Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 16 (1), 2024
pp. 1106 - 1114

The Role of Administrative Control in Protecting the Administration's Electronic Data

[1]Thakaa Nohad Sabri , [2]Batool Majid Jassim

[1]College of Law, University of Basrah, Basrah, Iraq

Email: lawpg.thakaa.nohad@uobasrah.edu.iq

[2]College of Law, University of Basrah, Basrah, Iraq

Email: betoul.majeed@uobasrah.edu.iq

Abstract

The issue of possible treatments and solutions to protect the electronic data of the administration requires knowledge of criminal protection and its forms and forms of infringement on that data. Information protection may also be through encrypting and archiving the administration's data. Moreover, organizational treatments may have an important role in protecting electronic data, through measures to control access to electronic sites and control their contents by blocking electronic sites, with the necessity of ensuring the protection of freedoms in measures to block electronic sites.

Keywords : Control , Electronic data protection

Received: 20 March 2024 Revised: 17 May 2024 Accepted:22 June 2024

Introduction

First - Research idea

Administrative control is the basic function of public administration in every country. This control function is the most dangerous and important and emerges as an essential aspect of the existence of the state and as a primary expression of the sovereignty of the ruling authority. It is possible to imagine the existence of a human society without a system that controls the behavior of the individual within it. Administrative control aims to protect the public order by taking measures that restrict the exercise of individuals' freedoms and private activities according to the type of freedom that is to be restricted. The powers of administrative control also expand under exceptional circumstances to confront these circumstances.

There is no doubt that the contemporary world is experiencing a huge information revolution, one of the results of which is controlling its administrative and political institutions, especially after the spread of electronic work, Internet networks, and local and global information and communications systems, and they began to play an important role in achieving economic, social and political development, which contributes to linking the citizen to social institutions on the one hand and linking institutions with each other through modern technological mechanisms, far from the traditional administrative concepts that contributed to the spread of administrative and financial corruption alike. Thus, electronic administration is no longer a social luxury as much as it is a necessity Its importance is imposed by local and international circumstances and challenges.

It is worth noting that E-administration is the transformation of all administrative processes of a paper nature into processes of an electronic nature using electronic technology files in the administration. There is no doubt that this importance of e-administration has an effective impact on governmental and

non-governmental institutions and on the efficiency of performance of individuals in those institutions. It is necessary to highlight the role of administrative control of the public administration in protecting electronic administration data, especially after the spread of the Internet, as public institutions need more attention to electronic administration in order to facilitate access to services. The researcher addressed the role of administrative control by using material and legal means to protect electronic administration data and protect it civilly and criminally as a penalty for violating it.

Second - The importance of the research The importance of the research is highlighted in:

1. Clarifying the role of the administration in protecting the administration's electronic data
2. Clarifying the means used by the administration to protect that data
3. Shedding light on the legal foundations and mechanisms adopted to protect data
4. Clarifying whether the legislation is sufficient to protect that data.

Third - The research problem

The research problem emerges in clarifying the extent of the efficiency of legislation related to data protection in general and electronic data in particular What are the mechanisms and means used by the administration and is there legislative control in the correct sense to protect data and is it characterized by its sufficiency and efficiency What are the legal solutions to increase the efficiency of the administration's role in protecting electronic data What is the legal basis for the administration to protect that data and what are the challenges and obstacles facing the administration in practicing administrative control over electronic data for the purpose of protecting it and identifying shortcomings due to weak administrative control.

Fourth - Research Methodology

The study relied on the analytical approach, as it was considered the most consistent approach with the nature and objectives of the current study. This approach is based on a theoretical study to build the cognitive framework by benefiting from various references and sources between books, research and scientific papers published in periodicals, conferences and seminars, whether those found in the university library or published in electronic databases via the Internet specific to the research topic. The study also relied on addressing the most important judicial decisions that highlight the role of the administration in protecting the administration's electronic data, with the help of comparative laws and standing on the extent of the efficiency of legislation and its importance in achieving optimal protection for the structure of electronic administration.

Fifth - Research Structure

To clarify and explain the research topic, we will address it in two sections. In the first section, we will discuss the legal treatments for protecting the administration’s electronic data, then in the second section, we will explain the criminal and administrative protection of that data.

The role of administrative control in protecting the electronic data of the administration

The issue of possible treatments and solutions to protect the electronic data of the administration raises problems related to determining the crime committed and how to apply the provisions of criminal laws to it, since this information has a moral nature abstracted from its physical media, and from here the difficulty of applying the provisions of traditional criminal law emerges; since this information does not take a tangible physical entity, because its location is programs or data that have a moral nature.

The first requirement

Criminal protection of information

Criminal protection is defined as a set of substantive and procedural legal rules that the judiciary relies on to regulate rights and impose penalties, as the criminal law, with its rules and texts, constitutes the means used for this protection. Criminal protection is what the criminal law guarantees in its two sections, the Penal Code and the Code of Criminal Procedure, from rules and procedures through the penalties it decides in the event of an attack on various information or damages caused to it as a result of acts of

aggression. Therefore, criminalization is primarily based on protecting interests that the legislator has considered among the interests worthy of protection, so he determines them by stipulating them in the law and estimating the degree of protection they deserve, as the legal text revolves with the interest it protects, in terms of existence, absence, and modification. Protection also loses its worthiness when the reason for criminalization disappears, and the legal justification also loses its justifications when the reason for criminalization disappears.

The criminal protection of information arises from the constantly growing and renewed technological development, especially in the field of information, as this information represents a set of symbols and tangible material facts, and once it is processed automatically, the data turns into flexible information that can be stored in multiple media. To discuss the criminal protection of information, we address this protection under the Iraqi Penal Code No. 111 of 1969, as amended, the draft of the Information Crimes Law of 2011, and the Document Preservation Law No. 38 of 2016. Based on the above, we must clarify this requirement in two sections. In the first section, we address the forms of criminal infringement on the administration's electronic data, and in the second section, we address the forms of criminal protection of information, whether it is substantive or procedural criminal protection.

Section One

Penal forms of infringement on the administration's electronic data

Penal protection is the criminalization of any form of infringement on the administration's data and information, whenever this infringement constitutes a crime in itself, and since this data is the main axis around which the administration revolves, we will show the most prominent forms of infringement on the administration's data, which are:

First: Manipulating management data

This type of informational assault is one of the most common forms of crime, as the data contained in the information system is manipulated in two forms: direct manipulation and indirect manipulation:

A- Direct manipulation: by entering data with the knowledge of the person responsible for the information department.

B- Indirect manipulation: This is done through indirect interference in the data recorded in the information system, and is often done using one of the storage media or by remote manipulation using certain means and knowing the numbers and codes of the accounts. The draft Cybercrimes Law of 2011, based on what was approved by the House of Representatives and ratified by the Presidency Council and based on the provisions of Clause (First) of Article 61 and Clause (Third) of Article 73 of the Constitution, indicated that "Whoever provides false electronic information or data to the judicial or administrative authorities, knowing that it is incorrect, shall be punished by imprisonment and a fine of not less than (5,000,000) five million dinars and not more than (1,000,000) ten million dinars." The draft Cybercrimes Law also indicated that "Whoever makes a change or manipulation in any electronic document and uses it before any private or public entity shall be punished by imprisonment and a fine of not less than (1,000,000) ten million and not more than (1,500,000) fifteen million."

From the above, we see the necessity of stipulating the crime of tampering with administrative data by the Iraqi legislator when approving the Anti-Cybercrime Law, as it is one of the most serious crimes that affect the administration's information system.

Second: Destruction of management data

The data contained in the information system is the target of many attempts at destruction and hacking, as the attacker of that data tries to obtain it in various ways, and when he does so, that data is exposed to damage in two ways: either replacing the data, such as replacing one number with another or a specific date with another date, and this type of crime is very dangerous because if the forgery is successful, the crime may continue for a long period of time until it is discovered, while the other way is to erase the data

by deleting it from the information system, and this crime does not require great skills in computer technology, as even an ordinary user can commit it with ease, in addition to the possibility of removing its effects with ease as well.

The French Penal Code of 1992 referred to the crime of information destruction by stating that "anyone who fraudulently enters data into an automated information processing system or deletes or modifies data shall be punished by imprisonment for a period of five years and a fine of (75,000) seventy-five thousand euros."

The American legislator has stipulated the crime of intentional and unauthorized destruction of information contained in a computer belonging to the United States government and its administration, or a computer not belonging to this government, but used by it or for its benefit, or obstructing this computer from performing its various tasks that it performs for the benefit of the government.

The Iraqi legislator indicated in the draft law on cybercrimes, "Anyone who uses the information network to intentionally destroy, disable, or damage computer systems and devices or the information network of state departments with the intent to harm their system and infrastructure shall be punished with temporary or life imprisonment and a fine of no less than (2,500,000) twenty-five million dinars and no more than (50,000,000) fifty million dinars," as well as Article (13, paragraph one) of the same draft law, which states, "Anyone who destroys or damages a signature, means, or electronic document shall be punished with imprisonment for a period of no less than three years or a fine of no less than (5,000,000) five million dinars and no more than (1,000,000) ten million dinars." The draft law on cybercrimes for the year 2011 also indicated that "Anyone who destroys, defects, or damages an electronic document or electronic document used to prove rights shall be punished with imprisonment for a period of no more than three years or a fine of no less than (1,000,000) ten million dinars and no more than (1,500,000) fifteen million."

Section Two

Images of Criminal Data Protection

The topic of criminal data protection is one of the topics of great importance that is regulated by multiple laws. To clarify the images of this protection, we must distinguish between two types of criminal protection: -

First: Objective criminal protection: This protection is regulated by the Penal Code by criminalizing acts that constitute an infringement on the protection of the interest subject to protection, such as protecting information from attack, and according to what is stipulated in penal laws such as the Iraqi Penal Code No. 111 of 1969, as amended, or special laws, as well as agreements related to data protection and imposing illegality on actions that harm it.

The TRIPS Agreement of 1994 stated that "collected data or other material, whether in machine-readable form or any other form, shall be protected if it constitutes an intellectual creation resulting from the selection and arrangement of its contents." The French Commercial Court of 1998 ruled that innovation is the scope of data protection, and that innovation related to data requires a special effort in research, selection and analysis, which when compared to mere documentation, shows the importance of the innovative effort of the work. Egyptian Law No. 82 of 2002 regarding the protection of individual property rights stated that "databases shall enjoy the legal protection established for the author's rights over his literary works, whether this data is readable from a computer or otherwise."

The concept of data refers to a group of words, numbers, symbols, facts or statistics that have no relation to each other, some of which have not been subject to interpretation or preparation and are not devoid of apparent meaning, while others see them as facts that may express certain positions and actions, whether that expression is in words, numbers or symbols, and according to Egyptian Law No. 38 of 1992 amending the repealed Egyptian Copyright Law No. 354 of 1945, which states: "The protection stipulated

in the Copyright Law includes computer works, programs, databases and similar works, determined by a decision of the Minister of Culture."

The Egyptian Law No. 82 of 2002 on the Protection of Intellectual Property also referred to the standard of innovation and required the element of distinction in the arrangement and presentation or any personal effort worthy of protection. The Egyptian legislator came in agreement with the TRIPS Agreement of 1994 (the Agreement on Trade-Related Aspects of Intellectual Property Rights), which required the availability of intellectual creation worthy of protection and not just abstract data, by stating "1- Computer programs and data collection.

2- Collected data or other materials, whether in machine-readable form or any other form, shall enjoy protection if they constitute an intellectual creation as a result of the selection or arrangement of their content. This protection does not include the data itself, and does not prejudice the copyright related to this data or the materials themselves."

The World Intellectual Property Convention of 1996 stipulates that "collections of data or other material, regardless of their form, which by reason of their content or arrangement constitute intellectual creations, shall be protected as such." However, not all laws and regulations follow this approach. The French law of 1998 does not require any condition for data protection, but rather the financial, human or material effort expended is sufficient. Therefore, the French law protects this data for a period of 15 years and prohibits any reuse of part or all of this data. This protection goes beyond the general rules that require innovation, as it adds special protection for the data, even if the element of innovation is not available in some cases, with the aim of providing better protection for copyright.

The Berne Convention is one of the first agreements that regulated the subject of digital works and provided protection for them. It was concluded in 1887 and was amended several times, the last of which was in 1971. We find that it refers to the protection of literary and artistic copyright, meaning that the purpose of the agreement is to protect the literary and artistic rights of authors over their digital works. The same agreement referred to the protection of computer programs regardless of whether they are in the source language or machine language, as they are literary works and computer data is considered literary works that require protection.

Second: **Procedural criminal protection** This protection is regulated by the Criminal Procedure Code No. 23 of 1971 through litigation procedures, the formation of courts, the determination of their jurisdiction, the issuance of judgments, methods of appeal, and the implementation of penalties. Since electronic crime has raised some problems regarding the objective framework in its legal structure, in search of the possibility of applying traditional criminal texts to this type of crime, it has at the same time raised many problems regarding the procedural framework of these crimes. As a result, the traditional texts of the Criminal Procedure Code have become a stumbling block that hinders the work of the authorities concerned with uncovering the truth of the crime and extracting its evidence, due to the ease of erasing or destroying evidence, which is called digital evidence due to its technical nature. Therefore, this type of crime has put the Criminal Procedure Code in a real predicament.

As for the possibility of conducting an inspection of a computer or any other electronic device, in fact the computer consists of physical components such as the keyboard and screen, and intangible components such as programs and processing data, and there is no dispute about the possibility of inspecting the physical components in search of evidence to reveal the truth and reach the perpetrators because they are subject to traditional inspection procedures. As for inspecting the intangible components of the computer, a jurisprudential debate has arisen about the extent to which it is possible to inspect data and information. The first trend is that it is not valid to conduct an inspection of data because the purpose of the inspection is to seize material evidence.

Therefore, the proponents of this trend propose to confront this legislative deficiency by explicitly stating the possibility of inspecting the intangible components of the computer, which is what French jurisprudence has tended towards, and the French legislator has amended the inspection texts by adding

the phrase (information data) to the text of Article 94 of the Code of Criminal Procedure, so that it becomes as follows: "The inspection shall be conducted in all places where objects or information data can be found, the discovery of which is useful for revealing the truth…"

In contrast, supporters of the second trend believe that programs and data are not originally material things, but they can be stored and recorded in specific material media or supports, so they are not purely moral things like ideas and rights, but rather things that have a tangible material entity, and therefore they are subject to traditional inspection procedures.

We find that what the supporters of the second trend went to, because not conducting inspection is an obstacle to the investigation process, and because of the importance of those components in revealing the ambiguity surrounding electronic crimes, especially since going with the first trend prevents the inspection of moral components, which forces the legislator to add special texts, or amend the current inspection texts, which leads to the inconsistency of the legislative system.

The second requirement

Information protection

Information protection or what is called civil protection means taking measures and procedures through electronic means that disrupt the process of infringement on electronic data or information, in addition to the possibility of accessing the identification of the perpetrator of these acts ([1]), and that work in state institutions depends on computers that are connected to each other through internal networks, and these internal networks are primarily connected to the Internet, and accordingly, the administration's data and information are circulated, and this in itself represents a danger to this information, its privacy and the confidentiality of some of it, and this matter requires providing an information protection system for this data, which achieves confidence and effectiveness in the administration system, and to provide security to this information and data specific to the computer system, it is necessary to protect it from forms of infringement, and this requires securing its confidentiality and privacy in addition to encrypting it, archiving it and making backup copies of it, and this is what we will discuss in this requirement, as we will divide this requirement into two branches, in the first branch we will discuss data encryption and ensuring its confidentiality, and in the second branch we will discuss data archiving and backing up, based on the above we will show the most important aspects of information protection for electronic data for the administration.

First section

Encryption and confidentiality of data

Encryption is the conversion of data from a readable form to an encrypted form that cannot be read or processed unless it is decrypted. Encryption is the basic building block of data security, especially in the case of data and information being exchanged between different management bodies in the form of decisions, orders or administrative contracts. It is the simplest and most important way to ensure that computer system information is not stolen or read by someone who wants to use it for any purpose.

Although private data is protected from theft and hacking, encryption also provides a means of proving that the information is original and comes from its original source. The basics of encryption revolve around the concept of encryption algorithms and keys, meaning that when information is sent, it is encrypted using an algorithm and can only be decrypted using the appropriate key. The key can be stored on the receiving system, or it can be sent with the encrypted data. A number of methods are used to encrypt and decrypt information, and these methods evolve with the continuous change of computer programs and methods of intercepting and stealing information. These methods include the symmetric encryption key, also known as the secret key algorithm, which is an individual method for decoding the message and must be given to the recipient before decoding the message. The key used for encoding is the

[1] Dr. Abdel Fattah Bayoumi Hegazy, The Electronic System of E-Government, Book Two: Criminal and Informational Protection of E-Government, Dar Al-Kotob Al-Qanuniyah, Cairo, 2007, p. 8.

same as the one used for decoding, which makes this method the best for the user. Otherwise, the key must be sent to the recipient, which increases the risk of being hacked if it is intercepted by an external party. This method is much faster than the asymmetric method, which uses two different keys, one public and the other private, linked together mathematically. The two keys are basically just large numbers that have been linked together. Together, but they are not identical, hence the name asymmetric, as the public key can be shared with anyone, but the private key must be kept secret, and the two keys can be used to encrypt a message, then the key that is different from the key that was originally used in the encryption is used to decode it. The draft law on information crimes for the year 2011 indicated that "Anyone who decrypts, removes or destroys the encryption of an electronic signature, computer devices, an information network or a card belonging to another person with the intent to commit a crime stipulated in this law shall be punished by imprisonment for a period not exceeding (3) three years and a fine of not less than (5,000,000) five million dinars and not more than (1,000,000) ten million dinars.

The second branch

Data copying and archiving

The reason for damage to computer components such as the hard disk carrying files, or the computer being exposed to theft or deliberate sabotage such as hacking by computer hackers, makes it difficult for the owner of the files to retrieve or recreate them, especially if they are large and important, or even bear the cost of losing them, so a backup copy of those files is made on external media such as a CD (DvD) or an external hard disk to avoid the consequences of losing files, and the process is repeated according to a strategy determined by the importance of the files, their size and the availability of external storage media, and backup programs are programs that create an additional copy of files or databases and computers in full, and these programs are used at a later time to restore the original contents in the event of data loss, and accordingly the official in the administration must take the necessary technical measures to make a backup copy of the information.

The electronic archiving system is one of the oldest traditional methods, as it can be activated by copying programs and referring to them when needed, and using electronic supports to ensure obtaining electronic data in the event of failure to operate any of the other supports, and working to carry out a daily transfer process outside the computer.

The components of a computer virus program are classified into main components:

1- Replication: It is one of the parts of the virus program that gives it the property of replication and spreading automatically.
2- Stealth: This part gives the computer program the property of secrecy, i.e. the inability to detect its presence easily.
3- Activation: This part of the virus has the property of being able to spread before it is detected and is usually within a specific time such as a specific hour or a specific date.
4- Execution: It is the task assigned to the virus to execute when it begins its activit.

Document Preservation Law No. 37 of 2016 referred to the archiving, documentation and registration of documents with natural or legal persons or those to whom possession is transferred later, provided that a copy of them is kept. The same law also referred to the importance of preserving documents of importance and belonging to the legislative, executive and judicial departments of the state, including bodies and entities not affiliated with a ministry. As for the draft law on information crimes of 2011, it referred to the backup copy of data "The competent judge may seize computer devices or part thereof or the medium in which the data was stored and transfer it to the investigation authority for analysis and study, and he may copy it without transferring the system and remove the data preventing access to the computer without harming the system or compromising the integrity of the data and programs stored in it."

Conclusion

After we have finished, thanks to Allah and His guidance, this research in which we discussed "The role of the administrative control authority in protecting the electronic data of the administration", we reached a set of results and recommendations as follows:

First: Results

1. Electronic administrative control is a modern means of administration to keep pace with scientific and technological development, after traditional means failed to confront electronic challenges.
2. The draft of the Information Crimes Law of 2011 did not stipulate any clear way to monitor or block websites.
3. In Iraq, there is no unified central agency whose mission is to follow up and combat electronic crimes, but there are several agencies linked to different security agencies that carry out the task of combating electronic crimes without any law regulating their work and defining their duties and limits.

Second: Recommendations

We call on the Iraqi legislator to adopt and explicitly stipulate the idea of electronic administrative control and define its powers and conditions of use, due to its great importance in maintaining public order with all its elements. We also recommend that the Iraqi legislator resort to the Egyptian Cybercrime Law No. 175 of 2018 when legislating the Iraqi Cybercrime Law, because it is a solid law and has defined the procedures for blocking electronic sites and the fixed legal periods for presenting the blocking decision to the administrative judiciary to take the appropriate decision to support or cancel the blocking decision, as well as amending the Criminal Procedure Code No. 23 of 1971, as amended, with a legal article that allows monitoring telephone and electronic communications during a specific period of time by a final judicial decision.

Reference :

First: Books

1. Abdul Qader Awda, Islamic Criminal Legislation Compared to Positive Law, 7th ed., Al-Risala Foundation for Publishing and Distribution, Beirut, no publication year, p. 5.
2. Dr. Abdul Hakim Dhnoon Younis Yousef Al-Ghazal, Criminal Protection of Individual Freedoms, 1st ed., Dar Al-Shu'un Al-Qanuniyah, Iraq, 2005, p. 98.
3. Ahmed Hossam Taha, Criminal Protection of Computers, a Comparative Study, Dar Al-Nahda Al-Arabiya, Cairo, 2000, p. 3.
4. Dr. Gamil Abdel Baqi Al-Sagheer, Criminal Protection of Magnetic Credit Cards, an Applied Study in French and Egyptian Judiciary, Dar Al-Nahda Al-Arabiya, Cairo, 1999, p. 7 and beyond.
5. Dr. Hossam El-Din Kamel Al-Ahwani, Protection of Intellectual Property Rights in the Field of the Internet, Cairo, 2005, p. 5.
6. Fouad Abdel Moneim, The Mediator in Private International Law, Part 1, Dar Al-Nahda Al-Arabiya, Cairo, 1977, pp. 49-50.
7. Osama Al-Majdoub, GAT, Egypt and the Arab Countries from Havana to Marrakesh, 1st ed., Dar Al-Masryah Al-Lubnaniyyah, Cairo, 1996, p. 150.
8. Abdel Fattah Bayoumi Hijazi, Electronic System of E-Government, Book Two, Criminal and Informational Protection of E-Government, Dar Al-Kotob Al-Qanuniyah, Cairo, 2007, p. 8.
9. Dr. Bashir Ali Baz, The Role of E-Government in Administrative Decision-Making and Electronic Voting, Ruh Al-Qanun Magazine, Faculty of Law, Tanta University, 2007, pp. 35-36.
10. Abdel Fattah Bayoumi Hijazi, Towards a General Formulation in the World of Crime and the Information Criminal, 1st ed., Dar Al-Fikr Al-Jami'i, Alexandria, 2009, p. 53.
11. Dr. Ayman Abdullah Fikry, Information Crimes, a Comparative Study in Arab and Foreign Legislation, 1st ed. Library of Law and Economics, Riyadh, 2014, p. 758.
12. Dr. Khaled Hassan Ahmed Lotfy, Electronic Litigation as an Information Judicial System between Theory and Practice, Dar Al Fikr Al Jami'i, Alexandria, 2020, p. 79.

13. Ahmed Khalifa Al Maqtat, Criminal Protection of Communications Technology, a Comparative Study, Dar Al Nahda Al Arabiya, Cairo, 2002, p. 525.

Second: Master's theses and dissertations

1- Abdul Azim Hamdan Aliwi, Criminal Protection of Animal Wealth, a Comparative Study, Master's Thesis, College of Law, University of Babylon, 2016, p. 28.
2- Shaza Hassan Abdul Zalzala, The Importance of Information in Building an Arab Development Strategy, PhD Thesis, Higher Institute for Political and International Studies, Al-Mustansiriya University, Baghdad 2005, p. 153.
3- Abdul Rahman Muhammad Al-Taf, Legal Protection of Digital Works in Light of Intellectual Property Agreements and Egyptian Law, Master's Thesis, League of Arab States, Arab Academy for Science, Technology and Maritime Transport, Institute of International Transport and Logistics, Cairo, 2010, p. 7.
4- Aisha Bin Qara Mustafa, The Validity of Electronic Evidence in Criminal Evidence, a Comparative Study, Master's Thesis Submitted to the Faculty of Law, Alexandria University, 2009, p. 49.
5- Maamish Zahia and Ghanem Nasima, Criminal Evidence in Cybercrimes, Master's Thesis submitted to the Faculty of Law and Political Science, Abdel Rahman Mira University - Bejaia -, 2013, p. 16.
6- Brahimi Jamal, Criminal Investigation in Electronic Crimes, PhD Thesis submitted to the Department of Law at the Faculty of Law and Political Science, Mouloud Mammeri University, Tizi Ouzou, 2018, p. 18.
7- Nagah Ahmed Abdel Wahab, Modern Development of Administrative Law under the E-Government System, PhD Thesis submitted to the Faculty of Law, Cairo University, 2011, pp. 181-182.

Third: Research and articles

1- Saif Alaa Hussein Al-Obaidi, The role of the Iraqi administration in combating cybercrimes that undermine public security, a research published in Al-Sada Journal for Legal and Political Studies, Algeria, Volume 4, Issue 3, 2020, pp. 32-33.
2- Imad Jawad Kazim, Munqith Abdul-Ridha Ali, Procedural protection of copyright in Iraqi legislation, a research published in the Journal of Legal Sciences, College of Law, University of Baghdad, Volume 32, Issue 1, 2017, p. 379.

Legislations

A- Laws

1- Iraqi Penal Code No. 111 of 1969 as amended.
2- US Penal Code of 1996.
3- Jordanian Information Systems Crimes Law No. 27 of 2015.
4- Kuwaiti Anti-Information Technology Crimes Law No. 63 of 2015.
5- French Penal Code of 1992.
6- UAE Anti-Information Technology Crimes Law No. 5 of 2012.
7- Saudi Anti-Information Crimes Law of 2007.
8- Egyptian Penal Code No. 38 of 1992.
9- Iraqi Copyright Law No. 3 of 1971.
10- Iraqi Criminal Procedure Code No. 23 of 1971 as amended.
11- Iraqi Electronic Signature Law No. 78 of 2012.
12- State and Public Sector Employees Discipline Law No. 14 of 1991 as amended.

B- Regulations and regulations

A- Decision No. 120 Criminal/2011 dated 4/28/2011, published in Al-Qada Al-Waqif newspaper, Issue 61, 2013, p. 6.