International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Criminal Liability for Deepfake Crimes: Legal Classification Challenges in UAE Legislation Compared to French Law

Mohammed Hassan Khalifa bin Surour Al Ketbi[1], **Dr. Wan Abdul Fattah bin Wan Ismail**[2]

[1]PhD Candidate at Universiti Sains Islam Malaysia

[2]Professor, Faculty of Leadership and Management, Universiti Sains Islam Malaysia

Abstract: ***This study examines criminal liability for deepfake-related conduct and the challenges associated with its legal classification under UAE and French law. It evaluates the adequacy of relevant UAE criminal and cybercrime provisions and compares them with the French legal approach to manipulated digital content, privacy, identity, and image protection. Using descriptive-analytical and comparative legal methods, the study examines relevant legislation together with selected doctrinal and judicial approaches. The analysis indicates that UAE law primarily addresses deepfake-related conduct through general provisions concerning cybercrime, privacy, and forgery, which may create uncertainty in legal classification. French law provides comparatively more specific mechanisms for addressing certain forms of manipulated digital content. The study therefore recommends clearer UAE legislative provisions defining deepfake-related conduct and the applicable elements of criminal liability while maintaining appropriate protection for individual rights and freedoms.***

Keywords: Deepfake, Artificial Intelligence, Criminal Liability, Cybercrime, UAE Law, French Law.

1. Introduction

In recent years, the world has witnessed a qualitative transformation in technology-related crimes. These crimes are no longer limited to hacking or electronic fraud; rather, they have evolved to include the production of highly realistic fabricated digital content through what is known as deepfake technology. This development has led to the emergence of new forms of criminal behavior that are difficult to subsume under traditional legal classifications, raising fundamental challenges related to determining criminal liability and legally classifying acts associated with this technology.

In the UAE legal framework, technology-related crimes are addressed primarily through Federal Decree-Law No. 34 of 2021 on Countering Rumors and Cybercrimes. Although the Decree-Law does not use the term "deepfake," Article 44 is directly relevant because, in addition to protecting privacy, it criminalizes the use of an information system or information technology to modify or process a recording, photograph, or scene with the intent to defame or insult another person. The provision therefore reaches an important category of manipulated media, but it does not establish a comprehensive, technology-specific regime for all deepfake uses. French law provides a useful comparator because Article 226-8 of the Penal Code, as amended in 2024, expressly extends its rules on undisclosed montages to visual or audio content generated by algorithmic processing that represents a person's image or words without consent. The comparison is therefore not between complete absence and complete regulation, but between different levels and techniques of statutory specificity (Al-Ali, 2022).

The significance of this study lies in its attempt to analyze the legal classification challenges of deepfake crimes through a comparative approach between UAE legislation and French law, with the aim of identifying gaps in the current legal framework and proposing legislative solutions that are aligned with the nature of this phenomenon.

2. Research Problem

The research problem concerns the extent to which existing UAE criminal provisions provide a sufficiently clear and comprehensive legal classification for deepfake-related conduct. UAE law contains provisions capable of addressing particular manifestations of manipulated media, most notably Article 44 of Federal Decree-Law No. 34 of 2021, as well as general rules on forgery, fraud, defamation, privacy, and criminal participation. Nevertheless, these provisions do not define deepfakes as a distinct legal concept or provide a unified classification covering their varied uses. This may create uncertainty as to which offense applies in a particular case and how the material and mental elements should be established. French law offers a useful comparative model because Article 226-8 expressly addresses certain algorithmically generated visual or audio content, while other Penal Code provisions remain applicable according to the legal interest affected.

3. Research Questions

1) To what extent are the legal provisions in UAE legislation—particularly those contained in the UAE Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes—adequate in addressing acts associated with deepfake technologies?
2) To what extent can deepfake-related conduct be classified under existing offenses in UAE law, such as forgery, privacy violations, defamation, or fraud, in the absence of a comprehensive deepfake-specific legal framework?

3) What practical challenges may judicial authorities in the UAE face when applying current legal texts to deepfake-related crimes?
4) How has French law addressed acts related to digital manipulation, particularly about the protection of image and digital identity, and how clear is their legal classification?
5) What are the fundamental differences between UAE legislation and French law in determining criminal liability for the use of deepfake technologies?
6) What is the most appropriate legal model that the UAE legislator could adopt to regulate the legal classification of deepfake crimes?

4. Research Objectives

1) To analyze the adequacy of legal provisions in UAE legislation for classifying deepfake crimes by applying them to real-life scenarios.
2) To identify the practical challenges faced by the UAE judiciary in determining criminal liability for acts related to deepfake technology.
3) To examine how French law addresses digital manipulation crimes, particularly regarding the protection of identity and image, and to identify areas of legislative advancement.
4) To conduct an applied comparative analysis between UAE legislation and French law in terms of legal classification, to identify strengths and weaknesses in each system.
5) To propose a comprehensive legal framework for improving the legal classification of deepfake crimes in UAE legislation, in line with the nature of this technology.
6) To support the development of a specialized legal regulation for deepfake crimes that clearly defines the elements of the offense and criminal liability.

5. Research Methodology

This study adopts a descriptive-analytical approach by examining the legal rules relevant to deepfake-related conduct in UAE and French law, together with a comparative method used to identify similarities, differences, and potentially transferable legal approaches. The statutory provisions were selected because they directly govern manipulated images or recordings, privacy and reputation, forgery, fraud, criminal intent, or participation—issues that recur in deepfake scenarios. Judicial and doctrinal materials were considered where they clarify the interpretation or practical application of those provisions. The study also draws on contemporary scholarship concerning artificial intelligence, digital evidence, and cybercrime to assess whether conventional criminal-law categories adequately accommodate technologically generated or manipulated content (UNODC, 2023; Europol, 2022).

5.1 Conceptual Framework and Legal Classification of Deepfake Crimes (Comparative Study)

The rapid development of artificial intelligence technologies, particularly deepfake technologies, has transformed the ways in which false or manipulated representations can be created and circulated. Deepfakes typically depend on advanced machine-learning techniques capable of synthesizing or altering audiovisual content with a high degree of realism (Goodfellow et al., 2016; Mirsky & Lee, 2021). For criminal law, the central difficulty is not that digital conduct falls outside law altogether, but that one technological act may implicate several protected interests- privacy, reputation, property, evidentiary integrity, or identity- each of which may trigger a different legal classification.

UAE legislation addresses relevant conduct through a combination of technology-specific and general criminal provisions. Article 44 of Federal Decree-Law No. 34 of 2021 on Countering Rumors and Cybercrimes protects privacy and, importantly, separately penalizes the use of an information system or information technology to modify or process a recording, photograph, or scene with the intent to defame or insult another person. This wording can apply directly to some deepfake scenarios, although it is limited by the conduct and intent specified in the provision. Other deepfake uses may instead fall under forgery, fraud, defamation, or participation rules. Accordingly, the principal UAE challenge is the absence of a unified deepfake-specific classification rather than the complete absence of provisions applicable to manipulated media (Al-Kaabi, 2024; Al-Harasi, 2023).

French law combines general criminal provisions with a more explicit rule on manipulated and algorithmically generated representations. Article 226-1 of the French Penal Code protects private life in specified circumstances, including the non-consensual capture, recording, or transmission of a person's image in a private place. More directly, Article 226-8, as amended in 2024, criminalizes communicating to the public or a third party, without consent and without obvious or express disclosure of its artificial character, a montage using a person's words or image; it expressly assimilates algorithmically generated visual or audio content representing that person's image or words. Article 441-1 separately defines forgery as a fraudulent alteration of truth, capable of causing harm, in a writing or other medium expressing thought that establishes or may establish proof of a right or legally consequential fact. These provisions illustrate distinct routes of classification according to the protected interest and function of the manipulated content (Chesney & Citron, 2019).

5.2 The Nature of Deepfakes and Their Legal Characterization

Deepfakes represent advanced applications of artificial intelligence that rely on deep learning algorithms to produce digital content closely simulating reality. This raises significant questions regarding their legal nature and the possibility of incorporating them within traditional criminal law concepts.

UAE legislation does not provide a statutory definition of "deepfake." The technology can nevertheless fall within the broad technological concepts used by Federal Decree-Law No. 34 of 2021, and Article 44 expressly reaches the modification or processing of a recording, photograph, or scene when undertaken through an information system or information technology with the intent to defame or insult

Paper ID: SR26908093519 DOI: https://dx.doi.org/10.21275/SR26908093519

another person. Thus, some manipulated-media conduct is directly addressed, while other deepfake scenarios must be classified through different offenses according to their purpose and effect. This fragmented coverage, rather than a total legislative vacuum, is the principal classification challenge (Mirsky & Lee, 2021).

French law addresses manipulated representations more expressly. Article 226-1 protects private life in the circumstances specified by the provision, while Article 226-8, following its 2024 amendment, covers undisclosed montages and algorithmically generated visual or audio content representing a person's image or words without consent. The latter provision is particularly relevant to deepfakes because it refers directly to algorithmically generated content rather than requiring the technology to be fitted solely into traditional categories (Muharram, 2022; Citron, 2020).

The legal nature of deepfakes can be understood as a technological means of altering reality, which opens the possibility of classifying them under forgery offenses, particularly when used as a tool for proof or deception. In UAE law, Article (251) of the UAE Federal Decree-Law No. 31 of 2021 on Crimes and Penalties defines forgery as "the alteration of truth in a document by one of the methods specified by law with the intent to use it," a provision that could extend to fabricated digital content. However, a key issue lies in determining whether video or audio content constitutes a "document." Article (252) further criminalizes the use of forged documents, which may include deepfake materials used as evidence.

In contrast, Article 441-1 of the French Penal Code provides a broader definition of forgery that includes any means of proof without limiting it to traditional documents. This flexibility allows deepfake content to be more readily classified as forgery within the French legal framework.

Deepfake technology is therefore better understood as a method capable of facilitating different offenses rather than as a single offense with one invariant legal classification. In the UAE, Article 44 directly addresses certain manipulated recordings, photographs, or scenes when the specified defamatory or insulting intent is present, while other uses may engage forgery, fraud, privacy, or participation provisions. In France, Article 226-8 expressly addresses certain undisclosed algorithmically generated representations, while Articles 441-1 and 313-1 may apply where the content functions respectively as legally consequential false evidence or as a means of fraud. Classification in both systems must consequently remain tied to the elements of the applicable offense and the protected legal interest.

The comparative issue is therefore one of scope, precision, and coordination among existing offenses. UAE law already contains a significant manipulated-media rule in Article 44, but a clearer statutory definition and coordination framework could reduce uncertainty where deepfake conduct falls outside its specified intent or overlaps with forgery, fraud, privacy, or other offenses (Al-Dulaimi, 2022).

5.3 Legal Classification of Deepfake Crimes (In-Depth Comparative Study)

Legal classification in the UAE depends on the factual purpose and effect of the deepfake. Article 44 of Federal Decree-Law No. 34 of 2021 is central: it criminalizes specified technology-enabled invasions of privacy and also penalizes modifying or processing a recording, photograph, or scene through an information system or information technology with the intent to defame or insult another person. Article 43, by contrast, concerns insult and defamation through digital means and may be relevant where manipulated content is used to insult another or attribute to that person a fact exposing them to punishment or contempt. These provisions demonstrate that UAE law can reach several deepfake scenarios, but through offense-specific elements rather than through a single deepfake classification (Al-Shamsi, 2021).

French Article 226-8 is more explicit with respect to synthetic representation. Since the 2024 amendment, it covers not only undisclosed montages made with a person's words or image without consent, but also visual or audio content generated by algorithmic processing that represents the person's image or words, where its generated character is neither obvious nor expressly disclosed. This provision therefore supplies a direct statutory basis for an important category of deepfake dissemination, while Articles 226-1, 441-1, and 313-1 remain relevant where the conduct instead implicates private-life intrusion, legally consequential falsification, or fraud. The comparative distinction is thus one of statutory specificity and the organization of overlapping offenses, rather than a simple contrast between regulation and non-regulation (Al-Ali, 2022).

From another perspective, deepfake conduct may be classified under forgery offenses in UAE legislation, particularly when fabricated content is used to prove false facts or mislead justice. Article (251) of the UAE Federal Decree-Law No. 31 of 2021 on Crimes and Penalties defines forgery as "the alteration of truth in a document, in one of the ways specified by law, in a manner likely to cause harm, with the intent of using it as a valid document," while Article (252) criminalizes the use of a forged document with knowledge of its falsity.

Applying UAE forgery provisions to deepfake content requires careful attention to the statutory concept of a document and to the legally relevant function of the fabricated material. Article 251 of Federal Decree-Law No. 31 of 2021 defines document forgery as changing the genuineness of a document by specified means, resulting in harm, for the purpose of using it as a valid instrument. A deepfake video or audio file will not automatically satisfy these elements merely because it is false; its legal treatment depends on whether it falls within the statutory notion of a document and is used in the manner required by the offense (Bayouwi, 2026; Abdelhamid, 2022). In France, Article 441-1 is broader in form, covering a fraudulent alteration of truth by any means in a writing or other medium expressing thought where that medium establishes or may establish proof of a right or a fact with legal consequences. Importantly, Article 441-2 concerns forgery of documents issued by a public administration and should not be treated as a general provision governing all uses of deepfake evidence.

Additionally, deepfake conduct may, in certain cases, be classified under fraud or deception offenses, particularly when used to mislead others and obtain unlawful benefits. This introduces another layer of complexity in determining the appropriate legal characterization. In UAE law, fraud provisions within the Penal Code may be invoked, which require the presence of deception and intent to obtain a benefit. However, proving these elements in deepfake cases may be challenging, especially given the difficulty of establishing criminal intent.

By contrast, French law does not rely on a single classification but allows for multiple legal characterizations depending on the nature of the act. Article 313-1 of the French Penal Code defines fraud as "the use of fraudulent means to deceive a person and induce them to deliver funds or a benefit," which may include the use of fabricated videos. Moreover, French law permits the combination of legal provisions- such as those related to forgery and violations of privacy—thereby offering significant flexibility in classification.

The comparison therefore shows overlapping classification pathways in both systems. UAE law contains a direct manipulated-media clause in Article 44 but does not provide a unified deepfake concept covering all purposes and harms. French law offers greater express specificity for undisclosed algorithmically generated representations through Article 226-8, while still relying on separate offenses such as forgery and fraud when their distinct elements are satisfied. The practical task in either system is to select the offense whose elements correspond most closely to the conduct rather than to assume that every deepfake belongs to one category (Vaccari & Chadwick, 2020).

5.4 Jurisprudential and Judicial Trends in the Legal Classification of Deepfake Crimes (In-Depth Comparative Study)

Legal scholarship in the UAE tends to treat deepfake technology as a technical means used to commit existing crimes, rather than as an independent offense. This approach is based on the absence of explicit legislative provisions addressing deepfakes, requiring reliance on general provisions such as Article (44) of the UAE Federal Decree-Law No. 34 of 2021 on Combating Rumors and Cybercrimes, concerning violations of privacy, and Article (251) of the UAE Penal Code, concerning forgery. However, this approach has been criticized in legal scholarship because it may lead to different legal classifications for the same act, thereby weakening the stability of the legal rule.

In contrast, French legal scholarship tends to expand the scope of existing provisions to include deepfake conduct. It relies on Articles 226-1 and 226-8 of the French Penal Code to protect a person's image, and on Article 441-1 to criminalize forgery. This provides a clearer legal basis for classifying such crimes. Some French scholars also call for the enactment of specific provisions on digital falsification, reflecting a more advanced awareness of the nature and risks of this phenomenon.

Published UAE legal materials do not yet demonstrate a sufficiently developed and uniform body of deepfake-specific case law to support a claim of settled judicial classification. In practice, courts must apply the elements of existing offenses to the facts before them, including Article 44 where manipulated recordings, photographs, or scenes are used with the specified intent, Article 43 where digital insult or defamation is alleged, and the general provisions governing forgery, fraud, and participation. The novelty and technical complexity of synthetic media can nevertheless make evidentiary authentication and the identification of the responsible actor particularly important (Casey, 2020; Europol, 2022).

The French statutory position is clearer than the manuscript's earlier formulation suggested because Article 226-8 now expressly refers to algorithmically generated visual or audio content. This reduces the need to rely solely on expansive interpretation for that category of conduct. At the same time, the application of forgery provisions remains dependent on the elements of Article 441-1, including a fraudulent alteration of truth, potential harm, and the evidentiary or legally consequential function of the relevant medium. The comparative analysis therefore rests primarily on verified statutory differences rather than on an assumption that French courts have already developed a comprehensive body of deepfake jurisprudence.

Overall, French law currently provides a more express statutory route for certain deepfake representations through Article 226-8, whereas UAE law addresses manipulated media through Article 44 and other offense-specific provisions without defining deepfakes as a unified legal category. The resulting policy question is whether UAE law would benefit from clearer definitions and coordination rules that preserve the existing protections while improving predictability across different deepfake scenarios.

6. Criminal Liability for Deepfake Crimes (Comparative Study)

The issue of criminal liability for deepfake crimes is among the most complex challenges in contemporary criminal law, due to the overlap between technical elements and the traditional legal components of crime. This raises fundamental questions about the adequacy of classical criminal law concepts in addressing such phenomena. Deepfakes are not merely simple material acts; rather, they result from complex technical processes that may involve multiple actors, such as software developers, users, and publishers, thereby complicating the determination of criminal liability for each party (Kietzmann et al., 2020).

In UAE law, criminal liability for deepfake-related conduct must be established through the elements of the particular offense invoked and the general rules governing responsibility and participation under Federal Decree-Law No. 31 of 2021 on Crimes and Penalties. The analysis therefore requires proof of the prohibited conduct and the mental element required by the relevant provision, rather than assuming that the technical production of a deepfake is criminal in itself.

French law similarly requires attention to the mental element specified by the applicable offense. Article 121-3 of the French Penal Code states the general rule that there is no felony or misdemeanor without intent to commit it, while recognizing negligence or breach-of-duty liability only where the law specifically provides for it. The provision therefore does not create a general negligence basis for every deepfake offense. Criminal liability must instead be assessed under the elements of Article 226-8, Article 441-1, Article 313-1, or another applicable offense, together with the general rules on participation.

6.1 The Material Element in Deepfake Crimes

The material element constitutes the foundation of criminal liability and consists of criminal conduct, the resulting harm, and the causal link between them. However, applying this element to deepfake crimes raises significant challenges, particularly regarding the nature of conduct itself, as it is not a direct physical act but is conducted through complex technological means.

In UAE legislation, Article 44 of Federal Decree-Law No. 34 of 2021 is particularly important to the material element. It covers specified forms of privacy invasion through information technology and separately penalizes the modification or processing of a recording, photograph, or scene through an information system or information technology when accompanied by an intent to defame or insult another person. Article 43 may additionally apply where the digital content itself constitutes insult or defamation. These provisions can encompass important stages of deepfake misuse, although not every act of technical creation is criminalized independently of purpose, intent, or subsequent use.

French law distinguishes among different forms of conduct. Article 226-1 addresses specified intrusions into private life, including non-consensual image capture, recording, or transmission in a private place. Article 226-8 more directly targets the act of communicating an undisclosed montage or qualifying algorithmically generated visual or audio content to the public or a third party without consent. Accordingly, Article 226-8 is principally a dissemination provision; it should not be described as independently criminalizing every production stage. This distinction is important when identifying the precise material act required for liability (Muharram, 2022).

Another issue arises concerning the criminal result. Deepfake content may be produced without causing actual harm, raising the question of whether a crime has occurred. In UAE law, some offenses require the existence of harm, such as forgery under Article (251) of the UAE Federal Decree-Law No. 31 of 2021 on Crimes and Penalties, which requires that the alteration of truth be capable of causing damage. This may be difficult to establish in certain deepfake cases.

French law does not dispense with the statutory elements of harm or protected-interest infringement. Under Article 226-8, liability turns on the communication of the specified montage or algorithmically generated content without consent and without adequate disclosure of its artificial character; proof of a separate consequential injury is not stated as an additional element. Article 441-1, by contrast, expressly requires an alteration of truth capable of causing prejudice and a medium linked to proof of a right or legally consequential fact. The appropriate analysis therefore depends on the offense invoked rather than on a general proposition that French law treats harm more flexibly (Bayouwi, 2026).

The causal link represents one of the most complex elements in deepfake crimes, due to the multiplicity of actors involved in producing and disseminating content. This complicates the identification of the party responsible for the result. In UAE legislation, no specific provision addresses this issue, and reliance is placed on general principles, such as Article (39) of the UAE Federal Decree-Law No. 31 of 2021 on Crimes and Penalties, which establishes that an offender is responsible for the consequences of their actions. However, this may be insufficient in complex technological crimes.

In contrast, French law explicitly addresses this issue. Article 121-7 of the French Penal Code establishes liability for accomplices, enabling the distribution of responsibility among multiple actors. This aligns more effectively with the nature of deepfake crimes. Accordingly, French law demonstrates a greater capacity to address causation in such cases (Kietzmann et al., 2020).

6.2 The Mental Element (Criminal Intent) in Deepfake Crimes (In-Depth Comparative Study)

The mental element- represented by criminal intent—constitutes one of the most essential components of criminal liability. In the context of deepfake crimes, it raises a particularly complex issue related to proving the offender's knowledge of the technical nature of the act and its legal consequences, especially given the technological sophistication of such crimes.

In UAE deepfake cases, the required mental element must be derived from the offense charged. Article 44 of Federal Decree-Law No. 34 of 2021 is especially significant because its manipulated-media clause expressly requires an intent to defame or insult another person. Where forgery, fraud, or another offense is invoked, the prosecution must establish the distinct knowledge or purpose required by that provision. This offense-specific approach can create evidentiary difficulty where several actors participate in creating, editing, uploading, or redistributing synthetic content.

French Article 121-3 should be read more narrowly than a general rule of liability for fault. It establishes intentionality as the default for felonies and misdemeanors and permits negligence, imprudence, or breach-of-duty liability only where legislation expressly provides for it. Consequently, deepfake-related liability cannot be expanded to negligence merely because the technology is complex. For Article 226-8, Article 441-1, fraud, or complicity, the mental element must be established according to the wording and interpretation of the particular offense (Westerlund, 2019).

Paper ID: SR26908093519 DOI: https://dx.doi.org/10.21275/SR26908093519

Another issue arises concerning specific intent, particularly in forgery-related deepfake offenses, where the law requires an intention to use the fabricated content as evidence or as a means of deception. In UAE legislation, Article (251) of the UAE Federal Decree-Law No. 31 of 2021 on Crimes and Penalties defines forgery as “the alteration of truth in a document with the intent to use it,” meaning that merely creating manipulated content is insufficient to establish the crime; rather, the intent to use it must be proven. This places a significant evidentiary burden on the prosecution in deepfake cases. Article (252) further criminalizes the use of forged documents, reinforcing the importance of this specific intent.

Under French law, Article 441-1 does not simply define forgery as any false content intended for use as evidence. It requires a fraudulent alteration of truth, capable of causing prejudice, made by any means in a writing or other medium expressing thought whose object or possible effect is to establish proof of a right or a fact with legal consequences. A deepfake can therefore fall within the provision only when those elements are satisfied. This more precise formulation avoids treating all synthetic media as forgery and keeps the classification tied to the evidentiary or legally consequential function of the content (Fadel & Abbas, 2022).

Deepfake cases may also raise questions about indirect or risk-aware states of mind, but such concepts should not be presumed to apply uniformly across offenses. In UAE law, liability remains tied to the mental element required by the relevant statutory provision, including the express intent to defame or insult under the manipulated-media clause of Article 44. Any extension to other forms of intent must therefore be grounded in the applicable general and special criminal-law rules rather than inferred from the technology itself.

The same caution applies in French law. Article 121-3 permits negligence or imprudence liability only when the law provides for it; negligence should not be equated with dol éventuel or treated as an automatic basis for liability for deepfake conduct. For intentional offenses, the prosecution must establish the mental element required by the specific provision. The comparative advantage of French law lies more clearly in the express coverage of certain algorithmically generated representations under Article 226-8 than in any generalized relaxation of mens rea requirements.

Accordingly, legislative development should focus on defining the mental element for any new deepfake-specific offense with precision, distinguishing intentional deception or harm from legitimate, disclosed, artistic, satirical, educational, or otherwise lawful uses. Such clarity would strengthen legal certainty without creating an overbroad form of technology-based liability.

6.3 Distribution of Criminal Liability among Actors in Deepfake Crimes

The distribution of criminal liability among actors represents one of the most significant challenges in deepfake crimes, due to the multiplicity of parties involved in producing and disseminating fabricated content, such as software developers, users, and publishers. This raises questions regarding the scope of liability attributable to each party.

In UAE legislation, reference is made to the rules of criminal participation. Article (45) of the UAE Federal Decree-Law No. 31 of 2021 on Crimes and Penalties provides that “a perpetrator is any person who commits the crime alone or jointly with others,” while Article (46) establishes the liability of accomplices. These provisions allow for the distribution of liability among participants. However, they do not address the specific nature of technological crimes, where it may be difficult to determine the precise role of each party.

French law addresses complicity through Articles 121-6 and 121-7 of the Penal Code. Article 121-6 provides that an accomplice is punishable as a perpetrator, while Article 121-7 defines complicity to include knowingly facilitating the preparation or commission of a felony or misdemeanor by aid or assistance, as well as specified forms of intentional instigation or instruction. These provisions are relevant to multi-actor deepfake cases, but liability still requires proof of the statutory conditions for complicity rather than mere technical involvement (Bayouwi, 2026).

Another issue concerns the liability of software developers. UAE legislation does not contain an explicit provision defining their liability for the use of deepfake technologies, leaving the matter to judicial interpretation based on general rules, such as Article (45) of the Penal Code. This may lead to inconsistency in judicial rulings.

Under French Article 121-7, a software developer or other technical contributor would not incur accomplice liability merely because a tool was capable of misuse. The prosecution would need to establish knowing assistance that facilitated preparation or commission of the offense, or another form of complicity recognized by the provision. The same analytical caution is important in UAE law: liability should distinguish neutral technology development from intentional participation in a specific criminal use (Al-Dulaimi, 2022).

The distribution of liability in deepfake cases should therefore be based on the conduct and mental state of each participant. General participation rules in both systems provide a foundation, but synthetic-media cases may make proof more difficult because creation, model development, editing, publication, and redistribution can be performed by different actors. A clearer UAE framework could specify how existing participation rules apply to these roles without imposing liability solely on the basis of providing general-purpose technology.

Legislative clarification in the UAE could therefore focus on role-specific conditions for liability, especially for creators, knowing facilitators, and disseminators, while preserving the requirement to prove the elements of participation and the underlying offense. This approach would improve predictability without converting ordinary software development or platform operation into automatic criminal responsibility (Bayouwi, 2026).

7. Conclusion

The comparative analysis demonstrates that deepfake-related conduct creates significant difficulties for conventional rules governing criminal classification and liability. UAE legislation provides mechanisms through cybercrime, privacy, forgery, fraud, and participation provisions, but the absence of express treatment of deepfake technology can produce uncertainty concerning classification, intent, causation, and the responsibility of multiple actors. The French framework offers useful comparative guidance through provisions addressing image protection, falsification, forgery, and participation. UAE legislation would therefore benefit from clearer treatment of manipulated AI-generated content, including its definition, relevant material and mental elements, digital evidentiary implications, and the conditions governing liability for persons involved in its creation or dissemination. Legislative clarification should preserve legal certainty while maintaining an appropriate balance between effective criminal enforcement and the protection of individual rights and freedoms.

8. Findings

The principal findings are as follows:

1) The study demonstrated that deepfake technology represents a qualitative transformation in criminal behavior, as criminal acts are no longer based on direct physical alteration but rather on the creation of an alternative digital reality, thereby weakening the effectiveness of traditional criminal law concepts.
2) UAE legislation does not define deepfakes as a distinct legal concept. Nevertheless, Article 44 of Federal Decree-Law No. 34 of 2021 expressly reaches the modification or processing of a recording, photograph, or scene through information technology when undertaken with the intent to defame or insult another person, while other deepfake uses may fall under different offenses.
3) Legal classification in the UAE may therefore vary among Article 44 manipulated-media conduct, digital defamation, forgery, fraud, privacy violations, and participation, depending on the facts and statutory elements. The challenge is fragmentation and overlap rather than complete absence of applicable law.
4) French law provides a more explicit statutory route for an important category of deepfake dissemination. Article 226-8, as amended in 2024, expressly covers qualifying algorithmically generated visual or audio content representing a person's image or words without consent where its artificial character is not obvious or expressly disclosed. Articles 441-1 and 313-1 remain separately applicable where their elements of forgery or fraud are satisfied.
5) The mental element must be established under the offense in both systems. French Article 121-3 does not create general negligence liability for deepfake conduct; negligence or imprudence applies only where legislation provides for it. UAE Article 44, for its manipulated-media clause, expressly requires intent to defame or insult.
6) The distribution of criminal liability among creators, users, disseminators, developers, and other contributors must remain tied to the participation rules and the proven mental state of each actor. French Articles 121-6 and 121-7 provide a structured complicity framework, while UAE general participation rules remain applicable to multi-actor conduct.
7) Digital evidence remains central to deepfake prosecutions because authenticity, attribution, provenance, and causation may be contested. The increasing realism of synthetic media strengthens the need for reliable forensic procedures and clear evidentiary standards.
8) The principal comparative difference is therefore the degree of express statutory treatment: French Article 226-8 directly names algorithmically generated visual or audio content, whereas UAE law addresses important manipulated-media scenarios without adopting a comprehensive deepfake-specific definition.
9) Overall, deepfake technology presents both technical and legal challenges. Legislative clarification should improve certainty while preserving offense-specific requirements, evidentiary safeguards, and protection for lawful expression and legitimate uses of synthetic media.

9. Recommendations

In light of these findings, the study recommends targeted legislative clarification rather than assuming that existing UAE law is wholly silent on manipulated media. The objective should be to coordinate current protections, close identifiable gaps, and maintain legal certainty and proportionality.

1) The UAE legislator should consider adopting a statutory definition of deepfake or synthetic manipulated media that is technologically neutral and clearly distinguishes covered conduct from legitimate disclosed or consensual uses.
2) Any new offense should complement, rather than duplicate, Article 44. It should specify the prohibited acts—such as creation for a criminal purpose, deceptive dissemination, or use—and define the required mental element and protected interests with precision.
3) The application of document-forgery provisions to AI-generated audiovisual material should be clarified. Any reform should specify when digital audiovisual content qualifies as a legally relevant document or evidentiary medium, rather than presuming that every deepfake is a forged document.
4) Criminal evidence rules and forensic practice should provide clear standards for authentication, provenance, integrity, expert examination, and evaluation of AI-generated or AI-manipulated evidence, thereby reducing the risk that fabricated content is accepted or rejected without a reliable technical basis.
5) The mental element of any deepfake-specific offense should be expressly defined. Comparative reliance on French Article 121-3 should be framed accurately: negligence or imprudence is punishable only where the law provides for it, and should not be treated as a general substitute for intent.
6) A legal framework addressing developers, platforms, and technical intermediaries should distinguish intentional or knowing criminal assistance from the neutral provision of general-purpose technology. Liability should depend on

clearly defined participation standards and the actor's proven knowledge or intent.

7) Judicial and technical capacity should be strengthened through specialized expertise in digital evidence and synthetic-media detection, with procedures that assist courts in assessing authenticity, attribution, and the limitations of automated detection tools.

References

[1] Abdelhamid, M. S. (2022). Digital forgery and its impact on the evidentiary value of digital evidence in criminal cases. Journal of Legal Research, 14(2), 115–148.

[2] Al-Abdullah, T. I. A. (2025). The crime of deepfake using artificial intelligence. Dar Al-Nahda Al-Ilmiyya.

[3] Al-Ali, A. Y. (2022). Legal challenges of artificial intelligence in criminal evidence. Journal of Legal Studies, 10(1), 112–140.

[4] Al-Dulaimi, M. A. (2022). Criminal evidence in cybercrimes. Dar Al-Thaqafa for Publishing and Distribution.

[5] Al-Harasi, A. bin S. (2023). Legal liability for cybercrimes considering Gulf legislations. Dar Al-Jami'an Al-Jadida.

[6] Al-Kaabi, F. A. (2024). The impact of digital transformation on criminal evidence rules. Journal of Law and Technology, 6(1), 55–89.

[7] Al-Shamsi, R. S. (2021). The evidentiary value of digital evidence in UAE criminal law. UAE Law Journal, 15(2), 45–78.

[8] Bayouwi, I. A. (2026). The criminal framework for addressing deepfake crimes and its impact on the criminal evidence system. Journal of Legal and Political Sciences, 3(1), 341–358.

[9] Casey, E. (2020). Digital evidence and computer crime (4th ed.). Academic Press.

[10] Chesney, R., & Citron, D. K. (2019). Deepfakes and the new disinformation war. Foreign Affairs, 98(1), 147–155.

[11] Citron, D. K. (2020). Sexual privacy. Yale Law Journal, 128(7), 1870–1960.

[12] Europol. (2022). Facing reality? Law enforcement and the challenge of deepfakes. Europol.

[13] Fadel, A. M., & Abbas, S. A. (2022). Deepfake: The language of artificial intelligence in cyber warfare. Dar Amjad.

[14] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[15] Kietzmann, J., Lee, L., McCarthy, I., & Kietzmann, T. (2020). Deepfakes: Trick or treat? Business Horizons, 63(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11.006

[16] Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes. ACM Computing Surveys, 54(1), 1–41. https://doi.org/10.1145/3425780

[17] Muharram, A. M. (2022). The use of deepfake technology in defamation. Journal of Jurisprudential and Legal Research, 39(39), 2491–2589.

[18] United Nations Office on Drugs and Crime. (2023). Artificial intelligence and criminal justice. UNODC.

[19] Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. Social Media + Society, 6(1). https://doi.org/10.1177/2056305120903408

[20] Westerlund, M. (2019). The emergence of deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52. https://doi.org/10.22215/timreview/1282.