

Criminal Protection for the Merchants from the Crimes of Electronic Publishing about Invasion of Privacy in UAE Legislation

Muayad Ahmad Obeidat¹, Nada Zuhair AIFil²,
Ahmed Moustafa Aldabousi³ &
Khalid Mohamed DGANNI⁴

Abstract

Numerous legislations, including those in the UAE, have instituted laws to safeguard individuals' reputations and privacy rights in cyberspace. These laws aim to prevent the dissemination of potentially harmful content, regardless of its accuracy. This article delves into how UAE laws protect the privacy of individual merchants, particularly examining the efficacy of Article 44, paragraph three. The article questions the extent to which this penal provision effectively protects merchants' privacy and family life. It notes that while the UAE legislature criminalizes the intentional dissemination of harmful content, including news, images, and data, it fails to explicitly differentiate penalties for harming merchants versus ordinary individuals. The article suggests enhancing penalties for crimes against merchants, especially in cases of severe harm. Additionally, it proposes stricter penalties for public officials who abuse their positions to commit such offenses. These recommendations aim to better protect merchants' privacy rights and deter misconduct in cyberspace.

Keywords: Invasion of Privacy and Private Life, Merchant, Harm and Offense.

Introduction

Considering the current rapid technological advancements, it is important to acknowledge the numerous benefits and advantages that these developments have brought to various aspects of life. However, it is crucial to recognize that such progress also carries the potential to jeopardize persons' rights and freedoms. This can manifest in the form of privacy violations or invasion of their personal or familial life (Abbas, 2020).

¹Professor of Commercial Law, College of Sharia and Law, University of Khorfakkan, Sharjah, Khorfakkan - United Arab Emirates (UAE). Muayad.obeidat@ukf.ac.ae.

²Associate Professor of Commercial Law, College of Sharia and Law, University of Khorfakkan, Sharjah, Khorfakkan - United Arab Emirates (UAE). NADA.AIFIL@ukf.ac.ae

³Associate Professor of Commercial and Maritime Law, College of Law, American University in the Emirates (UAE). Ahmed_aldabosy@yahoo.com; ORCID: <https://orcid.org/0000-0002-9073-7254>

⁴Associate Professor of Criminal Law, College of Sharia and Law, University of Khorfakkan, Sharjah, Khorfakkan - United Arab Emirates (UAE). KHALID.DGANNI@ukf.ac.ae

Consequently, the UAE legislator has deemed it necessary to intervene and enforce protective measures for the right to privacy and private and familial life. The text of Article 44 of Federal Decree Law No. 34 of 2021 addresses various topics related to countering rumours and cybercrimes. However, the regulation in this article is not clear when it comes to protecting the right to privacy and the private life of merchants, which needs more clarification in this article.

This article aims to clarify the problem surrounding the extent to which the criminalization provision in the third paragraph of Article 44 is comprehensive and sufficient to protect the right to privacy and the private and familial life of merchants in the UAE legislation. This article utilized a descriptive and analytical approach to examine the provisions and rules of the UAE Federal Decree-Law No. 34 of 2021 on countering rumours and cybercrimes. Additionally, it referenced relevant legislation from France and Egypt when applicable.

General Provisions Concerning Invasion of Privacy

Chapter Two of Federal Decree-Law No. (34) of 2021 in the UAE addresses the issue of countering rumours and cybercrimes. Article (44) specifically deals with revealing secrets and invasion of privacy using information networks, electronic information systems, or other means of information technology. This crime involves intentionally invading the privacy of a person or infringing upon the sanctity of their private or familial life without their consent or a legal permit.

Invasion forms encompass the act of broadcasting news, electronic photographs, or any content, including scenes, instructions, data, or information, even if they are true, to cause harm to a person. It is important to identify the person whose privacy has been invaded or whose private or familial life has been violated. It is crucial to identify the legal text's definition of privacy, which will be discussed in detail below.

a. Persons Subject to the Invasion

The UAE legislator introduced a term in the law that identifies the victim of these crimes as a "person." However, in Article 44 of Federal Decree Law No. 34 of 2021, the legislator did not clarify whether this term refers to a natural person or a legal person, this raises the question regarding the legal status of the person subject to the invasion.

In response to that question, some individuals argue that the right to privacy is an inherent right of every human being, serving as a safeguard for their secrets (Al-Mashaikhi, 2020). Some legal interpretations consider this right to be

one of the most significant rights enjoyed by individuals in advanced and progressing societies (Matrooshi, 2021).

Another perspective in legal interpretation suggests that privacy is closely linked to the identity and recognizability of the natural person (Aisha, 2016). Furthermore, some argue that privacy has become increasingly important. There have been numerous calls for it, not only to challenge its constitutionality but also to ensure its enforcement through legitimate and legal methods that provide assurance (Al-Qahwaji & Mahmoud, 2010).

From the information provided, we can conclude that the term "invasion of privacy" employed by the UAE legislator applies to natural persons rather than legal ones. This raises the question of whether this word can be applied to individual merchants. Particularly considering the UAE legislator's use of the two terms: invasion of a person's privacy or invasion of the sanctity of private or familial life of persons (Al-Mashaikhi, 2020).

In response to this question, it appears that there are no obstacles to applying this provision to an individual merchant. Therefore, anyone who utilizes the information network or any electronic information system or employs information technology means with the intention of invading the privacy of the individual merchant or the sanctity of their private or familial life, will be considered a perpetrator of this crime (Aldabousi, 2023)

This applies even if a crime is committed through the publication of news, electronic or photographic images, or any other form of content, including instructions, statements, or information. It is important to note that these forms of invasion, regardless of their accuracy or truthfulness, will be deemed harmful if their purpose is to cause harm to the merchant in question (Taha, 2015).

Therefore, it is evident, for example, that if someone shares electronic images depicting the uncleanliness of a restaurant, they have dined at to warn others to avoid it, they can be held accountable for a crime only if they intend to harm the restaurant owner. In such a case, the person sharing the images is considered the perpetrator of this crime (Taha, 2015).

The question at hand pertains to those who publish photographs, information, and data pertaining to a restaurant, hotel, or any other establishment controlled by someone else with the intention of safeguarding public health, benefiting the public good, or fulfilling a national obligation. It is evident that this individual is not regarded as a perpetrator of the crime of invading the privacy of the merchant as a person. Rather, it is more regarding physical, informational, organizational (Matrooshi, 2021), social, health, or financial privacy about the income, debts, and expenses of the person in question (Taha, 2015)

Therefore, we advocate for the view that the legislator should enhance the severity of the punishment to achieve deterrence and retribution when invading the privacy of these individuals.

b. Forms of Invasion

Article (44) of Federal Decree Law No. (34) of 2021 in the UAE addresses various forms of invasion. These invasions are considered illegal if they are carried out without the explicit consent of the person subject to them or if they occur in situations that are not permitted by law. Below, we outline the specific cases that prohibit these invasions:

c. Invasion of Privacy

Federal Decree-Law No. (34) of 2021 does not provide a clear definition of privacy. Some argue that this lack of definition is why the judiciary should not attempt to define privacy, as it is a vague and unspecified concept. Instead, it is necessary to examine each case individually to fully protect individuals by determining the correct approach for each situation (Matrooshi, 2021).

Furthermore, privacy is considered by some to be a term that is not absolute but rather relative and adaptable, evolving based on the customs and traditions of society as well as varying with time and location. Privacy is a fundamental right that encompasses various aspects. It is important to note that an individual's privacy can have two distinct characteristics. In certain situations, a person's private life may become public, thereby forfeiting legal protection when subjected to invasion. This occurs when their behaviour is openly observed by others.

However, in other situations, people have the right to live their private lives free from outside interference. Any violation or invasion of their privacy in such cases would be considered a breach of legal provisions (Al-Mashaikhi, 2020).

It is important to note that the right to privacy consists of two inseparable aspects. The first aspect is the right of an individual to have freedom in their personal life, including the ability to choose how they live without interference from others or authorities. However, the social system within the society in which the individual resides limits this right.

The second aspect pertains to the confidentiality of an individual's private life, which is a result of their personal choices and is exclusive to them. This includes personal information and facts that the individual wishes to keep to themselves or share with specific individuals who are connected to them.

The invasion of an individual's privacy is manifested through the violation of their personal space, such as the sanctity of their home and the confidentiality

of their correspondence, regardless of the medium of communication. This includes acts of observing and eavesdropping (Abbas, 2020), and the publication of news, electronic content, photographs, comments, data, and information related to the person. Even if these materials are factual and accurate, if the intention behind their broadcasting is to harm the victim, it still constitutes an invasion of privacy.

It is important to note that the UAE legislature has not provided specific guidelines regarding the publication of news, photographs, data, scenes, or comments related to individuals. It has not specified whether the published image was taken in a public or private place, nor has it specified the time of occurrence.

Therefore, the absolute occurs when it is done, and the publication is done regardless of whether it occurred in a public or private place (Fadlallah, 2020), or during the day or night. The only requirement is that the publication be done through information technology means, information network, or electronic information system. The legislature has not provided any instructions on how to obtain news, data, information, or published scenes.

In our opinion, the UAE legislator did not differentiate between individuals who invade privacy in terms of the prescribed punishment. However, we believe it is necessary to increase the severity of the penalty if the offender is a well-known social media figure with thousands or millions of followers. This is because the harm inflicted on the victim is directly proportional to the number of followers and the extent to which they are acquainted with the person's private life because of the publication.

i. Invasion of the Sanctity of Private Life

The UAE legislator has referred to two synonyms, namely the invasion of privacy and the invasion of the sanctity of private life. However, there is no clear standard to differentiate between the privacy of an individual and the sanctity of their private life. It appears that the criteria for distinguishing between them are subjective and objective. When the invasion targets an ordinary person, it falls under the subjective criterion, signifying an invasion of their private life's sanctity.

On the other hand, if the invasion is directed at a merchant, it is considered an invasion of privacy, which is an objective matter. Assault is an invasion of an individual's privacy, particularly when it involves an invasion of the sanctity of their home or engaging in activities such as photographing them, eavesdropping on their phone conversations, or revealing personal incidents such as marrying someone else or acquiring a specific disease (Safar, 2020).

Some argue that the right to privacy encompasses various personal rights, including the right to personal identity, professional confidentiality, housing, family rights, and anything that does not pertain to public life (Obaid, 2023).

It is clear to us that it is challenging to establish a clear criterion for distinguishing between the public and private lives of individuals. This difficulty arises from the subjective nature of the concept of private life, which varies from person to person and is influenced by factors such as their location and the time they lived in (Obaid, 2023).

An example of a situation that is not considered part of a person's private life is when a professor is present in a lecture hall or when a doctor is in an operating room. These instances fall under the public life of individuals (Al-Mashaikhi, 2020) and are therefore not entitled to the legal protection outlined in Article (44) of Federal Decree Law No. (34) of 2021 on countering rumours and cybercrimes in the UAE.

ii. Invasion of the Sanctity of Familial Life

In the text of Article (44) of Federal Decree-Law No. (34) of 2021, the UAE legislator mentioned this picture. However, the legislator did not provide a clear definition of the term "sanctity of familial life" or specify the extent of familial life for individuals. The legislator did not elucidate the scope of family life and the individuals who fall under its purview.

Here, the question arises regarding the individuals encompassed by this passage. Does it pertain solely to the person's spouse and children, or does it further encompass their parents and siblings?

To address this question, we do not find what helps us within UAE legislation, so we need to refer to the UAE legislator's involvement in this matter. The legislator's intervention is required as stated in Article (1) of Federal Decree-Law No. (34) of 2021. This decree-law aims to clarify the definitions of certain terms, particularly considering the various laws and regulations that define the concept of family. Some of these laws recognize same-sex relationships (homosexuality), while others acknowledge relationships between a man and a woman outside of marriage.

Consequently, the question arises regarding the extent to which the infringing act on these individuals constitutes an invasion of the sanctity of familial life.

Therefore, we have found a lack of clarity in the text the UAE legislator cited. We propose to first define the concept of the family, specifically regarding the violation of its members through the publication of news, pictures, and data. Such infringements also include invasion of the familial life of individuals, which

entitles them to legal protection as stated in Article (44) of the aforementioned law.

To address this issue, we suggest establishing and regulating the degree of kinship, particularly considering the varying definitions of family in different legislations and laws. In this regard, we propose that the second degree of kinship be adopted.

Section 2: Legal Structure around the Crime of Electronic Publishing to Cause Harm or Offense

Article 44 of the Law on Countering Rumours and Cybercrimes states in its first paragraph that: *“Whoever uses an information network, an IS, or any ITE with the intention of invading the privacy or sanctity of private or familial life of someone without his consent in cases other than those authorized by law through committing any of the following actions shall be punished with imprisonment for at least (6) six months and/or a fine of not less than (AED 150,000) one hundred fifty thousand dirhams or more than (AED 500,000) five hundred thousand dirhams:*

- 1. Eavesdropping, intercepting, recording, transmitting, broadcasting, or revealing conversations, communications or audio or visual materials.*
- 2. Taking photos of third parties in any public or private place, or preparing, transferring, disclosing, copying, or keeping electronic photos.*
- 3. Publishing news, electronic photos, images, scenes, comments, data, or information, even if it is genuine, intending to harm the person.”*

d. Elements of Crime

In this topic, we shall address the elements of crime as follows:

i. Material Element of Crime

According to Article 44/3 of the UAE Law on Countering Rumours and Cybercrimes, the prohibited behaviour in this offense is the act of publishing or sharing images, scenes, comments, and data to make them visible to others.

The behaviour in question pertains to news, images, data, scenes, comments, and information regarding individuals. The crime described in this paragraph occurs when images or scenes that invade people's privacy are published using an information network or technology, regardless of whether the images, scenes, news, or data were obtained with the person's consent, such as when a merchant allows a celebrity and content providers on a social networking site to enter their store. The individual in question filmed scenes and provided data to promote his store through advertising. However, a disagreement arose between the two parties regarding the price of the advertisement. Consequently, the

individual resorted to publishing offensive pictures, news, and scenes targeting the merchant.

In this scenario, the act of committing a crime occurs, regardless of the authenticity and accuracy of the pictures, news, and scenes. Furthermore, an individual's agreement to provide data, photographs, scenery, or news does not imply their consent to make them public. Regarding the outcome, it is important to highlight that the UAE legislator perceives this crime as one that necessitates a material outcome, specifically the publication of news, information, images, or scenes, regardless of their reliability.

Consequently, the legislator perceives this offense as one that causes harm rather than being a direct danger. As for the act of initiation, it is worth noting that this offense is considered an attempted offense. This means that if an individual is caught while attempting to publish pictures or transmit news and information through the information network, they will be penalized for their attempt.

The Egyptian legislator has made it a criminal offense to publish news, data, images, and other forms of media, such as photographs, electronic content, and video scenes. This is stated in Article (25) of Law No. 175 of 2018 on combating information technology crimes. The article specifies that the publication of these images must involve an invasion of individual's privacy and the sanctity of their private lives. In other words, the act of publishing must cause harm by infringing upon the personal privacy of individuals. Unlike the UAE legislator, who included the phrase "to harm," the Egyptian legislator did not explicitly state this requirement.

The crime occurs whether the published information is true or untrue, The Egyptian legislature has classified these offenses as crimes of harm rather than crimes of danger, following a similar approach used by the UAE legislature. Moreover, the legislature has explicitly tied the criminalization of these offenses to the absence of the victim's approval.

The legislator has associated the criminalization, as per the text, with the offender's use of specified means for publication, specifically an information network or an information technology means.

According to French legislation, Article 226-1 of the Penal Code is used to regulate the publication of images through information technology. This law was applied based on a decision made by the Minister of the Interior on August 24, 2010. Accordingly, the provisions of the mentioned article are applied to the broadcasting of satellite images over the internet with the intention of invading the sanctity of private life (Dec No 76067, JOAN Q 24 août 2010, D, 16 septembre 2010, No 31, p.1991), and their application aims to enhance the protection of private life's sanctity in France.

Furthermore, it should be noted that obtaining someone's consent to photograph or record videos of them while they are wearing bathing suits does not imply their agreement to circulate, transfer, or publish these images (CA Versailles 10 Novembre 1999, NO de RG, 1999-946). Similarly, if a merchant takes pictures of themselves or their store or provides information about themselves or their store, this should not be interpreted as consent to publish or use this information in a way that could be offensive or violate their privacy.

It is important to understand that publishing using computer networks or information technology does not refute the privacy aspect of the crime, as argued by the Federal Supreme Court (Federal Supreme Court, UAE, Appeal No. 104 of 2017, Penal, issued on Tuesday, 4/4/2017).

ii. Moral Element of Crime

In the UAE, the legislature has deemed the crime of publishing news, data, or images to offend someone to be an intentional crime. This offense requires both a general intent, which includes knowledge and will (Sattar, 2000), as well as a special criminal intent. In other words, the offender must be aware that publishing news, data, and images related to a merchant's personal life constitutes an invasion of their privacy.

If the offender doesn't possess this knowledge, it negates their criminal intent. For example, if the offender believes that their actions are permissible and not considered the privacy of individuals in society, or if they believe that they are fulfilling their duty by informing authorities about a crime and documenting it through photography and publication, the Federal Supreme Court has ruled accordingly.

Furthermore, the perpetrator must have the will to publish news, data, or images that invade the sanctity of the private life of the merchant. This includes the act of publishing images that were taken, copied, or saved during a previous offense if their publication constitutes an invasion of the sanctity of the private lives of persons.

Additionally, the legislature has established specific criminal intent requirements for offenses involving an invasion of personal privacy through the publication of news, images, data, or information. The user of the information network is acting in bad faith with the deliberate intention of harming the reputation of others. This involves publishing news, pictures, and data with the explicit aim of causing harm to a merchant. For instance, a person may take snapshots or videos of a store and make offensive comments about it on social media. They may also write an article that insults a merchant or store, again to cause harm and offense.

Based on the preceding information, bad faith is invalidated if the perpetrator genuinely believes that they were fulfilling an obligation mandated by Islamic law, such as preventing corruption or safeguarding the well-being of others or their money. It can also be negated if the individual genuinely believes that they are fulfilling a legal duty, such as reporting a crime or providing evidence to prevent the potential disappearance of a situation, such as aiding the authorities in carrying out their responsibilities (Federal Supreme Court, UAE, Appeal No. 950 of 2019 Penal, Tuesday, February 4, 2020).

In contrast to the UAE legislator, the Egyptian legislator only requires the crime to prove criminal intent, which consists of two elements: knowledge and will. The Egyptian legislature does not mandate the establishment of a specific criminal intent or the intention to cause harm by the offender.

iii. Penalty Prescribed for the Crime

The UAE legislator has established a punishment for the crime of publishing news, data, or images to cause offense. This penalty entails a minimum imprisonment period of six months and a maximum of three years, as well as a fine not less than one hundred and fifty thousand (150,000) dirhams and not more than five hundred thousand (500,000) dirhams.

Based on the wording of Article 44 of the Law on Countering Rumours and Cybercrime, it is evident that the legislator has classified this offense as a misdemeanour and imposed a punishment of imprisonment ranging from six months to three years. The fine for this offense is determined by Article 44 of the Law on Countering Rumours and Cybercrimes, which establishes both a minimum and maximum limit. The minimum fine is set at one hundred and fifty thousand dirhams, while the maximum fine cannot exceed five hundred thousand dirhams.

However, the legislator in the Law on Countering Rumours and Cybercrimes did not distinguish between the punishments for the crimes outlined in Article 44, regardless of whether the offender was a normal person or a public employee acting within the scope of their authority. This is unlike Article 431 in the Federal Crimes and Penalties Law, which imposes a higher penalty of imprisonment for a minimum of one month and a maximum of seven years, as well as a fine ranging from ten thousand (10,000) dirhams to five million (5 million) dirhams if the offender is a public servant acting within the scope of their authority.

Therefore, the legislator must amend Article 44 to increase the penalty for public officials who commit crimes within the scope of their authority. Moreover, the legislator failed to distinguish the penalty outlined in Article 44 of the Law on Countering Rumours and Cybercrimes, regardless of the extent of harm inflicted

upon the victim, particularly if the victim is a merchant. Committing a crime against a merchant can lead to substantial material and moral harm. Although the victim can seek compensation for being a victim of the crime, the legislator should increase the severity of the penalty based on the amount of damage or impose a proportional fine to deter the occurrence of such crimes.

In summary, the federal legislator has made amendments to the penalty stated in Article 44 of the Law on Countering Rumours and Cybercrimes. The minimum punishment for individuals who commit this crime using an information network or technology has been raised. However, unlike Article 431 of the Federal Penal Code, which tightened the penalties of imprisonment and fine, the penalty for public employees who commit this crime has not been increased. Therefore, the legislator must intervene and increase the penalty for this crime in Article 44 of the Law on Countering Rumours and Cybercrimes.

Under French legislation, individuals who commit this form of crime will be subject to the penalties outlined in Article 226-1 of the French penal code, which has already been explained in the previous offense.

In Egyptian legislation, the act of publishing images using information technology is subject to a penalty of imprisonment for a minimum of six months, along with a fine ranging from fifty thousand to one hundred thousand pounds. Either of these two penalties may be imposed.

iv. Complementary Penalty

According to Article 65 of the UAE Law on Countering Rumours and Cybercrimes and Article 38 of the Egyptian Law on Combating Cybercrimes, it is required to confiscate tools and machines used in a crime, which should not be legally owned by anyone, and to delete information or data. Additionally, in cases where a license is required to engage in a commercial activity, the penalty may include the closing down of a site or business.

In contrast to the general rules outlined in Article 47 of the Egyptian Penalties Code, which require explicit provision from the legislator that attempted misdemeanours should not be punished, Article 40 of the Egyptian Law on Combating Information Technology Crimes imposes penalties for attempted information technology crimes. These penalties do not exceed half of the maximum penalty prescribed for the committed crime, as specified in Article 57 of the UAE Law on Countering Rumours and Cybercrimes.

Given that the existing criminal sanction encompasses both punishment and precautionary measures (Al-Qahwaji & Mahmoud, 2010), it is determined that "Upon rendering a judgment of conviction of any of the crimes stipulated in this Decree-Law, the court may decide to take any of the following measures:

1. Order that the convict be placed under electronic supervision or monitoring, be deprived of using any information network, IS, or ITE, or be placed in a treatment shelter or rehabilitation center for the duration the court deems appropriate.
2. Close down the violating site completely or partially whenever this is technically feasible.
3. Block the violating site completely or partially for the duration decided by the court.”

Conclusion

The UAE legislature granted criminal protection of the right to privacy and private and family life to merchants under the third paragraph of Article 44 of the UAE Law on Countering Rumours and Cybercrimes, although it was not explicitly stated. In the UAE, the legislator considers a crime to have occurred when an offender publishes news, pictures, and data to cause harm. The legislator has established a penalty for this crime but has not distinguished between the severity of the penalty based on whether the victim is a normal person or a merchant, even though the damage caused to the latter would be more significant. Additionally, the legislator has not differentiated the penalty based on whether the damage was achieved or not, nor has it distinguished between whether the offender is an ordinary person or a public official who obtains data and information in an official capacity.

Recommendations

- We suggest that the UAE legislature revise the third paragraph of Article 44 of the UAE Law on Countering Rumours and Cybercrimes to explicitly include provisions for the protection of merchants from these crimes, or introduce a separate provision specifically addressing the criminal protection of merchants.
- We suggest that the UAE legislature enhance the punishment if the victim is a merchant, as well as increasing the penalty for severe harm inflicted upon the merchant. Additionally, we suggest increasing the penalty if the perpetrator is a public service employee who may have committed the crime in an official capacity.

References

- Abbas, Q. A. (2020). Legal Protection of the Right to Privacy for Social Media Users. *Kufa Journal for Humanities and Political Sciences*, 13(44), 255-256.
- Aisha, B. Q. (2016). The Right to Information Privacy between Technical Updates and the Reality of Legal Protection. *Arab Journal of Science and Research Publishing*, 2(5), 39.
- Aldabousi, A. M. (2022). LEGAL PROBLEMS OF CONCLUSION OF INTELLIGENT SOFTWARE AGENT FOR SMART COMMERCIAL CONTRACTS IN THE ERA OF BLOCKCHAIN U. A. E AS A MODEL. *Universidad y Sociedad*, 14, 713 - 7281.
- Aldabousi, A. M. (2022). Legal Problems of Electronic Pollution According to UAE and Egyptian Law. *Arab World Geographer* Volume 25, Issue 2-3, 25(2-3), 154 - 1681.
- Aldabousi, A. M. (2023). THE LEGAL PROBLEMS FACING THE CONCLUSION OF CLOUD COMPUTING CONTRACTS. *Universidad y Sociedad*, 15(3), 602 - 611.
- Al-Mashaikhi, N. H. (2020). *The Constitutional Regulation of the Right to Privacy and its Judicial Guarantees (A Comparative Study)*, Arab Center for Publishing and Distribution. Cairo.
- Al-Qahwaji, A. A., & Mahmoud, S. A. (2010). *The Origins of Criminology and Punishment*,. Beirut: Al-Halabi Human Rights Publications.
- CA Versailles 10 Novembre 1999, NO de RG, 1999-946.
- Dec No 76067, JOAN Q 24 août 2010, D, 16 septembre 2010, No 31, p.1991.
- Fadlallah, F. M.-H. (2020). The Crime of Violating the Sanctity of Private Life in UAE Legislation: An Analytical Study. *Journal of Jil Center Research*, 55.
- Federal Supreme Court, UAE, Appeal No. 104 of 2017, Penal, issued on Tuesday, 4/4/2017.
- Federal Supreme Court, UAE, Appeal No. 950 of 2019 Penal, Tuesday, February 4, 2020.
- Matrooshi, M. O. (2021). *Criminal Protection of Privacy in the Anti-Cyber and Information Technology Crimes Law, A Comparative Study*. United Arab Emirates: Dar Al-Haf.
- Obaid, A. Y. (2023). Violation of the Right to Privacy. *Iraqi University Journal*, 260.
- Safar, S. H. (2020). Legal Protection of Privacy in the Virtual World. *Journal of Arts, Literature, Humanities, and Sociology*, 2(98), 106.

Sattar, F. A. (2000). *Explanation of the Penal Code*. Cairo: Dar Al-Nahda Al-Arabiya.

Taha, A. S. (2015). Research entitled "The Privacy of the Individual in Islamic Jurisprudence and the Position of Legal Legislation in the United Arab Emirates towards it. *Journal of Security and Law*, 259.