*Pakistan Journal of Criminology*
Vol. 16, No. 02, April—June 2024 (47-60)

# The Crime of Invasion Electronic Data and Information in the Emeriti Law

Ali Salem Alalawi[1] &
Mohammad Amin Alkrisheh[2]

**Abstract**

This study examines the crime of unauthorized access to electronic data and information, focusing on the role of the UAE legislator in combating this crime through Federal Decree-Law No. 34 of 2021 on Combatting Rumors and Cybercrimes. It assesses the law's effectiveness in addressing unauthorized activities such as the destruction or removal of information and data, and invasions of privacy. The paper concludes with recommendations to strengthen legal measures against such crimes. Key suggestions include defining "invasion" within the law to clarify the crime and its penalties, distinguishing between personal and professional email breaches with harsher penalties for the latter due to their significant impact on both state-owned and private enterprises, and recognizing the disruption of information networks as a punishable offense. These recommendations aim to enhance the UAE's legal framework for protecting electronic data and information.

**Keywords:** Cybercrimes, Information Network, Electronic Information System, Information Technology Tool.

## Introduction

Advancements in science and technology have brought about a significant increase in the complexity and variety of cybercrimes. This evolution has necessitated a closer link between legal frameworks and technological developments to ensure adequate legal protection against these digital threats. As technology progresses, so too does the domain of legal incrimination, requiring continuous adaptation to keep pace with new forms of cybercriminal activity (Mphatheni, & Maluleke, 2022).

Cybercrimes, which are carried out using a range of electronic devices, present in diverse and previously unseen forms. These crimes, deeply intertwined with scientific and technological advancements, have become more discernible through meticulous scrutiny. The global surge in technological development across all sectors has invariably led to an uptick in crimes related to the theft of data and

[1] Ali Salem Alalawi is a graduate student, Master of Criminal Sciences program at the College of Law, Al Ain University, United Arab Emirates.
[2] Professor Mohammad Amin Alkrisheh is a Professor of Criminal Law at the Public Law Department, College of Law, Al Ain University, UAE. He stands out as a prominent figure in the realm of criminal law, with significant contributions to academic and legal discourse.

information within the electronic realm. This scenario is exacerbated by the widespread use of computers and the internet, highlighting the pressing need for updated or new legislation to protect data, with far-reaching implications for both individuals and businesses (Sarre, Lau, & Chang, 2018).

In response to the challenges posed by these emerging threats, the United Arab Emirates (UAE) has proactively updated its legal arsenal. This includes the enactment of the Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes, Law No. 5 of 2017 on the Use of Remote Communication Technology in Criminal Procedures, and Ministerial Decree No. 220 of 2017 on Establishing a Deputy for Information Technology Crimes. These legislative measures underscore the UAE's commitment to combating the multifaceted dangers posed by cybercrime, which threatens individuals, as well as public and private institutions alike. The present research aims to assess the effectiveness of these laws in addressing the complex landscape of cybercrime, emphasizing the need for continuous legal innovation in the face of evolving digital threats.

The following questions can be raised out of the research problem:

- What is the efficacy of the legal provisions on the crimes of invading data and information, and to what extent do these provisions help decrease the dissemination of such crimes?
- To what extent is practical criminal protection provided for the safety of data, information networks, and private life against invasion?

The present research makes use of the descriptive, analytical method, where description and analysis were used to investigate the Emeriti legislator's plan in incrimination and in determining the penalty for crimes of invasion of data. A description and analysis of the common judgments for this crime will also be made.

**Literature Review**

Before we define data, we should first show the difference between data and information, though sometimes they both have the same meaning. However, in information technology, there are some differences between the two terms. In other words, "data" are "raw facts that are not organized, unready for use, and not processed yet (Sari, 2018)." On the other hand, "information" is "processed and organized data and is ready for use (Sari, 2018 Bunga, 2019)."

In terms of safety, data are "a group of digital or paper materials which are owned by some party. Data may include information, facts, or both. These facts may be clear or unclear, may or may not be used, and may or may not be benefited from. They do not contain any actual value for any party (Sayyed, 2017)."

On the other side, in terms of safety, information is "part of data which is clear and understandable, and which can be used and benefited from. Information has an actual value for some party. Moreover, information is data (raw) for one party and information (meaningful) for another. Information doesn't need to be written as text. It may instead be a photograph, voice record, video record, or shapes (Sayyed, 2017 Bunga, 2019)."

Furthermore, "data are known, in their primary form or their disorganized form, as a group of facts such as numbers, alphabets, fixed photos, video, voice records, or stickers (Saudi Authority for Data and Artificial Intelligence, 2021)."

In addition, personal data has been defined as "any piece of data, no matter which source or form it has, that can lead to the recognition of the person in particular, or that make the person identifiable directly or after being combined with other pieces of data. Such a piece of data may include, but is not limited to, name, personal identity numbers, addresses, contact numbers, bank account numbers, credit cards, and fixed or moving photos of the user, among other personal data (Saudi Authority for Data and Artificial Intelligence, 2021)."

We should distinguish between two forms of information: casual information and private information. Casual information is general information that is shared with others and does not benefit only one party. Casual information does not contain harmful materials that inflict damage on other parties should they access them. Examples of this type of information include scientific information, literary information, medical information, news, TV programs, movies, songs, books, newspapers, and CDs (Baumann & Schünemann, 2017).

On the other hand, special information is linked to one party that does not want to share it with another party and does not want another party, unless with permission, to have access to information. This information should be protected from stealing, disclosure, or destruction. Meanwhile, the specialty of data security is concerned with protecting special data only and does not protect casual data or even information (Baumann & Schünemann, 2017).

**Legal Definition**

One meaning has been considered for data and information by the Emeriti legislator. We shall touch upon this topic from different parts of "Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes." He defined data and information as "a set of organized or disorganized input, events, concepts, instructions, observations or assessments that take the form of numbers, letters, words, symbols, photos, videos, signs, sounds, maps, among other forms. They are interpreted, exchanged, or processed either by individuals or computers. Once

processed or exchanged, they have termed information (Article 1 of Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes.)."

The Emeriti legislator distinguished between governmental, personal, and secretive data and information. He also highlighted route data and false data. Governmental data is "electronic information or data that are not accessible for all. Rather, they belong to one of the state-owned institutions (Article 1 of Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes)."

On the other hand, he defined personal data as "information or data that belong to real persons. That is, they are related to their personal life, determine their identity, or, by merging these data and information directly or indirectly, they help identify someone's identity (Article 1 of Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes)."

Finally, "route data" has been defined as "an information technology tool that is produced by an information system. This tool gives information about the caller and the receiver, the time, date, amount, duration, and type of service (Article 1 of Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes)." Route data have been defined by the Egyptian legislator as "data that are produced by an information system. This information shows the caller and receiver, the path of the call, the time, date, amount, duration, and type of service (Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes)."

The Emeriti legislator mentioned direct and detailed provisions on data and information. He considered different penalties based on the conducted crime (misuse, larceny, etc.).

**The Crime of Invading Data and Information**

The crime of invading networks, systems, and information technologies is among the most significant negative aspects caused by the information revolution. This is a technological threat to information (Farahbod, Shayo, & Varzandeh, 2020). To determine penalties, the different aspects of the crime should be clarified.

Based on what has been mentioned, we shall touch upon the aspects of the crime of invading data and information. We shall also discuss the penalty that is determined for invading data and information.

**Aspects of the Crime of Invading Data and Information**

There are two aspects to the crime of **invading governmental data and information:** material and spiritual.

**First: Material Aspect**

The material aspect is about "acquiring, taking over, uncovering, destructing, removing, coping, canceling, distributing or redistributing data and information without a secretive governmental permission (Article 7 of Federal Decree Law No. 34 of 2021 on Combatting Rumors and Cybercrimes)."

Thus, criminal activity manifests itself in multiple ways including achieving, taking over, entering, remaining, or hacking as indicated before. This entering shall be done to a website, email, personal account, or information system operated with the knowledge, or for the benefit, of the government or its relevant party. Moreover, the entering or remaining shall be without a right. Lastly, criminal behavior shall be done through an information network or one of the information technologies means (Al-Gondi: 2009).

**Second: Spiritual Aspect**

This crime is among the deliberate crimes in which the criminal intent is spiritual. The criminal intent is composed of two components: knowledge and will. Knowledge is about the criminal's perception of the criminal activity. It is about "entering with intent to receive governmental data or secretive information of a financial, trading or economic party. The criminal activity may include canceling, removing, destroying, uncovering, changing, copying, distributing or redistributing." Moreover, the criminal shall know the danger of his act. Thus, if the criminal does his act and still believes that he did not enter or invade with the wrong intent, the component of knowledge shall be cancelled (Qureh: 222).

The criminal's intent shall be the building block for one of the behaviours mentioned in the provisions. Without this intent, the criminal intent shall be disregarded. For example, if the act is performed because of a mistake or stupidity, the intent shall be missing (Al-Malat: 2006). Moreover, no import shall be given to the doer of the criminal activity (Al-Gondi: 2009).

**The Penalty Determined for the Crime of Invading Data and Information**

The Emeriti legislator has criminalized the act of invading governmental data, where this act is a form of stealing data, as provided in "Article 7 of Law of Combatting Rumours and Cybercrimes." The legislator provides "He who receives, takes over, destroys, reveals, cancels, removes, copies, distributes or redistributes secret governmental information or data without permission shall be penalized with a temporary imprisonment for a period lasting no less than 7 years and a fine no less than 500.000 Dirhams and no more than 3.000.000 Dirhams."(Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes )

The penalty for stealing governmental data shall be intense if the aforesaid acts inflict damage to the government, or if they cause the security and army electronic programs and systems, and whatever has to do with secretive communication and information transfer, to lose their secrecy. For the crime, the penalty determined by the Emeriti legislator is prison for a period no less than 10 years and fine of no less than 500.000 Dirhams and no more than 5.000.000 Dirhams." Furthermore, if the criminal "reserves the information or data, or saves or makes use of the data or information despite his knowledge about the illegality of doing so" the penalty shall be a temporary imprisonment. (Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes)

**Invading Data of Personal Life**

Here, we shall discuss the aspects of invading data in personal life and the penalty considered for it.

**Violation of the Personal Life**

This crime has two aspects: material and spiritual.

**Material Aspect**

The material aspect concerns an activity where the criminal invades the "privacy of a person or the personal or family life of individuals (Article 44 of Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes)" without their consent and beyond what has been permitted in law.

No legal definition has been provided for the idea of private and family life either in constitutions or legislations responsible for protecting life. The personal life of the individual has been defined as "something away from proneness to others without the permission of the person, or something that puts the person and his secrets in a safe zone. By secrets, we mean those things that the person wants to be distant from others, no matter who they are; they might be close relatives or others who have no relation to the person at all. Moreover, personal life applies to the person either when he is at home or outside. Also, personal life ensures that the person spends some time with himself, during which time, he and his family members behave with freedom (Parent, 2017; Al-Shamesi, 2021)."

The behaviour of invasion can be the following: eavesdropping, traversing, recording, transferring, or uncovering conversations, calls, or voice or video materials. Such behaviours may also include taking photos from others, or creating, transferring, uncovering, copying or reserving electronic photos. Furthermore, disseminating electronic photos or news, photographs, videos,

comments, data, and information (even if true) can be considered as among other forms of invasion. Finally, any form of editing or processing a record, photo, or video with the intent to inflict damage to the reputation of someone or invade and violate the privacy of someone shall be regarded as other forms of invasion (Article 44, paragraphs 1 through 5 of Federal Decree-Law No. 34 of 2021 on Combatting rumors and Cybercrimes)."

"The invasion of family values and principles occurs using an information network, electronic information system, or one of the information technology tools." This invasion may include distributing news about a whole family, which affects the reputation and values of that family. Alternatively, distributing messages that destroy the values and principles of a family or distributing photos of a certain family being present in a bar, where selling alcohol or gambling occurs, are other forms of invasion. Invasion of family principles and values also includes attributing a certain occurrence to a certain family which in turn devalues the family (Parent, 2017. Al-Haj, 2013). The right to privacy strongly has to do with human beings, and this right has long been among the disputed rights among jurists, Moreover, personal life is holy and was protected by ancient civilizations, religions, constitutions, and positive laws in most countries.

**Spiritual Aspect**

The crime of invading private life is among the intentional crimes where the criminal intent is spiritual. The criminal intent comprises two components: knowledge and will. Knowledge is about the criminal's perception of the reality of the criminal activity. In this case, the criminal invades the privacy of the person without permission, for example through eavesdropping, traversing, recording, transferring, or uncovering conversations, calls, voice, or video content. Other forms of invasion include taking photos from others, making electronic photos, or uncovering, copying, or reserving photos. Distributing news, electronic photos, photographs, videos, comments, data, or information, even if true and real, shall be regarded as an invasion. Lastly, making any editing or processing of a record, photo, or video with the intent to damage the reputation of someone else, or invade and violate the privacy of someone is also a form of invasion (Article 44 of paragraphs 1 through 5 of the Federal Decree-Law No. 34 of 2021 on Combatting rumours and Cybercrimes).

The criminal shall be knowledgeable about the danger of his crime. Moreover, the criminal shall be aware of using a tool for listening or eavesdropping on private conversations or phone calls. Yet if the criminal was not proven to be aware of his criminal behaviours, the spiritual aspect shall be

cancelled and thus the condition shall not be considered as a crime (Khirshah, 2016).

To consider it as a crime, the act shall be done with the will to eavesdropping or recording the private or phone conversations. Moreover, the person on whom the crime is done must not have consent to the act. Last, the will must lead to a behaviour and a result, which is acquiring a conversation or phone call. Thus, if the will is not present, the spiritual aspect shall be absent and there shall be no crime.

Furthermore, if the eavesdropping to the phone call was due to an interference of lines caused by impairments in a communication network, there shall be no crime. In this case, the basis for canceling the crime is the lack of the two components of criminal intent (Johl,2018).

**Use of Personal Data in a Way Against Public Etiquette**

This crime premises upon the material and spiritual aspects, which shall be discussed as follows:

**Material Aspect:**

The material aspect is about the criminal's intentional use of an electronic information system or one of the information technology tools for processing the personal data of someone else. He does so to relate those data with content against public etiquette or to display those data in a way that inflicts damage on someone's credit and dignity (Klitou, 2014).

Article 34 provides that criminal behaviour lies in "creating, managing or supervising a website, or displaying, sending, distributing or redistributing, through information network, sexual content or whatever is against public etiquette. A criminal is he who creates, prepares, sends or stores such contents with intent to exploit, distribute, or display to someone else through the information system (Article 34 of Federal Decree-Law No. 34 of 2021 on Combatting rumours and Cybercrimes)." With public etiquette, it is meant "any rules that people find themselves obliged to follow (Yahia, 2019)."

Taking over and disseminating unpermitted information is dangerous. However, the most dangerous behaviour is when this information is used by someone who took over the information from his opponent in an illegal manner. This incrimination includes any processing of the personal information of someone else to combine it with content against public etiquette or display it in a way that inflicts damage on the victim's privacy.

It can be inferred from the provision that exploiting the information even once would make the crime happen, given that the provision does not mention the

number of times that the stealing must occur. The legislator, however, made it a condition to use an electronic information system or one of the information technology tools in processing and editing the personal data of someone else to combine it with content against public etiquette or to display it in a way that invades the privacy of the victim (Johl, 2018).

**Spiritual Aspect**

This crime is among the intentional crimes where the criminal intent is spiritual. The criminal intent is comprised of two components: knowledge and will. Knowledge is about the criminal's perception of the reality of the criminal activity. That is, the criminal must deliberately make use of the electronic information system or one of the information technology tools in processing the personal data (editing or processing a record, photo, or video) to combine them with content against public etiquette (damaging the reputation or invading the privacy of someone), or to display it in a way that damages his credit and dignity. (Johl, 2018. Parent2017).

The criminal must know the danger of the behaviour. The criminal's will, moreover, shall be directed at criminal behaviour. Thus, without this will, there shall be no crime. In addition, it may be proven that the person did not conduct the criminal activity with the intent to combine the data with data against public etiquette (to damage the reputation or invade the privacy of someone), or to damage a victim's dignity and credit. Rather, it was shown that the person merely wanted to draw and teach, or the person was a student who sent the data to an information system (Al-Malat, ibid: 549). In such a case, there shall be no crime.

**The Penalty for Invading Data in Personal Life**

**Invading the Privacy of Personal Life**

The Emeriti legislator criminalized invading the principles of family and personal life. He specified an appropriate penalty for this crime, as mentioned in Article 44 of the Law of Combatting rumours and Cybercrimes. That is, the criminal shall be jailed for no less than six months and a fine of no less than 150.000 Dirhams and no more than 500.000 Dirhams. The criminal is whoever makes use of an information network electronic information system or one of the information technology tools with intent to invade the privacy of someone or the family life of individuals without their consent and beyond what has been mentioned in law. The crime may be done through the following ways: 1. Eavesdropping, recording, transferring, displaying, or uncovering conversations, calls, voice, or video materials; 2. Taking photos from others in any public or private place, as well as making, transferring, copying, and restoring electronic

photos; 3. Disseminating news, electronic photos, photographs, videos, comments, data, or information (even if true and real) with intent to inflict damage to someone; Taking photos of the dead or victims of events or disasters, and transferring and disseminating them without permission of the responsible figures. In addition, whoever makes use of an electronic information system or one of the information technology tools to make any editing or processing to a record, photo, or video with intent to damage the reputation of someone, or to inflict damage on them, shall be penalized with an imprisonment of no less than a year and a fine of no less than 250.000 Dirhams and no more than 500.000 Dirhams, or with one of the two aforesaid penalties. (Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes)

The reason for the incrimination is that the public attaches a high weight to several principles including the protection of the family and its values. Moreover, the incrimination shall decrease the influence of internet networks and information technology tools on society and family (which is part of society) and shall protect the privacy of personal and family life.

**Using Personal Data in a Way Against Public Etiquette**

The Emeriti legislator, as mentioned in Article 34 of the Law of Combatting rumours and Cybercrimes, criminalized using personal data in a way that violates public etiquette. He has mentioned that "whoever creates, manages or supervises a website on sexual content, or whoever exchanges, sends, distributes, redistributes or displays such a content or anything that may inflict damage on the public etiquette, shall be penalized by an imprisonment and a fine of no less than 250.000 Dirhams and no more than 500.000 Dirhams, or with one of the two penalties (imprisonment or fine)." Moreover, whoever creates, prepares, sends, or restores such content with the intent to exploit, distribute, or display to someone else through the information network, shall be penalized with the same penalty. Furthermore, if the subject of the sexual content is a child, or if the content was prepared to attract children, the criminal shall be jailed for a period no less than one year and a fine of no more than 50.000 or by one of the two penalties. (Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes

When the incrimination occurs, the systems, programs, or tools used for conducting any of the crimes shall be taken over and the data and information shall be removed (Article 56 of Federal Decree-Law No. 34 of 2021 on Combatting rumours and Cybercrimes). Meanwhile, initiating the crime shall result in half of the penalty (Article 56 of Federal Decree-Law No. 34 of 2021 on Combatting rumours and Cybercrimes).

The rationale for incrimination, in the first place, is that using information networks and information technology tools has led to the spread of activities and practices that violate public etiquette and the credit and dignity of individuals. This led the Emeriti legislator as well as the Arabic and counterpart legislations to confront this phenomenon through incrimination. This is especially true as these practices occur secretively. Secondly, those activities are against Islamic instructions and contradict the principles and values of a healthy family. Thirdly, the criminal's behavior is exploitation of computers to disseminate shameful sexual affairs, and to train individuals, regardless of their age and gender, on practicing them. Computers are also used to display photos and videos that are seductive or against etiquette (Al-Alfi, 2011).

Based on what has been discussed about the forms of invasion of data, it can be clear-cut that the Emeriti legislator did not distinguish between destroying data, information, and programs, and hampering, destructing, or removing legal information through detailed legal provisions. Instead, he incriminated all these activities and combined them in legal provisions. In addition, the Emeriti and counterpart legislations are not limited to protecting a certain type of invasion of data and information. Rather, all forms of invasion, regardless of their difference, are considered in the same domain. These forms may include cancelling, removing, destroying, revealing, destructing, changing, copying, distributing, or redistributing.

Multiple and various are preventive actions either for individuals or for objects. The court is permitted, when making a judgment for any of the aforesaid crimes, to consider any of the following actions: 1. Ordering to put the accused person under electronic monitoring or to deprive him of using the information network, electronic information system, or any other information technology tool. Moreover, the accused person may be put in a treatment environment or a rehabilitation centre for some time that the court finds appropriate; 2. Closing the violating site partially or completely if it is technically possible; and 3. Boycotting the violating site partially or completely, as determined by the court.

An imprisonment for a period not longer than a year and a fine not higher than 5.000 Dirhams shall be considered for he who violates any of the judgments made by the court against him. Meanwhile, the court shall order to let the action last for a period not longer than half of the length of imprisonment and it shall not be, whatsoever, longer than three years. Instead, the court may order to change the preventive action with another one. (Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes

## Conclusion

This research has critically examined the legal framework established by the Emeriti legislator under Federal Decree-Law No. 34 of 2021 on Combatting Rumours and Cybercrimes, with a particular focus on its approach to various forms of cyber invasions. Our findings reveal several key insights into the current legal provisions and their implications for privacy, intellectual property, and economic security. Notably, the law's treatment of photography in public places as an invasion of privacy, its relative leniency towards personal email data breaches compared to previous legislation, and the absence of distinction between personal and spiritual email invasions raises important considerations for the effectiveness and comprehensiveness of cybercrime legislation.

Furthermore, the legislation's generalized approach to criminalizing the destruction of data, information, and computer systems without distinguishing between different forms of cyber harm highlights the need for more nuanced legal provisions. The comparison with Egyptian legislation on the criminalization of information system tampering underscores a potential area for legislative enhancement in the UAE.

Based on our analysis, we recommend the introduction of specific definitions and distinctions within the law, particularly regarding the term "invasion" and the differentiation between types of email invasions. Additionally, recognizing the use of virus-infected programs to compromise data integrity and proposing targeted penalties for such acts would significantly strengthen the legal framework. The recommendation to explicitly criminalize tampering with information networks further aligns with international best practices in cybercrime prevention.

In conclusion, while Federal Decree-Law No. 34 of 2021 represents a significant step forward in addressing cybercrimes within the UAE, our study suggests areas for refinement and expansion to better protect against the evolving landscape of cyber threats. Future legislative amendments should aim to address these gaps, ensuring a more robust and effective legal response to safeguard personal and economic interests in the digital age. Such enhancements will not only reinforce the UAE's cybersecurity infrastructure but also contribute to the global efforts in combating cybercrime.

**References**

Ahmad, A. A. (2013. The Criminal Accountability of the Crimes of Electronic Distribution in Light of Law of Combatting Cybercrimes in the Emirate, *Al-Fikr Al-Shorti Journal*, version 22, No. 2, General Authority of Sharjah Police, Research Center for Police, UAE, p. 12.

Ahmad, M. A. (2006). *Information Crimes*, Dar Al-Fikr Al-Jami'i, 2nd edition, Alexandria. P.138.

Asma, A. S. (2018) "*Crimes of Invading the Privacy of the Personal Life of Individuals in Light of the Decree Law No. 5 of 2021 on Combatting Cybercrimes: A Comparative Study*." MA thesis in public law, UAE University, College of Law, p. 8.

Baumann, M. O., & Schünemann, W. J. (2017). Introduction: Privacy, Data Protection and Cybersecurity in Europe: The Conceptual and Factual Field. *Privacy, data protection and cybersecurity in Europe*, In book: Privacy, Data Protection and Cybersecurity in Europe, (1-14) DOI: 10.1007/978-3-319-53634-7_1.

Bunga, D. (2019). Legal Response to Cybercrime in Global and National Dimensions. Padjadjaran Journal of Law, 6(1), 69-89.

Farahbod, K., Shayo, C & Varzandeh, J. (2020). Cybersecurity Indices and Cybercrime Annual loss and economic impacts. *Journal of Business and Behavioural Sciences*, *32*(1), 63-71.

Hosni. G. (2009). *Special criminal legislation in the United Arab Emirates*," (Academy of Police Sciences), Sharjah,p. 244.

Ibrahim, K. Y. (2019) "*Towards Narrowing Down Public System for the Benefit of Foreign Law within the Context of International Private Law: A Comparative Study*." University of Sharjah Journal of Sharia and Law Sciences, 16th edition, No. 2, p. 154.

Johl, R. (2018). Reassessing Wiretap and Eavesdropping Statutes: Making One-Party Consent the Default. *Harv. L. & Pol'y Rev.*, *12*, (177-207).

Klitou, D. (2014). Privacy-invading technologies and privacy by design. *Information Technology and Law Series*, *25*, 27-45.

Mohammad, A. K. (2016) "Legal Protection for the Privacy of Private Life in the Emeriti Penal Law," *University of Sharjah Journal of Sharia and Law Sciences*, 13th edition, No. 1, p. 74.

Mohammad, M. A. (2011). *The Criminal Accountability of Moral Crimes on the Internet*," PhD dissertation, Cairo University, College of Law, p. 64-65.

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering

recommendations to the African regions. *International Journal of Research in Business and Social Science*, *11*(4), 384-396.

Naelah, A. Q. (2005). "*Economic Computer Crimes*", Al-Halabi Publications, 1st edition, Beirut. p. 222.

Parent, W. A. (2017). *Privacy, morality, and the law*. In *Privacy* (pp. 105-124). Routledge.

Sari, M. K. (2018). *"Directions in the Safety of Information: The Importance of Cyphering Technique,"* Obaikan Publication, Riyadh, Saudi Arabia, p. 7.

Sarre, R., Lau, L. Y. C., & Chang, L. Y. (2018). Responding to cybercrime: current trends. *Police practice and research*, *19*(6), 515-518.

Saudi Authority for Data and Artificial Intelligence, "Policies of Governance of National Data," National Data Management Office, second issue, 26/05/2021, p. 13.

Somayeh, S. M. (2017). *"Factors of Digitalization in Arabic Electronic Periodicals in Science and Technology***,**" Al-Fajr for publication and distribution, first edition, Cairo, p. 379.