the nature of such offenses.

In this context, the central question arises: To what extent are current laws sufficient to effectively confront the various forms of revenge porn, or is there a need to adopt special legislative provisions specifically addressing it?

2.1.1. First: The Egyptian Legislative Response to the Crime of Revenge Pornography

Egypt's Cybercrime Law No. 175 of 2018[31] contains a set of provisions that criminalize a range of unlawful behaviors, including:

Creating fraudulent websites, accounts, or email addresses and falsely attributing them to natural or legal persons.

Infringing upon the sanctity of private life.

Publishing or circulating unlawful digital content.

These provisions also cover behaviors such as sending repetitive electronic messages to a specific person without consent, disclosing personal data to third parties or websites for commercial use without authorization, and publishing news, images, or other material online in ways that violate others' privacy, regardless of whether the information is true or false.

Article 26 of the same law stipulates:

"Anyone who intentionally uses any program or technological means to process personal data belonging to another, in order to link it with content contrary to public morals, or to present it in a manner that would harm the victim's reputation, honor, or dignity, shall be punished with imprisonment for a period of not less than two years and not exceeding five years, and with a fine of not less than one hundred thousand Egyptian pounds and not more than three hundred thousand Egyptian pounds, or with either penalty."[32]

The law also defines "content" in Article 1 as:

"Any information that, by itself or when combined with other data, may lead to the deduction of new information, the identification of a trend or perception, the attribution of meaning, or the reference to other data."

While these provisions may be applied to criminalize certain forms of online revenge porn, they remain insufficient to provide a comprehensive and specialized legal framework capable of addressing all dimensions of this crime. Moreover:

The law does not make explicit reference to revenge porn or to other actors involved in such crimes, such as developers of deep fake technologies or service providers, and their responsibilities in limiting the spread of these materials.

It does not address the issue of redistribution or sharing of fabricated content, nor does it provide protection for the original content owners whose data was used to create fake materials.

The provisions lack detailed mechanisms for prevention and remediation, making them limited in scope.

2.1.2. Second: The Algerian Legislative response to the Crime of Revenge Pornography

National legislations in general have sought to provide protection against cybercrimes, with particular emphasis on safeguarding the right to privacy in the digital sphere. Revenge porn, defined as the non-consensual distribution of intimate content with intent to harm or defame, falls within this scope.

The Algerian legislator has enshrined the protection of privacy in successive constitutions—from the 1976 Constitution to the 2020 Constitution—most notably in Article 47, which guarantees the protection of this right.

Additionally, amendments to the Penal Code (Law No. 04-15) introduced Articles 394 bis and 394 bis 7[33], which address cybercrimes, alongside Articles 303 bis and 303 bis 3[34], which specifically criminalize the distribution of private images or recordings without the owner's consent. These provisions directly apply to acts of revenge porn.

Further, the Electronic Signature Law No. 15-04[35] strengthened data protection by prohibiting electronic certification providers from collecting or using personal data without explicit consent, restricting data use solely to what is necessary for authentication services. Violations are subject to criminal penalties under Articles 42, 43, 70, and 71 of the same law.

Moreover, other legislative[36] instruments have introduced dispersed provisions aimed at reinforcing the right to privacy. Within this broader context of safeguarding digital privacy, the Algerian legislator promulgated Law No. 18-07 of June 10, 2018,[37] on the protection of personal data. This statute offers additional guarantees regarding the processing and disclosure of personal information without the express consent of its owner. Article 2 expressly provides that "the processing of personal data, irrespective of its source or form, shall be carried out in a manner that respects human dignity, private life, and public freedoms, and without prejudice to the rights, honor, or reputation of individuals." Such principles are directly relevant to instances of revenge pornography, as these acts represent a flagrant breach of the values enshrined therein.

However, despite the legislator's efforts to address cybercrime through general provisions, the Algerian legal framework has not yet established a specific regulation that expressly criminalizes revenge porn. The existing provisions, such as those relating to violations of privacy or the unauthorized publication of images, remain of limited effectiveness when confronted with the digital nature of this offense and its profound impact on victims. Reliance on such traditional norms in practice leads to inconsistencies in judicial classification and weak deterrence, which exposes a clear shortcoming in the national legislative policy. Consequently, revenge porn continues to represent a gap within the Algerian criminal justice system—one that can only be filled through a dedicated legislative intervention that explicitly criminalizes the act and provides penalties proportionate to its gravity.

Accordingly, while the existing legal framework may permit the criminalization of certain behaviors associated with revenge pornography, it falls short in terms of both accuracy and comprehensiveness. Current provisions are generally framed within the broader protection of privacy and personal data, without offering clear or specific criminalization of the publication of intimate material for purposes of revenge or defamation. This legislative gap poses a substantive

difficulty in legal qualification and underscores the necessity for more specialized statutory intervention.

3.Conclusion

This study concludes that revenge porn over the Internet constitutes one of the most dangerous forms of cybercrime, given its blatant violation of privacy, its severe psychological and social impacts on victims, and its exploitation of modern technologies to broaden the scope of harm.

An analysis of the Algerian legal framework shows that while the legislator has established a system of legal provisions to protect informational privacy—including successive constitutions from 1976 to 2020, as well as Penal Code provisions (Articles 303 bis, 303 bis 3, 394 bis, and 394 bis 7)—these remain inadequate. Although these texts criminalize violations of private life through the unauthorized distribution of personal images or recordings, they do not explicitly define or criminalize revenge porn as a distinct offense.

Additional safeguards exist under Law No. 15-04 on Electronic Signatures and Law No. 18-07 of June 10, 2018, on the Protection of Personal Data, both of which emphasize respect for human dignity, private life, and freedoms. However, despite these protective measures, the absence of specific and detailed legal provisions addressing revenge porn remains a significant legislative gap that limits the effectiveness of prosecution and punishment.

This study has yielded key findings that shed light on the dimensions of revenge pornography, which can be presented as follows:

Current legal provisions criminalize acts infringing upon private life and digital privacy, but lack a clear definition or detailed description of revenge porn.

The absence of a legislative definition leads to inconsistency in the legal qualification of such acts.

Acts of revenge porn may be prosecuted under existing provisions on privacy or data protection, but such reliance on judicial interpretation leads to legal uncertainty.

The Algerian legal framework offers only partial and indirect protection for victims, relying on general provisions rather than specific rules.

The transnational and digital nature of the crime makes identifying perpetrators and collecting evidence particularly challenging.

In light of the conclusions reached in this study, the following recommendations are proposed:

- Strengthen the legislative framework by enacting clear and explicit provisions that specifically criminalize revenge porn in all its forms, with penalties proportionate to the gravity of the act and its impact on victims.
- Establish technical and judicial mechanisms for the rapid removal of unlawful content and effective tracking of perpetrators.
- Provide support mechanisms for victims, including legal counseling, psychological assistance, and confidential reporting channels.
- Develop robust digital evidence standards through unified technical and legal procedures for the collection and preservation of electronic evidence to ensure its admissibility in court.
- Create specialized units within law enforcement agencies to address cybercrimes of a sexual nature, equipped with advanced technical expertise.
- Promote public awareness campaigns to highlight the dangers of sharing or circulating intimate content without consent, targeting all age groups through education and media initiatives.

References:

[1]Al-Saeedi, Lubna Abdul-Hussein and Al-Saedi, Jalil Hassan – Compensation for Damages Arising from Cyberbullying: A Comparative Study – Al-Muasasa Al-Haditha lil-Kitab (The Modern Institution for Books) – 2021 – p. 11.
[2]Citron, Danielle K. & Chesney, Robert – Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security – California Law Review – Volume 107 – 2019 – p.1759. Available at: https://scholarship.law.bu.edu/faculty_scholarship/640 (last visited 30/7/2025).
[3]Purwadi, Ari and Rahmati, Citi – Legal landscape on National cyber security Capacity in Combating cyberterrorism using Deepfake technology in Indonesia – International Journal of Cyber Criminology – vol 16 – Issue 1 – 2022 – p.128.
[4]Vincent, James – Why we Need a Better Definition of Deepfake – The Verge – 2018. Available at: https://www.theverge.com/2018/5/22/17380230/deepfake-definition-ai-manipulation-fake-news (last visited 30/7/2025).
[5]Silverman, Craig – Verification Handbook for Disinformation and Media Manipulation – Al Jazeera Media Institute in collaboration with the European Journalism Centre – 2020 – p. 180.
[6]Pantserev, K.A. – The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability – In: H. Jahankhani, et al. (ed.) Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity – Springer, Cham – 2020. Available at: https://doi.org/10.1007/978-3-030-47946-7_2 (last visited August 04, 2025).
[7]Chan, C. Chun Ki, et al. – Combating Deepfakes: Multi-LSTM and Blockchain as Proof of Authenticity for Digital Media – IEEE/ITU – 2020. Available at: https://ieeexplore.ieee.org/abstract/document/9311067 (last visited July 17, 2025).
[8]Barber, A. – Freedom of Expression Meets Deepfakes – Synthese – 2023. Available at: https://doi.org/10.1007/s11229-023-04236-4 (last visited July 28, 2025).
[9]Youssef, Amir Faraj – Criminal and Civil Liability of Artificial Intelligence in Attacks on Information Security – Dar Al-Matbouat Al-Jame'iya (University Publications House) – 2023 – p. 387.
[10]Purwadi, Ari and Rahmati, Citi – Legal landscape on National cyber security Capacity in Combating cyberterrorism using Deepfake technology in Indonesia – International Journal of Cyber Criminology – vol 16 – Issue 1 – 2022 – p.130.
[11]Cybercrime Law No. 175 of 2018 – Official Gazette, Issue 32 (bis C), August 14, 2018. Available at: https://manshurat.org/node/31487 (accessed on August 1, 2025)
[12]Law No. 18-07 of June 10, 2018, on the Protection of Natural Persons in the Processing of Personal Data – Official Gazette, No. 34, June 10, 2018.
[13]Law No. 25-11 of 24 July 2025, amending and supplementing Law No. 18-07 of 10 June 2018 – published in the Official Gazette, No. 48, dated 24 July 2025.
[14]Youssef, Amir Faraj – Criminal and Civil Liability of Artificial Intelligence in Attacks on Information Security – Dar Al-Matbouat Al-Jame'iya (University Publications House) – 2023 – p. 387.

[15]Shorter, Mary – Artificial Intelligence and the Prevention of Violent Extremism: A Primer – Global Network on Extremism and Technology (GNET), International Centre for the Study of Radicalisation, King's College, London – p. 17.
[16]Al-Saidi, Lubna Abdul-Hussein and Al-Saidi, Jalil Hassan – Compensation for Damages Arising from Cyberbullying – A Comparative Study – Modern Book Institution – 2021 – p.106.
[17]Simon, Gabriella Ürmösné and Nyitrai, Endre – "The phenomena of epidemic crime, deepfakes, fake news, and the role of forensic linguistics" – Információs Társadalom XXI – no. 4 – 2021 – p.89. Available at: https://inftars.infonia.hu/pub/inftars.XXI.2021.4.5.pdf (last visited July 28, 2025).
[18]Mohamed, Asmaa Osama – Moral and Social Crimes on the Internet – Dar Al-Ahramat for Legal Publications – 2025 – p.89.
[19]Cybercrime Law No. 175 of 2018.
[20]Al-Marri, Bahaa – Crimes of Social Media – Al-Ahram Publishing House for Legal Publications – 2022 – p.394.
[21]Abdel-Moneim, Sulaiman – The General Theory of Criminal Law – University Publications House – 2014 – p.225.
[22]Law No. 151 of 2020, issuing the Personal Data Protection Law – Official Gazette, Issue 28 (bis E), July 15, 2020. Available at: https://masaar.net/ar/egypt_laws/ (accessed on July 31, 2025).
[23]Ordinance No. 66-156 of June 8, 1966, containing the Penal Code as amended by Law No. 04-15 of November 10, 2004.
[24]Cybercrime Law No. 175 of 2018.
[25]Ordinance No. 66-156 of June 8, 1966, containing the Penal Code.
[26]Mohammed, Asmaa Osama – Moral and Social Crimes on the Internet – Dar Al-Ahramat for Legal Publications – 2025 – p.93.
[27]Muwaafi, Ahmad Mahmud – Provisions of the Cybercrime Law – Al-Ahram Publishing House for Legal Publications – 2022 – p.643.
[28]Mohammed, Asmaa Osama – Moral and Social Crimes on the Internet – Dar Al-Ahramat for Legal Publications – 2025 – p.94.
[29] Hawraa Musa, Compound Crimes through Social Media – A Comparative Study, Dar Al-Nahda Al-Arabiya, Cairo, 2018, p.131.
[30]Ordinance No. 66-156 of June 8, 1966, containing the Penal Code.
[31]Cybercrime Law No. 175 of 2018.
[32]Cybercrime Law No. 175 of 2018.
[33]Ordinance No. 66-156 of June 8, 1966, containing the Penal Code.
[34]Ordinance No. 66-156 of June 8, 1966, containing the Penal Code as amended by Law No. 09-01 of February 25, 2009.
[35]Law No. 15-04 of February 1, 2015, establishing the general rules relating to electronic signature and certification – Official Gazette, No. 6, February 10, 2015.
[36]Law No. 18-05 of May 10, 2018, on Electronic Commerce – Official Gazette, No. 28, May 16, 2018.

Law No. 09-04 of August 5, 2009, containing special rules on the prevention and combating of crimes related to information and communication technologies – Official Gazette, No. 47, August 16, 2009.

[37]Law No. 18-07 of June 10, 2018, on the Protection of Natural Persons in the Processing of Personal Data.