TPM Vol. 32, No. S6, 2025
ISSN: 1972-6325
https://www.tpmap.org/

CRIMINAL CONFRONTATION REGARDING PIRACY OF ELECTRONIC INVENTIONS

AMEEL JABBAR ASHOUR
AMEELASHOUR@UOMISAN.EDU.IQ
COLLEGE OF LAW, UNIVERSITY OF MISAN

Abstract:
Modern technology has brought distances between peoples closer together by providing many new communication media that were not known before, and we also find that those technologies have produced many negatives and risks, perhaps the most important of which is the difficulty of control and retention the individual with his privacy due to the spread of many easy means of hacking electronic applications. Through this study, we will highlight the various challenges and difficulties facing security informatics in the face of electronic piracy.
Keywords: Information Security, Electronic Piracy, Communication Technology, Internet.

1. INTRODUCTION

The world has witnessed a revolution in the world of technology, media and communication, to the extent that some experts or specialists have prepared the electronic information field as the fifth field of conflicts after land, sea, air and space. Perhaps this is due to the rapid spread or development of this technology, as hardly any field of life does not rely on the latter in light of the transformation that has reduced effort, time and cost and contributed with its speed and flexibility to meeting needs. However, despite the positives that the Internet has brought, it has brought with it many threats and risks that have been translated into cybercrimes, which have not differentiated between individuals, institutions and countries, not to mention the threats that may affect the security and stability of countries. These crimes are characterized by a special nature that differs from ordinary crimes. They do not leave material traces through which the perpetrator can be identified, as in ordinary crimes. Also, destroying or changing evidence in these crimes within moments without this change leaving material traces makes them more difficult to discover This may increase with the virtual digital nature in which the criminal commits his crime and the ease it provides him in committing it, as one simple click on the computer is enough to reach the potential victim. It is also often not done in secret, as the criminal deliberately does so by playing with data and destroying evidence if he wants to.

2. Study Problem.

Contemporary legislation, including Iraqi legislation, suffers from a tangible gap between rapid technical development and the flexibility of criminal texts. The problem of this research is evident in its attempt to assess the adequacy of Iraqi laws in confronting the crime of electronic piracy, and the extent of its ability to keep pace with the technical and practical challenges posed by this crime. A number of fundamental questions arise from this problem:

1. To what extent are Qatari legal texts clear and integrated in defining the crime of electronic piracy and determining its pillars?
2. Do the sanctions contained in Iraqi law constitute a real deterrent in light of the scale of the threat?
3. What are the shortcomings or deficiencies compared to comparative Arab legislation?
4. Does it require legislative intervention to amend or update the Anti-Cybercrime Law in Iraq?

3. Study Importance.

The importance of this research lies at several interconnected levels:

A. The legal significance of the crime of electronic piracy represents a direct challenge to the principle of criminal legality, because it is not subject to traditional legal adaptation, and is not consistent with classical crime concepts. This requires Iraqi legislation to reconsider its legal structure to keep pace with the development of this crime, whether in terms of defining the pillars, organizing penalties, or controlling criminal liability. The research seeks to provide an accurate legal treatment that contributes to bridging this legislative gap.

B. Security and national importance: Electronic piracy does not only threaten individuals or commercial entities, but its effects extend to sovereign data, state infrastructure, and national security institutions, which makes confronting it part of the state's duty to protect its digital security, and therefore, developing the legal framework for this crime is primarily a matter of national security .

C. Scientific and research importance: Despite the passage of nearly a decade since the issuance of Iraqi Penal Code No. (111) of 1969, scientific studies specialized in analyzing this law and comparing it with more advanced legislation are still limited. This research comes to fill this deficiency through accurate analytical treatment and providing an objective comparison that enriches the legal research arena.

4. Study Objectives.

1. Definition of this type of electronic piracy crime.
2. Awareness and sensitization of the risks of exposure to this type of crime.
3. Trying to confront this type of crime while providing solutions and knowing how to protect the data provided electronically.

5. Definition of the Crime of Electronic Piracy.

Criminal jurisprudence has agreed that the term "Electronic piracy" is used to refer to any aggressive act carried out through technological means with the aim of unlawfully penetrating digital systems. Jurists almost unanimously agree that the essence of this crime lies in illegal entry into an information system or protected network with the intention of accessing, manipulating, destroying, or exploiting data (Hajej & Ghazi, 2016,pp.72-89). Some researchers have defined it as: "A process of hacking electronic systems, often carried out over the Internet, and carried out by a person or group of people who possess technical skills that allow them to bypass protection systems to access information, whether with the intention of destruction, theft, espionage, or blackmail"(Al Hammadi, 2019,pp.50-64).

It is noted from this jurisprudential definition that this crime is characterized by several main characteristics, the first of which is that it is based on illegal infringement on protected technical systems, where the perpetrator exceeds the legal limits established to protect these systems. It is also characterized by the presence of aggressive intent or deliberate criminal will that drives the perpetrator to commit this behavior. It is inconceivable that this crime would occur without the presence of an electronic means that is a necessary element in carrying out the act, such as the use of computers or digital networks (Al-Fitouri Kandi, 2017, pp.90- 98).

These actions lead to harmful consequences, whether direct harm such as data corruption or system disruption, or indirect harm such as compromising information security or threatening digital privacy and confidentiality. Some jurisprudential opinions classify piracy as a crime of attacking digital money, while others consider it a crime "against the digital security of the state" if it targets sovereign regimes or vital institutions (Barghit, 2022, pp.220-229).

Iraqi legislation in the Iraqi Penal Code is based on 11 years 1969, as amended. We did not find a definition for the crime of electronic piracy, but in comparative legislation, including Qatari legislation, which defined electronic piracy in the text of Law No. (14) of 2014 regarding combating electronic crimes, in its second article, criminalizing illegal entry into information systems: "Intentionally entering, without right, by any means into a website, information system, or information network... or exceed the authorized entry or continue to be there after learning that he is not entitled to stay. It is also noted that the Qatari legislator relied on the concept of illegal entry as a basis for defining the crime, without providing a comprehensive definition of the concept of "electronic piracy" in its complex sense, which is considered a legislative deficiency (Muhammad Safi, 2023, pp.59- 80).

In Egyptian legislation, the Anti-Information Technology Crimes Law No. (175) of 2018 (1) used the term "illegal entry," and in Article (14) it criminalized acts of intentional or unintentional entry on websites or information systems without a permit, with an increased penalty if the entry is accompanied by destruction, copying, or modification of data. However, the Egyptian legislator was relatively distinguished by providing broader details of cases of electronic infringement, and linking the text to penalties more clearly, which contributes to clarifying the judicial adaptation of the crime (Al-Ghathbar & Al-Qahtani, 2021, pp. 65-74).

In international legislation, the Budapest Convention against Cybercrime (2001) adopted the concept of "unlawful interference with data or systems", and defined this through several articles. Article 2 criminalizes "illegally entering, when committed, a computer system or any part thereof," whether by breaching security measures. Article 3 also criminalizes "objection, when committed intentionally, unlawfully and by technical means to non-public computer data during its transmission"(Rustum, 2000, pp.34-41). In Article 4, the Convention considered that "unjustly damaging, deleting, deteriorating,

modifying or suppressing computer data, when committed intentionally", is a crime requiring criminalization. Article 5 expanded the scope of legal protection to include the system as a whole, stipulating that "serious disability, when committed intentionally, without right, to the function of a computer system through the entry, transfer, destruction, deletion, deterioration, modification or suppression of computer data, shall be criminalized"(Al-Momani, 2023,pp. 256-267).

6. Pictures of Electronic Piracy Crime.

The seriousness of the crime of electronic piracy lies in its multiple forms and the different methods of committing it, which makes combating it more complex than traditional crimes. This crime is not limited to one image or stereotype, but rather varies according to the pirates' goals and technical capabilities. Hence, familiarity with its forms is a necessary condition for understanding the elements of the crime, adapting them legally, and confronting them effectively (Badri, 2018, pp.42-53).

A. Illegal Access to Information Systems.

Illegal entry is the primary and most common form of cybercrime, and is the starting point for most hacking operations, whether they are later intended to destroy, steal, or even simply conduct reconnaissance. Criminal legislation has explicitly criminalized this act, defining it as: "intentionally entering, without right, by any means into a website, information system, or information network, or exceeding the authorized entry, or continuing to be present there after learning of the lack of right to remain" (Al Ajmi, 2014,pp.38-57). This is similar to Egyptian Law No. (175) of 2018 who increased the penalty in the event that illegal entry is accompanied by other acts such as destruction, copying or deletion. This act is considered a formal crime that is completed as soon as the behavior is committed without the need to achieve a harmful result, unlike some other forms in which material or moral damage is required (Muhammad Battikh, 2021, pp. 91-104).

B. Illegal Objection or Eavesdropping on Data.

Illegal interception is the second form of hacking, which involves capturing or eavesdropping on data as it travels across an information network, whether personal, commercial, or security data. It is one of the most common acts of espionage and extortion crimes. Article (4) of the Qatari Cybercrime Law stipulates that anyone who intentionally captures, objects to, or eavesdrops, without justification, on any data sent over the information network, any information technology means, or traffic data shall be punished (Al-Otaibi, 2017,pp.51-59).

Egyptian law also included in Article (16) a similar criminalization, and considered illegal objection to be an act that represents a violation of digital confidentiality. This crime is considered a crime of a positive-negative nature; that is, it is committed through negative means such as silent surveillance), but it leads to extremely dangerous consequences, especially in the context of leaks or political and media blackmai (Muhammad Battikh, 2021, pp. 91-104). l.

C. Attack on the integrity of data and information systems

It refers to any act that disrupts damages, distorts, or modifies data, programs, or information systems. It is considered one of the most harmful and influential forms of hacking, especially if it targets vital systems (such as health, energy, or banking systems) (Al-Qahtani, 2016, pp. 88-97). The penalty is increased if the illegal entry results in actions such as: "cancellation, deletion, addition, disclosure, destruction, and change, transfer, copy, or republish data, or destruction or disruption of the site or system, or modification of its contents or designs. Article (21) of the Egyptian law stipulates that anyone who unlawfully stops, disrupts, or limits the efficiency of an information network or information system shall be punished (1). This crime often occurs in the context of deliberate attacks against digital infrastructure, and is sometimes used for major terrorist or economic purposes, such as in cases of "ransom attacks" or "vandalism of sovereign databases"(Abdel Razek, 2016, pp.74-102).

7. Reasons for the Spread of the Crime of Electronic Piracy.

There are many reasons that contributed to the spread of this crime, but jurisprudence and reality agree on the existence of four main motives: weak moral and educational motivation. Specialized studies have indicated that the absence of internal value controls among some individuals - especially young people or adolescents - leads to crossing legal and moral lines in the digital environment, whether out of amusement, curiosity, or revenge. This factor is clearly evident in societies that have not kept pace with digital expansion with an educational structure based on a culture of respect for digital privacy and data privacy (Jandal, 2022, pp.99-123).

Economic Motives and Ease of Illicit Profit Hacking is an "attractive" way to make quick profits without direct risk. A crime can be carried out remotely, from a closed room, against a target in another country, which weakens the possibility of legal prosecution and inflates the financial return, and these motives become more acute in environments that suffer from high unemployment rates or weak legal awareness. Technical development and ease of access to hacking tools hacking and hacking tools are no

longer limited to "digital geniuses", but have become easily available online, either for free or at a low price, and some sites even offer paid hacking services" according to the customer's request (Sidqi, 2015,pp.55-61).

The evolution of malware and the emergence of "hacking-as-a-service" (HAS) have transformed crime into an organized, semi-professional digital activity, with security and judicial authorities lacking technical expertise. Most countries face a real challenge represented by the wide gap between the capabilities of hackers on the one hand, and the technical skills available to control and investigation agencies on the other hand. This defect makes prosecuting the crime more difficult and increases the audacity of its perpetrators. Many victims, both individuals and organizations, do not report cybercrimes for fear of scandal or lack of confidence in the feasibility of prosecution (Al-Mudhahki, 2014, pp.30-48).

8. Characteristics of the Crime of Electronic Piracy

This crime has a number of characteristics that make it unique in its legal and social structure, the most prominent of which is a cross-border crime practiced via the Internet, which makes determining jurisdiction complex and raises real problems in international cooperation, especially if the perpetrator is in a country that does not criminalize the act or does not have legal cooperation agreements with the affected country (Tayeb, 2017, pp. 67-90).. Soft crime is non-violent but devastating and does not require the use of violence or the presence of a physical scene, making it difficult to detect in the field.They are committed with the click of a button, but can lead to disastrous results, such as destroying data banks, disabling navigation systems, or leaking sensitive security information (Al-Hamdani, 2014, pp. 9- 23).

The speed of development of the means of committing them compared to the speed of amending laws confirms that laws always lag behind the pace of development of cybercrimes. As pirates develop their tools day by day, legal texts remain rigid, relying mostly on traditional descriptions that may not capture the new picture of crime. This is the time difference between the development of crime and the development of laws (Hassan, 2021, pp.12-19).

It makes it difficult for lawmakers to keep up with rapid changes in hacking methods. Difficulty in proof and the large number of dark numbers many hacking crimes are not discovered at all, are discovered late, or are not reported, which makes official statistics much lower than the actual reality (Muhammad Safi, 2023, pp.59- 80). This gap in criminology is known as the "dark number," and it poses a significant challenge to researchers and legislators. This phenomenon reflects a lack of confidence in the ability of legal systems to protect individuals and institutions, leading to a greater spread of crime (Al-Ghathbar & Al-Qahtani, 2021, pp. 65-74). In conclusion, we conclude that the crime of electronic piracy does not arise only from an individual defect, but is the product of a complex social, technical, economic and legislative interaction, which requires an integrated legal approach. Its special nature in terms of tools and characteristics makes it one of the crimes most in need of continuous legislative updating and effective international cooperation. Without realizing these reasons and characteristics, the legal confrontation remains ineffective and has limited impact.

9. Assessing the Adequacy of Penalties & Analyzing Criminalization & Punishment Gaps.

Punishment is not only a tool for responding to crime, but is essentially a means of societal deterrence and prevention, and thus represents an essential pillar of the criminal system. In light of the increasing rates of cybercrime, especially piracy, assessing the adequacy of the legal penalties prescribed for these crimes is a real test of the feasibility, modernity, and ability of legislation to actually confront. This section addresses whether the penalties provided for in Qatar's Anti-Cybercrime Law are adequate and effective, highlighting the most significant gaps in criminalization or shortcomings in punishment compared to the actual development of crime(Hajej & Ghazi, 2016,pp.72-89).

A. The adequacy of Sanctions in Terms of Public & Private Deterrence.

Penalties in criminal laws represent an attempt by the legislator to achieve a balance between the criminal act and the prescribed penalty (Abdel Razek, 2016, pp.74-102). Penalties start from imprisonment and a fine for minor crimes such as illegal access to information systems, and gradually escalate in the event of aggravating circumstances, such as modifying, destroying, or disclosing data, or in the event of targeting sovereign and sensitive systems (Al-Fitouri Kandi, 2017, pp.90- 98). However, the actual deterrence is not only represented in punitive texts Rather, it requires guarantees in the practical application of these sanctions. One of the fundamental observations pointed out by many jurists is the absence of a minimum penalty, which enhances the judiciary's ability to make varying decisions based on the judge's discretion, which may contribute to the large disparity in judicial rulings and may lead to leniency in applying penalties in some cases. The punitive progression on which the law is based is not governed by precise controls, which may create a kind of ambiguity in interpreting criminal acts and determining appropriate penalties for them, which reflects a legal problem in adapting legal texts to actual facts (Muhammad Battikh, 2021, pp. 91-104).

Furthermore, some cybercrimes lack the effective consequential penalties necessary to combat digital crimes, such as denying defendants the right to engage in digital activities or confiscating the tools used to commit the crime. These consequential penalties are essential tools for deterring cybercrime, as they contribute to reducing the chances of recurrence by the individuals involved. Accordingly, it is clear that Qatari law, despite its progress, still needs further scrutiny and revision to more effectively meet the requirements of public and private deterrence (Al-Qahtani, 2016, pp. 88-97).

B. Absence of Texts on Attempted Crime.

One of the most prominent gaps in criminal legislation is the lack of an explicit treatment of the issue of attempted cybercrime (Al-Otaibi, 2017, pp.51-59). While most traditional crimes criminalize attempted crimes, digital crimes, which are often discovered in the middle of their execution, require special provisions criminalizing attempted crimes. If a hacking attempt is detected before the damage is achieved, there is no explicit article punishing the attempt, which makes the control devices lose the opportunity for early intervention. Egyptian law stipulates in Article (45) of Law No. 175 of 2018 the criminalization of attempted cybercrimes, which is considered an advanced model to be emulated (Barghit, 2022, pp.220-229).

C. Weak Legislative Treatment of Electronic Criminal Contributions.

Criminal legislation has not been unique in precisely regulating the liability of accomplices, instigators or assistants in cybercrimes. This is extremely dangerous, as many hacking crimes are carried out through organized networks in which more than one perpetrator works, one of whom plans, another carries out, and another facilitates or conceals evidence. Limiting the punishment of the direct perpetrator empties the legal text of its content in confronting organized crimes online, especially in light of the increasing use of "middleware" and "ready-made hacking tools" sold by a third party (Al-Hamdani, 2014,pp. 9- 23).

D. Weak Legislative Treatment of Electronic Criminal Contributions.

Criminal legislations do not provide precise regulation of the liability of accomplices, instigators, or assistants in cybercrimes. This is extremely dangerous, as many hacking crimes are carried out through organized networks in which more than one perpetrator works, one of whom plans, another carries out, and another facilitates or conceals evidence. Limiting the punishment of the direct perpetrator empties the legal text of its content in confronting organized crimes online, especially in light of the increasing use of "middleware" and "ready-made hacking tools" sold by a third party (Al Ajmi, 2014,pp.38-57).

E. Textual Shortcomings in Keeping Pace with Developments in Technical Crime.

Technical crimes are inherently variable, with their tools and implementation methods evolving rapidly, posing a constant legislative challenge to maintaining the effectiveness of legal texts. However, since the issuance of Law No. 14 of 2014 on Combating Cybercrime, Qatari legislation has not witnessed any fundamental amendments to accommodate these transformations, despite the qualitative shift in modern cybercrime patterns. The most prominent of these patterns are:

1. Using artificial intelligence techniques to carry out AI-Powered cyber attacks (Cyber Attacks)
2. Employing dark networks (Dark Web) as a hidden environment for exchanging data and malware.
3. Exploiting smart devices and Internet of Things (IoT) technologies in hacking and hacking activities (Al-Momani, 2023, pp. 256-267).

The absence of legislative updates to address these challenges creates a real legislative vacuum that makes it difficult for law enforcement agencies and places a heavy burden on judges to interpret existing texts in a manner consistent with these emerging realities. In some cases, the absence of explicit texts may lead to unsatisfactory legal consequences, such as weak criminal protection or even acquittal based on the rule of "no crime" and no punishment except by text(Al-Mudhahki, 2014,pp.30-48).

F. The Need for Supplementary Penalties in Cybercrime.

Although original penalties such as (imprisonment and fines) are important in reducing cybercrime, modern legislation in the field of combating cybercrime has not been satisfied with them, but has included complementary penalties aimed at achieving public and private deterrence, and correcting the imbalance resulting from crime (Sidqi, 2015,pp.55-61). However, penal legislation has neglected to provide for these supplementary penalties, which constitutes a legislative loophole that must be addressed. The most prominent forms of these penalties include: confiscation of the devices or software used in committing the crime, temporary deprivation of the use of specific technologies that may be used for harmful purposes, obligation to provide financial compensation to victims for the resulting damages, and publication of the ruling judicial in electronic media to enhance public deterrence (Barghit, 2022, pp.220-229).

These penalties reflect the nature of cybercrime, whose effects are not limited to the criminal aspect only, but extend to economic, security and social dimensions. The application of these penalties also contributes to addressing the practical effects of crime, which is stipulated in much comparative

legislation such as the European Uniform Cybercrime Law and the American law known as (Computer Fraud and Abuse Act (CFAA) (Al-Hamdani, 2014,pp. 9- 23).

CONCLUSION

First: Results:

Based on the above, the research reached the following results:

1. The crime of electronic piracy is a complex and technologically advanced crime, characterized by a cross-border nature, which makes combating it require flexible and constantly updated legal tools that go beyond the traditional pattern of criminalization and punishment .
2. Although criminal legislation has taken the initiative to issue laws to combat these cybercrimes, these laws lack a number of essential components necessary to confront contemporary digital crime, especially in terms of the comprehensiveness of criminalization and the modernity of the images covered by the law .
3. The study revealed that criminal legislation does not explicitly criminalize attempted cybercrime or technical criminal involvement, despite the prevalence of such forms in practice. This creates a legislative vacuum that impacts the effectiveness of criminal prosecution .
4. The law focuses on the original penalties, but completely ignores complementary penalties of a preventive nature, such as electronic confiscation, prohibiting the use of technical means, and publishing judicial rulings via digital media, which are tools that have become necessary to achieve deterrence in the cyber environment.
5. It is noted that criminal legislation has been poorly responsive to the development of modern forms of piracy, such as crimes related to artificial intelligence, the Internet of Things, cryptocurrencies, and dark networks. This limits its effectiveness and, in some cases, makes judicial adaptation the subject of uncertain interpretation.

Second: Recommendations:

Based on these results, the research recommends the following:

1. Amending laws to include explicit provisions criminalizing the initiation of cybercrimes, as it is a common act in this type of crime, especially with the digital nature that allows the attempt to be monitored before the result is achieved.
2. Include clear provisions relating to criminal contribution to cybercrime, including incitement, assistance, and the provision of technical tools, similar to what is stated in European legislation this is to avoid impunity in mass or network cases of crime.
3. Adding complementary penalties of a technical nature to the current penal system, such as electronic confiscation, temporary prohibition from using specific technical means, or electronic publication of judicial rulings, in a manner consistent with the nature of the crime and its digital environment .
4. Updating the scope of criminalization to include new forms of crime, such as crimes related to artificial intelligence, the Internet of Things, digital currencies, and hacking via dark networks by reformulating materials related to the pillars of cybercrime.
5. Issuing detailed executive regulations that keep pace with legal texts, specifying digital investigation mechanisms, electronic means of proof, and controls for the use of technical evidence before the judiciary, in a manner that achieves legal security and provides fair trial guarantees.
6. Establishing a public prosecution and judicial departments specialized in cybercrime, exclusively responsible for investigating and adjudicating this type of case, with continuous training of legal competencies on technical developments in the digital crime environment.
7. Strengthening international and regional judicial cooperation in the field of cybercrime and acceding to relevant international agreements, most notably the Budapest Convention, to ensure the exchange of information and the more efficient prosecution of perpetrators across borders.
8. Supporting legal research in the field of digital crimes, and encouraging universities and legal studies centers in Qatar to produce applied research that contributes to the development of criminal legislation and policies related to cybersecurity.
9. Launching digital legal awareness campaigns for the community, aiming to spread legal culture about cybercrimes and the penalties prescribed for them, with the aim of community prevention and deterrence before the crime occurs.

REFERENCES

1. Abdullah Daghash Al Ajmi, (2014). "The Practical and Legal Problems of Cybercrime: A Comparative Study", Master's Thesis, Middle East University.
2. Ahmed, Moaz Ahmed Abdel Razek, (2016). "Information Security and Its Role in Reducing Electronic Piracy", Master's Thesis, Omdurman Islamic University, Sudan.
3. Al-Mousawi, Ahmad Hassan, (2021). "Cybercrime and Means of Combating It in Comparative Arab Legislation", Beirut, Arab Center for Legal and Judicial Research.
4. Anwar Muhammad Sidqi, (2015). "Illuminations on the Qatari Cybercrime Law", Legal and Judicial Journal, Qatari Ministry of Justice.
5. Bashir Muhammad Al-Fitouri Kandi, (2017). "Cybercrimes in Libyan Legislation: A Comparative Study", PhD, Cairo University.
6. Bushra Hussein Al-Hamdani, (2014). "Electronic Piracy: A Weapon of Modern Warfare", Dar Osama, Amman.
7. Fahd Al-Otaibi, (2017). "Analyzing the Effectiveness of Penal Legislation in Combating Cybercrime: A Comparative Study", Arab Thought Foundation.
8. Faisal Badri, (2018). "Combating Cybercrime in International and Domestic Law", Thesis, University of Algiers.
9. Hanan Rayhan Al-Mudhahki, (2014). "Cybercrimes, Al-Halabi Legal Publications, Beirut.
10. Hassoun Obaid Hajej & Safaa Kazem Ghazi, (2016). "The Effects of the Crime of Email Hacking", Al-Qadisiyah Journal of Law and Political Science, Issue 2, Volume 7.
11. Hatem Ahmed Muhammad Battikh, (2021). "The Development of Legislative Policy in the Field of Combating Information Technology Crimes", Sadat University, Egypt.
12. Hesham Farid Rustum, (2000). "Principles of Technical Investigation," Conference on Law, Computers, and the Internet, United Arab Emirates University.
13. Jassim Muhammad Jandal, (2022). "Cybercrimes", Dar Mu'taz, Amman.
14. Khaled Al-Ghathbar & Muhammad Al-Qahtani, (2021). "Information Security in Simplified Language", Center of Excellence for Information Assurance, Riyadh.
15. Khaled Hamed Mustafa, (2013). "Criminal Liability of Publishers of Technology Services", Emirates Strategic Visions Journal.
16. Khalid Sulaiman Al Hammadi, (2019). "The Crime of Illegal Access to Information Systems in Qatari Law: A Comparative Study", Master's Thesis, Qatar University.
17. Madawi Saeed Al-Qahtani, (2016). "Cybercrime in Gulf Society and How to Confront It", Cooperation Council.
18. Maryam Balta Asia Barghit, (2022). "Information Security in the Face of Electronic Piracy", Journal of Human Rights Studies, Volume 7, Issue 1.
19. Mervat Mahmoud Tayeb, (2017). "Cybercrime: Types, Tools, and Penalties," Arab Center for Cyberspace Research.
20. Nahla Abdul Qader Al-Momani, (2023). "Cybercrimes", Dar Al-Thaqafa, Amman, 2008.
21. Wafaa Muhammad Safi, (2023). "Criminal Protection for the Crime of Electronic Piracy of Electronic Intellectual Property: A Comparative Study", Center for Arab Studies.