# Fighting the Information Forgery Crime in the Light of the Comparative Laws

**Dr. Moshtaq Talib Wahaib Alnaimi**

Mwahaib@yahoo.com

## Abstraction

Legislation may be often not enough for protecting information, and regulatory strategies are insufficient as well. Technical means are not also sufficient in preventing risks threating information whatever their effectiveness is. Thus, the protection is a complex structure consisting of law, regulation strategy and technology. The increasing use of and reliance on computer information systems has highlighted the need for good information system management. Legislative control can have a positive effect on this system by providing deterrence and increasing the public awareness of users about the problem.

Consequently, it is required looking for legislative means at the time in which the fight is more effective against this kind of criminality, and creating a safe environment and regulated according to legislations providing an acceptable amount of the protection of information circulated within the range of the technological society through making a comparative study of some legislations in order to establish a common ground if we want to find effectively legislative fight.


**Keywords**: Germany, Poland, Morocco, Oman, Iraq, Legislation, Information Crimes, Information Forgery Crime.

## Introduction

The legal agreements, undertaken between parties acting individually or acting as individuals, are governed by the civil and commercial laws: so, the rules setting the disputes are primarily subject to these agreements. Instead, the criminal code is always governed or based on two principles: the legality principle, which specifies that no crime and no punishment without law, and the non-analog principle in the

criminal texts. Therefore, any legal treatment for any act should be based on the balance between the two previous principles.[1]

Hence, the efforts are made to lay down a legal treatment based on the balance between these principles and the amount of interest, which require protection. In accordance with the penal code, a person cannot be punished unless there is a crime firstly. Then, there must be a law incriminating the act according to criteria proportionate to the size of the challenges encountering the law-maker; as well as, considering the nature of the continuously renewed environment in the field of electronic transactions.[2]

As it is well- known, the traditional laws were not written in the internet community,[3] i.e. they have been legislated at a time that the current technological services were not known and are accompanied by terms strange to these legislations. The concepts used in the previous texts have become unsuitable with the nature of the unsocial activities committed currently.

If the cyber laws are enacted, the criminals will be found guilty with their explicit acts according to the texts capable of dealing with these acts, and not according to the wide interpretations of the traditional texts, which are not capable of dealing with such acts and the concepts they involve.[4]

The dependence on the broad interpretation of the concepts of the texts will have no positive results in all cases. There will definitely be difficulties in applying these texts to the variables of modern technology. The modernization, therefore, of the currently used laws is required, where the failure in confronting the problems of

the modern techniques may result in a shadowy future, since they seriously influence the civil liberties.[5]

As well as, the modernization of the criminal laws may somehow contribute, to creating harmony among the legal rules of the world countries. This is necessary in facing the criminal activities, which transgress the boundaries of the countries whether on the substantive level or the procedural.

Additionally, the modernization is in some aspects suggested by some international efforts (which have been made in this respect), a matter which helps establish a unified legal environment between the world countries which is based on common grounds and proportionate criteria especially when the criminal laws across the world are different, because they reflect political, economic, historical, religious, social and cultural visions of that country.[6]

Such matter stands in the way of the efforts which seek to unify these bases which can only be accessed through[7]:-

1. The bilateral, regional, or international agreements.[8]
2. Recommendations of the regional and international organizations.[9]
3. The directions and models.[10]

Most countries of the world have recently started enacting the laws concerning the technology crimes including the computer-related crimes "information forgery".[11] But that does not deny the fact that the technological advance is quicker than the response of the foundations concerned of this danger.

So, it is a surprise that a lot of criminals seek a safe haven in countries, which have no cyber laws to incriminate such acts, to commit their crimes without being afraid of the legal pursuing and the deterrent punishments.[12]

The countries have taken two approaches in dealing with the unsocial activities resulted from abusing technology:

i. Some countries have tended to amend the existing laws, and have introduced modernizations to the texts of these laws via making the necessary amendments supported by the concepts capable of treating the diversity and development resulting from the nature of these techniques.[13]

ii. Some other countries[14] have tended to legislate new laws specialized in dealing with all the criminal activities resulting from the use of these techniques.[15]

In the last group, the laws of the countries have differed as to the treatment of the information forgery in its electronic form as follows:

1. Considering the information forgery as information fraud within the scope of computer-related crimes. Namely, that any change, or modification, or alteration of the information should be listed as information fraud crime or the so-called the computer-related fraud.[16]
2. Considering the information forgery an independent crime and should be addressed in a special text.[17]
3. Not addressing the information forgery crime, and confining to applying the texts concerning the other formation crimes.[18]

This will be shown through the analysis of the texts of some chosen laws in this context, so as to arrive to a comprehensive overview capable of drafting a typical text criminalizing the information forgery and the electronic documents. This means, in this context, we adopted a method of analysis and comparison between the texts of the laws that dealt with this crime in order to reach the desired aim.

On the other hand, the choice of laws from different countries helps to know the way in which these laws treated this crime, and benefiting from the texts of these laws to solve the problems arising from drafting an integrated text to confront this crime, let alone displaying the best drafting from among the laws proposed by these countries' legislators.

## The First Topic: The European Laws

### The First Requirement: Germany

The German Criminal Code of 1998 "Strafgesetzbuch (StGB)"[19] has confronted all the images of forgery crimes in the articles 267 – 282 in detail for most of the forgery cases.

Generally, what matters to us is how the German Criminal Code tackled the forgery, which takes place in the field of information and electronic documents. This law, under the title forgery of data intended to provide proof, showed that whosoever, for the purposes of deception in the legal commerce, stores or modifies data intended to provide proof in such a way that a counterfeit or falsified document would be created upon their retrieval, or uses data stored or modified in such a manner, shall be liable to imprisonment not exceeding 5 years or a fine.[20]

From above, it is made clear that the German law has incriminated the act of forgery, which takes place according to one of the specific acts, namely storage or modification. A matter, which denotes that the criminal conduct as one of the material elements "actus reus" of the forgery crime is done through the two specific acts mentioned above. That is to say, the other acts, which can be listed under the heading of forgery like inputting, changing or hiding the computer information or data,[21] according to the article above, are not considered a forgery crime, which requires a punishment.[22] It also appears that German Code does not refer to the forgery, which occurs with non-physical means, and the law seems to limit the forgery to the material means only.

On the other hand, it follows that the mental element - as one of the elements of which the forgery crime consists - represents the intent of deception in the legal commercial dealings. A matter, which means that any storage or modification of these data without the intent of deception in these dealings keeps the description of crime away from the act, because of the lack of its mental element which is the special criminal intent. The German Code views the influence in the processing of the data in the legal commerce as a forgery and equivalent to deception in the commercial transactions.[23]

Added to what is preceded, the German Code has set a condition that the data - which have been subjected to one of the acts forming the forgery crime - are intended to provide proof upon which a false document will be created. Namely, that the act will be a crime whenever a false document is established depending on the retrieval of the data which have been manipulated by the criminal. The

criminalization is also restricted to incriminating the data which is initially depended to issue the false and forged documents, that is, it does not include any manipulation of the data, which is entered into the document following its issuance or making. Consequently, it should consider this issue when encountering the criminalization of the acts, which constitute a forgery crime punishable.

It is noteworthy that the German law, within the scope of computer-related forgery, has criminalized the act of using the stored or modified data in such way mentioned before. The law here equals between the act of using the stored or modified data and the forgery which is represented under this article by modifying or storing the data which are adopted in creating a forged or false document. So, the law does not distinguish between the forgery crime and the crime of using the false document in terms of punishment in the field of manipulating the data in the electronic environment; despite they are different from each other. This position, in our opinion, comes to observe the danger of the two crimes and their interconnection.

The German Criminal Code has stressed the criminal responsibility of the offender for forging the computer-related data and decided the punishment from 6 months to 10 years imprisonment if: "

*1- The offender causes major financial losses.*[24]

*2- Endangers the security of the legal commerce through a large number of counterfeit or forged documents.*[25]

*3- Abuses his powers or position as a public official".*[26]

The German legislator increased the minimum punishment to one year when the offender would commit forgery on commercial basis or as a member of a gang whose purpose is to constantly commit the forgery crime, whereas the punishment will be the imprisonment from 6 months to 5 years for anyone who commits forgery in less serious cases.[27]

From what has been said, it follows that the German legislator has taken into account the amount and danger of forgery and size of the damage caused by this act on suiting the punishment to the offender. In this respect, we argue that considering the damage, which may result from the forgery and taking that into consideration when suiting the punishment to the criminal is an advisable thing, owing to the great damages caused by the forged information in the electronic field.

## The Second Requirement: Poland

Para 14 of Art 115 of the Polish Criminal Code of 1997 "Kodeks karny"[28] has defined the concept of document, which states:

*"A document is any object or other recorded information carrier to which is attached a specified right, or which, in connection with the subject of its content, constitutes evidence of a right, a legal relationship or a circumstance that may have legal significance".*

In accordance with this Art and Para (1) of Art 270[29], person who counterfeits, forges, alters or uses a document – according to the concept above – so as to use it as an authentic document, he will be punishable by fine and restricting liberty or imprisonment for a period ranging from 3 months to 5 years. Consequently, the

document could be considered an object of the forgery crime according to the concept and formulas mentioned above in the polish law.[30]

From above, it is understood that the Polish legislator- in Para 14 of Art 115 of the mentioned law- has expanded the scope of the concept of the document to include all the instruments in any form as long as it contains the information. Namely, this text includes any electronic carrier of the information,[31] which is related with the right or which, through association with its content, provides proof to the right or the legal relation or circumstances of great legal importance. Consequently, the forgery involves the content of the electronic and paper documents equally.

The aforesaid law has defined the nature of the material element of this crime and showed the criminal acts which are regarded as ways to change the correct information in a way that makes it contrary to the truth. Precisely, the methods of changing the truth in the forgery crime are represented by some acts, namely, forging, counterfeiting and altering document.

The definition of forgery, in our estimation, according to this article is not clear and adequate since the Polish legislator interpreted and defined the crime through the use of one of the terms – forgery, counterfeit – which basically need clarifying, i.e. he interpreted the crime as the forgery itself without defining the forgery crime which is represented by making the content of the document contrary to the truth. So, it may be useful in some aspect to use the terms such as changing, modifying, inputting, creating and suppressing and other criminal acts to which the other laws referred. But in the meanwhile, this drafting may support the required flexibility to cope with the development in the field of technology which may include any act or

conduct emerging in the future through adopting the broad interpretation of the forgery act (the material element) provided by the text mentioned. Moreover, the text above does not distinguish the forgery made by material means and the forgery made by nonmaterial means (i.e. forgery in the meaning).

The Polish legislator explicitly showed that the forgery crime is a deliberate crime, and referred to the special criminal intent through the expression "with the intention of using". This indicates that the criminal intent in this crime is the intention of using the forged documents as if they were authentic. This reference goes with the nature of the forgery crime because it is an intentional crime, which cannot be thought without a special criminal intent besides the general intent. But, according to what we have already gone into discussing the special criminal intent of this crime, the restricting of the special criminal intent to the intention of using the forged document may not be preferable in this context for the reasons already mentioned.[32]

The Polish legislator has adopted the approach adopted by some other laws,[33] which addressed the forgery crime of information and electronic documents, and equaled between the forgery crime and the crime of using the forged documents, and assimilated them in terms of responsibility and punishment.[34]

Moreover, the Polish law on dealing with the forgery crime does not clarify the issue of damage. The damage, which is explained is an influence produced by the process of forgery as a whole, and the above law does not refer to this issue and does not identify the nature of damage in relation to the forgery crime, whether it is an element or influence in this crime.[35]

Some of jurists,[36] under the Polish Penal Code of 1997, view that the crime of forging the computer documents ranges within the scope of fraud crime committed with the help of computer. Accordingly, the person who, for the purpose of getting a material benefit, or causing damage to another person, influences the automatic processing, collecting or transferring of the information, or changes, deletes or introduces a new record on an electronic information carrier without being authorized to do so, shall be punished by fine and restricting liberty or the penalty of deprivation of liberty for up to one year.[37]

## The Second Topic: The Asian Laws

### The Frist Requirement: Indonesia

Law of the republic of Indonesia number (11) of 2008 concerning electronic information and transactions[38] has treated this crime under article 35, which provides:

*"Any Person who knowingly and without authority or unlawfully manipulates, creates, alters, deletes, tampers with Electronic Information and/or Electronic Records with the intent that such Electronic Information and/or Electronic Records would seem to be authentic data".*

From the article already mentioned, it shows that the Indonesian law has identified the acts, which are listed under the criminal conduct of forgery Crime (manipulating, creating, altering, deleting and tampering). But it does not refer to the issue of suppressing the information and electronic records, which have been protected under this article. Consequently, every person commits one of these acts

shall be sentenced to imprisonment not exceeding 12 years and/or a fine not exceeding 12 billion rupiah.[39] Thus, the mentioned law has restricted the scope of punishment to the material forgery only without reference to the forgery, which occurs in the meaning.

Also the law has explicitly defined the nature of the forgery crime as a deliberate crime through the expression used *"knowingly",* in the sense that the offender commits this act knowingly. That agrees with the eroding where most laws treating this crime that emphasized that it is one of the intentional crimes.

It should be mentioned, despite that the Indonesian law has clarified the nature of this deliberate crime, but it did not clarify the special criminal intention, which most laws referred to. The law sufficed to show the purpose of forgery crime, that is, these electronic information and records seem as if they were original (correct). This may be regarded as an orientation to make the special criminal intent general to include all the criteria mentioned by a number of laws or jurisprudence. Seemingly, the intention of making the electronic information or records contrary to the truth may represent the special criminal intent. This alone constitutes a general criterion which may involve all what has already been mentioned- this is partly preferable- especially under the continuous technological developments which need adopting such a criterion in the current conditions.

Related to this, the law above does not refer the issue of damage in the forgery crime, and does not consider this issue neither in describing the damage and its nature in the forgery crime, nor the influence of this issue on estimating the punishment as some of laws did already mentioned.[40] Also the law did not

distinguish between whether the object of the forgery crime is information or electronic documents belonging to the public authorities or documents relevant to the activity of the private sector which have no official status.

## The Second Requirement: Philippines

The computer-related forgery crime has been treated under (Cybercrime Prevention Act of 2012).[41] The acts which are regarded as a legally punishable crime by punishment of *prison mayor* or a fine at least two hundred thousand pesos and up to a maximum amount commensurate to the damage incurred or both punishments,[42] for any person who is found guilty because: "

1- *The input, alteration, or deletion of any computer data without right resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic data, regardless whether or not the data is directly readable or intelligible.*[43]

2- *The act of knowingly usage of the computer data, which is the product of the computer-related forgery, for the purpose of perpetuating a fraudulent or dishonest design".*[44]

From above, it follows although the law above has treated the forgery in an independent text and identified the acts, which may constitute a computer-related forgery crime. There are some remarks about this law that we would like to present as follows:

- Restricting the acts which may constitute a forgery crime in three cases, namely inputting or changing or deleting without reference to the other cases which may lead to commit this crime like creating or suppressing

the data or information which form an electronic document later on, mentioned by some laws which have been reviewed. Consequently, the question here is: Does creating basically inauthentic data or hiding authentic information considers a legally punishable crime according to the law above when treating the forgery crime? Does the forgery constitute a punishable crime only when it is made by material ways not by non-material ways?

- Although the forgery crime is an intentional crime, the Philippine legislator does not explicitly clarify the nature of forgery crime, as well as, he does not define the special criminal intent in this crime. While he referred to this nature in another crime relevant to the forgery, which he treated at this point, that is, the crime of using the forged data knowingly, where he restricted the intention here to continuing the fraud project. The legislator at least should have clarified the purposefulness of the forgery crime in whole even when he did not state the nature of the intent peculiar to this crime, where he sufficed mentioning that it is done without any right.
- The legislator has equalled between two cases, each one constitutes an independent and self-contained crime. He equalled between the forgery crime and the crime of using the data or the forged documents in terms of treatment despite the differences between them in many respects.
- The law above neither reviews the issue of damage in the forgery crime, nor shows the importance of this subject in the computer-related forgery crime, except in the case of suiting the fine punishment to the criminal in a way proportionate to the amount of the damage done in this respect,

despite that most studies have referred to the amount of loses resulting from the processes of manipulating in the data of electronic systems, programs and devices besides the communication networks, especially under the attempts to electronize all the works of life in the present time in all sectors across the world.

- The legislator has focused on the result of the criminal conduct, which is represented by revealing data, which are inauthentic and contrary to the truth that are acted upon to realize the legal purposes.
- Not attaching any importance to the issue of the direct readability or understandability of the data that is an object of a forgery crime. The readability or understandability of these data has influence neither on their value nor on considering the act a crime or not. In other words, the acts to which the legislator referred will be considered a punishable crime whenever they are performed according to the form determined by the legislator, and whose subject are data which are understandable or readable even if indirectly. This orientation, which is adopted by the legislator, deserves a positive evaluation.
- This law does not consider the cases mentioned by some laws which have treated the crime of forging the information. For example, this law does not observe to aggravate the punishment in case that the object of the forgery crime is documents or data relevant to the state activities or the foundations charged with providing public services, or the banking and financial institutions.[45] Additionally, the law does not pay any attention or

intensify of the punishment in case that the criminal abused his job or position when committing the forgery crime.[46]

## The Third Topic: The Arabic Laws

### The Frist Requirement: Morocco

Morocco is classified as one of the countries, which took care of treating the information crimes under an existing law following modifications made to it to contain the technical developments in the field of crime.[47] The Moroccan legislator has added an independent chapter to the current criminal law according to which the law treated this new kind of the criminal activities.[48]

Under this addition, *it is a crime punishable by imprisonment from 1 to 5 years and by fine from 10.000 to 1.000.000 Moroccan Dirham without affecting the maximum criminal punishments, everyone who:*

1- *Forges or counterfeits information documents, whatever their form is, if that forgery or counterfeit may cause damage to others.*
2- *Uses information documents referred to above despite his knowledge that they are false or forged".*[49]

Through these provisions, the Moroccan law has addressed the process of forging the information documents using two general terms in criminalizing the act, which constitutes a forgery crime, namely "counterfeit, forgery", without reference to the other acts which falls within the scope of forgery crime. In other words, we argue that the law tried, through this drafting, to leave the text general as to involve any change or development which may occur in the technological environment,

especially it is continually renewed. The Moroccan law, therefore, did not define the nature of the forgery crime and the acts through which the criminal conduct occurs in the crime. It also follows that the law above does not distinguish between the material forgery and the non-material forgery, which takes place in the meaning. Despite the aforesaid characteristic of this drafting, the courts may interpret this drafting arbitrarily and this is not dangerous to some extent.

When treating the forgery crime within the scope of informative space, the Moroccan legislator did not show the criminal intent, which is one of the key elements in incriminating the acts, which make the information contrary to the truth in a way that causes damage to the others. The law above does not explicitly refer to the purposeful nature of this crime; as well as, this cannot be concluded from the context of the legal text which is originally free of that. So, it was advisable for the Moroccan legislator to mention that this crime, which occurs in the field of information, is a crime is committed intentionally and purpose fully, and this is a matter that most laws emphasized in this respect.[50]

On the other hand, the Moroccan legislator, in the context of his treatment of this crime, did not consider the relationship of the forgery object to the state organizations or the associations charged with a public service, and the case in which the offender in a forgery crime is a person abusing his position or job to commit the crime.

Realizing the danger of these crimes and the amount of damages which may be caused by these crimes in the present time, especially under globalization and the adoption of computer systems into all fields, the law referred, on treating this

crime, to the issue of damage without observing the nature, amount or kind of the damage which may be caused as a result of these criminal activities. But what it appears from the text mentioned that the Moroccan law stipulated that damage is done to others in order for the act is considered a punishable crime, and that is interpreted for making the damage one of the essential elements of the information forgery crime, and that goes against the logical and mental description of the position of damage in this crime as a resultant influence because it is one of the danger crimes which do not requires the occurrence of the actual damage.

Related to this, the Moroccan law does not deny the relationship of the forgery crime within the scope of information space to other crimes. So the law, when reviewing the legal treatment of this crime, also mentioned the crime of using the counterfeited or forged information, and decided the same punishment for both crimes in one text.

The Moroccan legislator should have allocated an independent text for this crime though being associated with the forgery crime, and whose subject is a result of forgery, this crime should be treated individually. The mentioning of the two crimes into a single text may confuse some specialists with the oneness of the crime and give an impression that the use is only an aspect of the conducts according to which the forgery is committed, and also the emphasis on the separation between the two crimes though they are interconnected.

## The Second Requirement: Oman

Oman has treated the modern technology crimes under a special law called the Cyber Crime Law issued by the royal decree no. 12-2011 in chapter four under

the title “Forgery and Information Fraud”, and specifically in Article 12 that incriminates the conducts of performing the information forgery. This Article provides:

*“The penalty with imprisonment for a period not less than one year and not exceeding three years and a fine not less than OMR one thousand and not exceeding OMR three thousands or by either penalty, shall be applied to any person who uses the information technology tools in the commission of information forgery crimes by changing the nature of such data or the electronic information by addition or deletion or replacement with the intent to use it as proper data or electronic information, acceptable in an information system legally a matter which might causes personal benefit to him or the other or causes damage to the other.*

*If such data or electronic information is governmental, then the penalty shall be temporary imprisonment for a period not less than three years and not exceeding fifteen years and a fine not less than OMR three thousands and not exceeding OMR fifty thousand. The same punishment provided for in the previous paragraph shall be applied mutatis mutandis to any person who knowingly uses the forged data or electronic information”.*

According to the article above, the Omani law required the change of truth for performing the information forgery that is replacing it by its contrary, without stipulating that this change includes all the data of the document, where the partial change in one of these data is sufficient. But the change of truth is to be concerned with the electronic information or data. The legislator also identified three actions “addition, deletion or replacement” in which the real content of the electronic

document is changed, and this is the core of forgery.[51] The legislator necessitated that the forged information or data be used as proper electronic information or data, which are legally accepted in the information system. But that should be done to achieve a personal benefit for the criminal or another one, or to cause damage to others whether materially or non- materially, and it may be a general damage caused to a collective interest, or a particular damage caused to a certain person.[52] This indicates that the focus is on the material acts, which change the truth without considering the change of truth which occurs in the meaning or with non-material means.

The law has emphasized that the information forgery crime is an intentional crime, which requires the presence of the criminal intent along with the material element, which is represented by the criminals' volition to commit the act although he knows that law prevents that. And this denotes the general criminal intent, which is not enough (in accordance with what is common in jurisprudence) for performing the forgery crime.[53] There must be a special criminal intent in this crime which is represented- according to this article specifically- by the intention of causing damage to the others, i.e. the criminal intends to damage the one targeted by the forgery crime, or the intention of getting an illegal benefit through changing the truth in the document, and this benefit belongs to the person who changed the truth, or belongs to others.[54]

It is remarkable that the punishment under the article above consists of imprisonment, which deprives the liberty and a financial punishment which is a fine. The amount of the punishment varies as follows:

- The punishment of the simple crime: The punishment is a period not less than a year and not exceeding 3 years imprisonment and a fine not less than thousand Rials and not exceeding 3000 Rials or one of these two punishments. This punishment applies to the forgery crimes whose object is ordinary documents, or belonging to ordinary persons having no particular status.
- The punishment of the aggravating crime: The Omani legislator aggravated this punishment when the object of the information forgery crime is the state information or data. In such a case, the punishment shall be a temporary imprisonment not less than 3 years and not exceeding 15 years and a fine not less than 3000 Rials and not exceeding 15 Rials.

In our opinion, the Omani legislator, in this article, although he rather treated this crime in an accepted way, it must be emphasized that the legislator overlooked the other cases of the criminal conduct which change the truth, and which are regarded as the essentials of the material element in the forgery crime. These cases are inputting, creating and suppressing. Consequently, the forgery crime is achieved by these cases in addition to the cases mentioned by the Omani legislator when the other elements of the crime are available. The Omani legislator also restricted the incrimination to the scope of forgery, which is done by the material means only.

Also, from the expressions contained in the article above, the use of the forged information or data as if they were correct and legally acceptable. It should be

emphasized that the intention of causing damage to the others is always among the influences resulting from this crime, and these influences may cause damage to the others negatively or may be positive achieving an advantage to the criminal or another person.

## The Third Requirement: Iraq

It seems that there is a step in the right direction realized by a draft law (act) concerned with treating the crimes related to the computer and information systems which is called the Information Technology Crimes Law Draft of 2010/ 2011. This draft of act has addressed this crime in the light of Article 8, which provides:

*"First- The penalty shall be temporary detention and a fine of not less than (10.000.000) ten millions ID and not exceeding (15.000.000) fifteen millions ID for whoever commits one of the following acts:*

a. *Forge, imitate, or create by himself or by another person a signature, deed, email, authentication certificate, or a license to practice e-signature services and the like, or intentionally used them illegally.*
b. *Forge, imitate, or create by himself or by another person in any form an electronic card or smart card or any means for transferring the local or foreign currency inside Iraq or using, circulating, or dealing with it while he knows that it is false.*
c. *Use or try to use fake or false electronic card while he knows that it is false, or accept to pay using the fake or false credit card while he knows that it is false.*

*d. Create intentionally to himself or to other person any false electronic data, documents, registers, or records, or make any change, manipulation or modification in any electronic deed, or use any of them before any public or private body.*

*e. Make for the purpose of sale, or any technical means to be used in forgery, counterfeiting, creating, or modification with intention of committing a felony or misdemeanor.*

*Second- The penalty shall be imprisonment for a term not less than (10) ten years and a fine of not less than (20.000.000) twenty millions ID and not exceeding (30.000.000) thirty millions ID if the acts defined in sub-article (first) of this article:*

*a. Relate to the rights of the state, the public sector, or the private entities with public benefit.*

*b. Commit by an officer or by a person in charge of public service during performing his job or because of it".*[55]

These solutions appear to acknowledge to the importance of the forgery crime, especially, when its object is information or data whose forms can be subsumed under the concept of the electronic document. It shall be taken here into account that the Iraqi law draft legislator of 2010 - 2011, has been treating such problems in detail through dealing with the act of forgery and the actions associated with it which sometimes constitute a crime legally punishable relevant to the electronic documents. Hence, the mentioned draft attempted to fight these acts as follows:

**First:** Forging the electronic written documents. The law draft tried to treat any action constitutes a forgery of a document or electronic writing that leads to change

its real content and contrary to the original truth. The draft incriminated the forgery act represented by manipulating or changing or modifying these data or information, which stand for the contents of the document.

This crime may be committed by making an electronic document, which never existed before and attributing it to somebody. This crime may take the form of imitating an electronic document as if it was a correct one, but it is a false document. Thus, the draft identified the ways, which lead to the commission of forgery, and make the information or data of the electronic documents contrary to the truth.

The draft stated items, which may constitute an object of a forgery crime as follows:

1- The signature, bond, writing, the certificate or license of practicing the services of electronic signature or what is associated with it.
2- The electronic or smart cards or any means, which is used to exchange the foreign or local currencies circulated inside Iraq.
3- The data, documents, records, or electronic registers which are used in dealing with a private or public body.

It is remarkable that the criminal result under discussion, namely the change of truth is represented by making the data, information, electronic document or register contrary to the fact which the concerned parties meant in the document. Precisely, the data or information contained in the electronic document is contrary to the fact which the concerned parties meant under the law or reality.

The draft in treating this crime did not focus on the nature of the material element of this crime, which is represented by the truth change which constitutes the criminal result- as an element in the material element, but once in the clause (D) of Para (1) of Art (8) "false". A matter, which requires to call the attention of those who are concerned to respecting the nature of forgery particularly in the change of truth, i.e. (focusing that the data or information of the document are contrary to the truth). Provided that the object of changing the truth "the data or information of the document" is essential, having influence on the change of the legal effects resulting from this document. Namely, the change of truth should have an influence on the legal value of the electronic document and threaten the legal statuses of the individuals.

In addition, the forgery crime will not be complete once the occurrence of material acts making up the material element of this crime unless this is associated with the criminal intent. Since the crime here is an intentional crime, no person can be blamed or be held answerable unless he has a criminal intent, where he did not intend to perform the acts constituting the material element for the purpose of achieving a certain end. The criminal intent, in its general sense, is realized when the criminal knows that he changes incorrect data or information to seem as if they were correct, yet he wants to accomplish the material elements of the crime.[56]

Through reviewing the previous texts in their current from, it appears that they explicitly referred to the intentional nature of the crime. However, they did not mention the identification of the special criminal intent, which they came free of. We believe that it is better to determine the special intent to the illegal intention of

the criminal, through which the availability of the criminal's criminal intent can be deduced as one of the key factors of the forgery crime. It should be emphasized that the estimation and interpretation of this intention shall be an effective criterion subject to the judge's estimation and interpretation according to the circumstances of each case. A matter, which can expand the capacity of the legal system to absorb any updates resulting from the modern technologies. Consequently, this criterion will be comprehensive of all the interpretations of the special criminal intent which jurisprudence and the concerned laws, old and modern, referred to as the intention of using the document or the intention of causing damage to others or the intention of deception or fraud…etc.[57] So, we prefer to put the phrase (intentionally and illegally) to the preface of the article (8) which involves all the paragraphs so that the text will be as follows *"whoever commits intentionally and illegally one of the following acts".*

These texts are devoid of referring to the damage in the forgery crime, unlike the current Iraqi Penal Code.[58] Although the current form did not refer to the damage resulting from the forgery, it may be advisable in our estimation, since a wording like this supports our view that the damage is an influence produced by the forgery crime, and cannot under any circumstance, be described as an element of the material element or mental element, not a condition for the punishment or an independent element in this crime. What emphasized this is that there is a direction not to relate the criminalization of the crime to the concept of damage. There is a direction to criminalizing the act of forgery even if there is no certain damage resultant. Precisely speaking, the damage in all the cases of forgery crime is an assumed influence, i.e. the forgery, in all the cases, causes the damage,

even if that damage is not incurred on a specific person, it is incurred on the society. Consequently, the public's trust in the document will be weakened including the documents and information in their electronic from. This denotes that the occurrence of forgery crime is possible even if the damage is probable or may be peculiar to a specific person or the whole society.

This direction, therefore, helps to remove the obstacles which may be placed by some in punishing the forgery, especially, if we used one of the previous descriptions of damage, then it will be an obstacle to incriminating the acts which produce the forgery committed against the electronic documents which may not lead to an immediate damage, but a future or probable damage. Especially, when it is taken for granted that the damages, resultant from these acts in this electronic environment, are great cannot be estimated at a certain figure in certain times. The crime of forging the electronic documents, which is characterized by difficulty in proving, can be easily proved at the same time. As a result, there will be no outlet for the criminals to get away with the punishment, when convicted, under the pretext that there is no damage.

**Second:** using the forged electronic documents. The previous article laid stress on important issues relevant to the forgery crime including the use of the electronic documents according to the forms mentioned by this article. It appears that there is an emphasis on incriminating the use of the forged electronic documents provided that this use is deliberate and illegitimate. This is an expected thing, since there is an interconnection between the forgery crime and the crime of using the forged

documents, and the danger of forgery appears at the time when these documents are used in the everyday transactions.

The draft treated the issue of using the forged electronic documents by the criminal who committed the forgery crime, and that means that the offender is the same in both crimes. The user may be a person different from the offender in the first crime, so, the second person will be convicted of using the forged documents.

On the other hand, the draft allocated a ruling in which it treated the case of a person who accepts forged electronic documents when used by the criminal in the crime of using forged electronic documents. This is clearly shown when he accepts the fake paying card or forged despite that he knows that the card is incorrect. Consequently, he shall be punished by the same punishment imposed on the person who uses this card.

This ruling, in our estimation, is advisable to stop the criminals who evade the punishment under the pretext that he did not use the false or forged card in person. It also incriminated the attempt of using the forged documents or electronic cards in spite of his knowledge that these cards are false or forged. This ruling applies even to the rest of the electronic documents which are used in dealing with a private or public body.

**Third:** Making or possessing technological means used in committing the forgery crime. The draft has treated other acts relevant to the forgery crime, especially, that these acts are catalysts for committing a crime or misdemeanor (the forgery crime in all its forms). The clause E of the paragraph 1 of the article 8 of the draft has incriminated everyone who made or possessed, for the sake of selling,

distributing or displaying; programs, devices, data or any technological means which are used in forging or imitating or modifying with a view of committing a felony or misdemeanor.

In fact, the text in its current drafting meets with an obstacle, that is, the freedom of trade or economic activity practice. Under this drafting, is it possible (reasonable) to punish the person who deals with these items, taking into consideration that all the programs or technological devices have two sides in use: positive and negative (criminal). This means, all these items are used in social activities, and meanwhile are used for criminal purposes as in the forgery process, which may be a felony or a misdemeanor according to the circumstances. So, in accordance with this article, every person dealing with these items shall be punished even if he is good-willed, and cannot know that the offender who took these items will use them in committing a criminal act.[59]

So, we argue that this matter should be respected in drafting the paragraph, through adopting a certain criterion under which the incrimination is restricted to dealing with the materials, devices, programs, or any technological tool which can be exclusively used in the criminal purposes including the forgery crime, or at least the punishment or incrimination is restricted to the scope within which these tools, items, programs or means are really used in committing the crime, or they will be used by the criminal in committing the crime, or may have known that they would be used in illegal action.[60] So that an innocent human being will not be punished who does his activities according to the principles of the freedom of economic activity.

Hence, this point is preferable to be drafted as follows: *"manufactured or possessed with a view to selling, distributing or displaying programs, devices, data or any technological means despite his knowledge that they will be exclusively used, or have been used, or they will be used in forging, making, imitating, modifying with the intention of committing a felony or misdemeanor"*.

**Fourth:** The punishment: The article above punished everyone who commits one of the acts already referred to by a temporary imprisonment and a fine not less than 10.000.000 Iraqi Dinars and not exceeding 15.000.000 Iraqi Dinars. The draft aggravated the punishment to be an imprisonment not less than 10 years and a fine not exceeding 30.000.000 Iraqi Dinars if the acts, specified in the paragraph (1) of this article, are relevant to the rights of the state or the public sector or the private bodies authorized with public interest. Or they are committed by a civil servant during his duty or because of it. With the last paragraph, the draft distinguished between the punishment of the electronic document forgery which is associated with the rights of the state or the public sector or the private bodies authorized with public interest, or if these acts are committed by a state employee during his duty or because of it (i.e. considering the character of the criminal in this case). This indicates that there is a desire to support the trust in the documents issued by that civil servant, also the desire to protect the rights of the state and the public or private institutions when performing a job for the public interest. That means, the aggravation of the punishment came to protect the rights of the state which are generally related to the interests of the public, i.e. considering the character of the victim; while the aggravation in the second paragraph came to consider the character of the criminal who is supposed to be trustworthy in performing his duty, this matter is advisable in the draft.

The draft is not limited to these punishments, but specifies additional punishments when it allowed the court under the Article 29 to confiscate or destroy the devices or programs used in committing the crime without affecting the rights of the others good-willed.[61]

Finally, it must be said that despite the detailed treatment of the matters arising from or accompanying the forgery crime in the Article 8 and the paragraphs included within, it may be sometimes unnecessary. Especially, that the legislator of the draft expanded the concept of document under Para 13 of Article 1, which defined the electronic document as follow:

*"A Letter containing information, which is created, merged, saved or transmitted in whole or in part by electronic, digital, optical or any other similar means"*[62].

As well as the definition of information included in the paragraph 12 of the same article that provides:

*"Data, texts, images, shapes, sounds, codes, database, computer programs and the like which are created, saved, processed or sent by electronic means"*[63].

Consequently, it is better to treat all the cases of forgery, which are committed against the electronic documents, whatever their form may be, in a unified text with effective concepts and bases capable of absorbing all those cases in the present time or in the future. There is also an exaggeration in estimating the punishments of this crime and the crimes included or associated with it in a way that triggered the ire of the organizations and supporters of human rights,[64] where there is some right logic in some part of their defense.[65]

## Conclusion

Most countries pay attention to this phenomenon due to their awareness of the dangers associated with modern technologies and their applications in everyday life. There are always bad intentions and illegitimate use to achieve illegal purposes. This fact has made many countries adopt a unified attitude against criminal actions. This attitude is represented by enacting the necessary laws to combat electronic crime. However, the approach to the criminal characteristics and modalities of forging alternatives or counterparts differ from one country to another. According to the method of treatments, countries are classified into two categories:

- The first one prefers to criminalize this act by introducing the necessary amendments or improvements to the provisions of existing laws and to be adequate to cope with the evolution in the concepts of forgery as in Germany, Poland and Morocco.
- The second category (Indonesia, the Philippines and Oman) prefers to criminalize newly developed crimes within the scope of these techniques by enacting new independent laws applied to them including information and computer-related forgery, since this type of crimes has characteristics which distinguishes it from traditional crimes previously known. The current laws cannot treat the problems associated with technology, even if some amendments are made. Therefore, it is better to find new formulas to deal with this growing threat. Iraq follows the second approach.

Countries differ in determining the actions that constitute the crime of forgery, which are punishable by law. In other words, the countries – subject of the

comparison – differ in determining the material element and the acts, which constitute the behaviors through which forgery is committed. This shows that there is really a desire among countries to combat this crime. There are also many definitions to determine these various acts. All this confirms the expansion aiming to accommodate any new behaviors through which the crime may be executed.

There is almost a consensus among the laws of those states that this crime is intentional, even in light of the technological developments introduced in the execution of the crime. There is a confirmation that this crime is executed with full knowledge and awareness of the actor who knows from the very beginning that s/he is violating law, nevertheless, he\she insists on executing forgery to reach the intended result.

Imposed punishments are restricted to the criminalization of the act, which constitutes a crime by a financial penalty (which is a fine) and punishment as restriction or deprivation of liberty. However, there is a difference among the texts of laws in different countries concerning the estimation of the amount of the penalty. These differences of course stem from the different points of view of legislators in estimating the seriousness of the crime, which reflect the social, economic and political philosophy of the system followed in each country.

Most of the countries covered by the comparison do not differentiate, in the treatment of crime of forgery, between the subjects of crime whether concerning the activities of official institutions or private sector institutions. Namely, these

countries do not attach importance to the subject of the crime of forgery whether it is information or electronic documents concerning the state or private sectors.

At the end of this research we suggest to make a comparison between the texts of the Iraqi draft law related to information crimes and the texts of international conventions, guidelines and directives made in this respect, and every crime of information crimes.

We call at the same time to studying the way of harmonizing texts of the Iraqi draft law to the laws of other countries that have enacted laws concerned with anti-information crimes, whether on the procedural or substantive level.

## Footnotes

[1] Younis Arab, *"Laws and Legislations Concerning the Internet in the Arab Countries,"* (Working paper submitted to the conference and exhibition of the international and Arabic banking technologies, Union of Arab Banks, Jordan - Amman, held from 28-29/10/2002), p. 3.

[2] In this meaning: Sulaiman Ahmed Fadl, *Legislative and Security Addressing of Crimes Arising from the Use of the International Information Network (Internet)* (Cairo: Dar Al Nahda Al-Arabia, 2007), p. 412.

[3] Stein Schjolberg, "The History of Global Harmonization on Cybercrime Legislation: The Road to Geneva," December, 2008, available at: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf. (05/02/2011), p. 1.

[4] Stein Schjolberg, op. cit., p. 1; in this context see as well, ESCWA Cyber Legislations Directives: Regional Harmonization of Cyber Legislations to Promote the Knowledge Society in the Arab World. Beirut: 2012, available at: http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf. (13/09/2012). ( مشروع تنسيق الاسكوا. ارشادات الاسكوا للتشريعات السيبرانية: التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية. بيروت، ٢٠١٢), p. 117.

[5] In the same meaning: Aleš Završnik, *"Towards an Overregulated Cyberspace: Criminal Law Perspective,"* Masaryk University Journal of Law and Technology: Iss. 2/10, p. 174, available at: http://mujlt.law.muni.cz/view.php?cisloclanku=2010120003. (05/03/2013).

[6] Accordingly, we will see later the differences in drafting the laws, which deal with these crimes.

[7] In this meaning also see: Stein Schjolberg, op. cit., p. 1.

[8] See for example the Council of Europe Convention on Cybercrime 'Budapest – 2001'.

[9] For example, UNCITRIAL model laws on Electronic Commerce and also on Electronic Signature. Commonwealth Model Laws on Computer and Computer-related Crime (2002).

[10] For example, ESCWA's efforts for making directives helping Member States in order to enact the legislation specializing in this field. See: The ESCWA *Cyber Legislations Directives* and the UAE Guiding Law to fight information technology crimes and related crimes.

[11] The legislations, which we are going to display later – when making a comparison among them- are a proof on states' desire to regulate and to incriminate the acts resulting from abusing modern technologies.

[12] Michela Menting Yoell, *Research on Legislation in Data Privacy, Security and the Prevention of Cybercrime* (First Printing, Geneva: International Telecommunication Union, 2006), p. 107.

[13] See for instance, penal legislations of Germany, Poland and Morocco. These legislations will be later discussed.

[14] See for instance, legislation of Indonesia, Philippine, Oman. They will be later discussed.

[15] Rizgar Mohammed Kadir, *"The Scope and the Nature of Computer Crimes Statutes – A Critical Comparative Study,"* Germany Law Journal: Vol. 11 No. 1, June 2010, p. 625, available at: https://www.germanlawjournal.com/. (10/01/2014).

[16] Note the Jordan Law Draft on Information Systems Crimes of 2009 in Para 1 of Art 9. It is available at: http://www.lob.jo/List_FeedBack_Public.aspx?ID=182&Type=1. (01/11/2011).

[17] Note the legislations which we are going to examine later.

[18] See for example, Unauthorized Computer Access Law of Japan no 128 of 1999. And Arts 214 and 215 of the Criminal Code of Lithuania no VIII-1968.

[19] Its translation is available at: http://www.gesetze-im-internet.de/englisch_stgb/index.html. (22/01/2013).

[20] See: Para 1 of Art 269 of the German Criminal Code.

[21] We think that the Germany legislator used these terms in other cases of the forgery crime, see for example Para 1 of Art 273 concerning tampering with official identity documents, which provides: *"Whosoever for the purpose of deception in legal commerce*
*1. removes, renders unrecognisable, covers up or suppresses an entry in an official identity document or removes a single page from an official identity document or……), and Para 1 of Art 274 which provides: (Whosoever*
*1. destroys, damages or suppresses a document or a technical record which does not belong to him or not exclusively to him with the intent of causing damage to another;*
*2. deletes, suppresses, renders unusable or alters legally relevant data (section 202a(2)), which are not or not exclusively at his disposal, with the intent of causing damage to another; or*
*3. takes away, destroys, renders unrecognisable, moves or falsely places a border stone or another sign intended as a designation of a border or water level with the intent of causing damage to another, shall be liable to imprisonment not exceeding five years or a fine".*

[22] Lorenzo Picotti and Ivan Salvadori, "*within the framework of the Project on Cybercrime of the Council of Europe, Economic Crime Division and Directorate General of Human Rights and Legal Affairs"*, Strasbourg – France, 28 August 2008, p. 29, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf. (19/02/2013).

[23] See: section 270 of the German Criminal Code.

[24] See: Para 3 of section 269, which refers to Para 3 of section 267 after mutatis mutandis; in this context see: Para 2 of Art 223.A of the Criminal Code of the Republic of Croatia No. 110 of October 21, 1997 (entered into force on January 1, 1998), which provides: *"If the criminal offense referred to in paragraph 1 of this Article is committed in connection with the computer data or programs of a governmental body, a public institution or a company of particular public interest, or if significant damage is caused, the perpetrator shall be punished by imprisonment for three months to five years".*

[25] See: Para 3 of section 269, which refers to Para 3 of section 267 after mutatis mutandis.

[26] See: Para 3 of section 269, which refers to Para 3 of section 267 after mutatis mutandis.

[27] See: Para 3 of section 269, which refers to Para 4 of section 267 after mutatis mutandis.

[28] Its translation is available at: https://www.imolin.org/doc/amlid/Poland_Penal_Code1.pdf. (23/10/2012).

[29] This Para provides: *"Anyone who forges, counterfeits or alters a document with the intention of using it as authentic, or who uses such a document as authentic, is liable to a fine, the restriction of liberty or imprisonment for between three months to five years".*

[30] A side of doctrine sees that in the new Polish Penal Code of 1997 the crime of the forgery of computer documents falls within the range of computer-aided fraud as stated in section 287. Note in this context: Grzegorz Kopczyński and Maciej Szostak, *"The Notion of The Document in The Polish Penal Code Of 1997,"* "Dokumento sąvoka 1997 m. Lenkijos baudžiamajame kodekse," *Jurisprudencija*, 2000, t. 18(10), p. 144, available at: https://www.mruni.eu/lt/mokslo_darbai/jurisprudencija/archyvas/?l=103771. (10/03/2013).

[31] Andrzj Adamski, *"Cybercrime Legislation in Poland",* Nicolaus Copernicus University, Torun – Poland, pp.16-17, available at: http://www.cybercrime.umk.pl/files/files/Cybercrime%20Legislation%20_PL_2010.pdf. (01/03/2015).

[32] For more information about the views, which has been said in the aspect of defining the special criminal intent, and what view, which is suitable before the reality of such crime, please see, Moshtaq Talib Wahaib, *"Information Forgery as One of the Information Crimes in the Light of the Iraqi Law"*, University of Szczecin - Faculty of Law and Administration, Poland, Doctor Dissertation, 2015, (II) of chapter three of the dissertation, p. 74.

[33] The Arabic text of Art 298 of the Iraqi Penal Code states:

(يعاقب بنفس العقوبة المقررة لجريمة التزوير – بحسب الاحوال – من استعمل المحرر المزور مع علمه بتزويره).

This text is translated: *"Any person who uses a forged document knowingly, according to circumstances, shall be punished by the punishment prescribed for the offence of forgery"*; as well as, see: chapter (607-7) of Morocco Criminal Code that will be examined later; Arts 267, 268 and 269 of the German Criminal Code, which have been already mentioned.

[34] Look once again at: Para 1 of Art 270 of the Criminal Code of Poland.

[35] More about the damage and its nature please see Dr. Moshtaq Talib Wahaib Alnaimi, *"Information Forgery as One of the Information Crimes: Comparative Study"*, Al-Halabi Legal Publications, Lebanon, Beirut, 1st Edition, 2018 p. ٣٢٣,

د. مشتاق طالب وهيب النعيمي، *"تزوير المعلومات كأحد صور الجرائم المعلوماتية: دراسة مقارنة"*، مشنورات الحلبي الحقوقية، لبنان، بيروت، الطبعة الاولى، ٢٠١٨.

[36] See: Grzegorz Kopczyński and Maciej Szostak, op. cit., p. 144.

[37] See: Art 287 of the Criminal Code of Poland.

[38] Its translation is available at: http://www.bu.edu/bucflp/laws/law-no-11-concerning-electronic-information-and-transactions/. (23/01/2014).

[39] See: Para 1 of Art 51of Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions.

[40] In this aspect we have seen the German Criminal Code in Para 3 of section 269, which refers to Para 3 of section 267 of the German Criminal Code after mutatis mutandis; and Para 2 of Art 223.A of the Criminal Code of the Republic of Croatia No. 110 of October 21, 1997.

[41] It is available at: http://www.senate.gov.ph/lisdata/111349486!.pdf. (22/09/2012).

[42] See: Section 8 of Cybercrime Prevention Act 2012 of Republic of Philippines.

[43] See: (i/1/B) of Art 4 of Cybercrime Prevention Act 2012 of Republic of Philippines.

[44] See in this context: (i/1/B) of Art 4 of Cybercrime Prevention Act 2012 of Republic of Philippines.

[45] Please see: Art 4 of the Federal Law of UAE No. 2 of 2006 on the Prevention of Information Technology Crimes.

[46] Please see: Para 3 of section 269 of the German Criminal Code, which has been previously said.

[47] This is the Penal Code of 1962, and its translation in the French language is available at: http://www.wipo.int/wipolex/en/text.jsp?file_id=190447. (21/01/2013).

[48] The Moroccan legislator has added the tenth chapter to the Penal Code, under tittle (Infringement of the automatic process systems of data) by the law no 03.07 for (Tetmim) completion of the penal code concerning the automatic process systems-related crimes issued by Dahir Shareef no 1.03.197 in (16/Ramadan/1424) 11/11/2003.

[49] See: section (607-7) of Morocco Criminal Code.

[50] It should be said here; one of the legislations, addressing the information forgery crime in the field of electronic systems, communication networks and any other device, which do not refer to the intentional nature of the forgery crime, is The Federal Law of UAE No (2) of 2006 on The Prevention of Information Technology Crimes that came free of this element, in Art 4.

[51] Mustafa Blassey, *"Features of the Cybercrimes Law (3-5)," a* series of analytic essays published by *Oman Daily*, available at: http://omandaily.om/?p=194033. (13/04/2015).

[52] Hussein Saeed Al-Ghafri, *"Legal Views on Fighting the Information Technology Crimes,"* Oman Daily, Monday 07/05/2012, an analytical essay was published on the former website of *Oman Daily*, available at: http://www.main.omandaily.om/node/94898. (22/10/2012).

[53] Please see the jurisprudential dispute about the nature of the special criminal intent in the forgery crime, which we have mentioned by Moshtaq Talib Wahaib, Dissertation, op. cit., p. 192.

[54] Hussein Saeed Al-Ghafri, op. cit., (N. Pa).

[55] The Arabic text of this Art provides:

(اولا: يعاقب بالسجن المؤقت وبغرامة لا تقل عن (١٠,٠٠٠,٠٠٠) عشرة ملايين دينار ولا تزيد على (١٥,٠٠٠,٠٠٠) خمسة عشر مليون دينار كل من ارتكب احد الافعال الاتية:

أ- زور او قلد او اصطنع بنفسه او بواسطة غيره توقيعا او سندا او كتابة الكترونية او شهادة تصديق او الترخيص بمزاولة خدمات التوقيع الالكتروني وما في حكمها او استعملها عمدا بشكل غير مشروع.

ب- زور او قلد او اصطنع بنفسه او باسطة غيره بأي شكل من الاشكال بطاقة الكترونية او ذكية او أية وسيلة تستخدم في تحويل النقود المحلية او الاجنبية المتداولة داخل العراق او استخدامها او روج لها او تعامل بها وهو يعلم بعدم صحتها.

ج- استعمل او حاول استعمال البطاقة الالكترونية المقلدة او المزورة مع علمه بذلك ، او قبل الدفع ببطاقة الوفاء المقلدة او المزورة مع علمه بذلك.

د- اصطنع عمداً لنفسه او لغيره بيانات او وثائق او سجلات او قيود الكترونية غير حقيقة او احدث اي تغيير او تلاعب او تحوير في اي سند الكتروني او استعمل ايا منها امام اية جهة عامة او خاصة .

ثانياً: تكون العقوبة السجن مدة لا تقل عن ١٠ عشرة سنوات وبغرامة لا تقل عن (٢٠,٠٠٠,٠٠٠) عشرين مليون دينار ولاتزيد على (٣٠,٠٠٠,٠٠٠) ثلاثين مليون دينار اذا كانت احد الافعال المنصوص عليها في البند (اولا) من هذه المادة:

أ- تتلق بحقوق الدولة او القطاع العام او الجهات الخاصة ذات النفع العام .

ب- ارتكب من موظف او مكلف بخدمة عامة اثناء تأدية وظيفته او بسببها).

[56] For more details about the concept of criminal intention, please see: Moshtaq Talib Wahaib, Dissertation, op. cit., p. 188.

[57] For that reason, it can be said; what most of the said legislations have required in the special criminal intent, it is just one of forms of the illegal intent's concept.

[58] On the discussion, which has taken place about the nature of the damage in the forgery crime, please see Dr. Moshtaq Talib Wahaib Alnaimi, Comparative study, op. cit., p. 323.

[59] See in this context: Art 4 of chapter 33 of the Criminal Code of Finland; and Para 4 of Art 3 of the Portugal Cybercrime Law no 209/2009.

[60] It is worth mentioning in this aspect, that we find Art (607/10) of Morocco Criminal Code which punishes these acts if these materials (items) are exclusively prepared to be used for commission of such crimes. Namely, it has limited the scope of criminalization to the exclusive preparation of these items to commit the crime only.

[61] In this aspect we find most of the previously mentioned legislations have stated these supplementary punishments, for instance, see: Art 32 of the Cyber Crime Law of Oman; Art (607/11) of the Moroccan Criminal Code.

[62] The Arabic text of this Para provides:

(المحرر الالكتروني: رسالة تتضمن معلومات تنشأ او تدمج او تخزن او ترسل او تستقبل كلياً او جزئياً بوسيلة الكترونية او رقمية او ضوئية او بأية وسيلة مشابهة).

[63] The Arabic text of this Para provides:

(المعلومات: البيانات والنصوص والصور والاشكال والاصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك التي تنشأ او تخزن او تعالج او ترسل بالوسائل الالكترونية).

[64] Note about these criticisms, which have been mentioned by some of organizations such as Human Rights Watch. Please see: http://www.hrw.org/ar/node/108738/section/2. (10/10/2013).

[65] It is noteworthy; this Law draft has been not passed, because it has been stopped according to request of the media and culture commission in the Iraqi Parliament no. 27/Lam Tha Aeen in 22/01/2013.

**Bibliography:**


1. Aleš Završnik, *"Towards an Overregulated Cyberspace: Criminal Law Perspective*," *Masaryk University Journal of Law and Technology*: Iss. 2/10, p. 174, available at: http://mujlt.law.muni.cz/view.php?cisloclanku=2010120003. (05/03/2013).
2. Andrzj Adamski, *"Cybercrime Legislation in Poland", Nicolaus Copernicus University*, Torun – Poland, available at: http://www.cybercrime.umk.pl/files/files/Cybercrime%20Legislation%20_PL_2010.pdf. (01/03/2015).
3. Commonwealth Model Laws on Computer and Computer-related Crime (2002)
4. Criminal Code of Lithuania no VIII-1968
5. Cybercrime Prevention Act 2012 of Republic of Philippines
6. ESCWA, *Cyber Legislations Directives: Regional Harmonization of Cyber Legislations to Promote the Knowledge Society in the Arab World*. Beirut: 2012, available at: http://isper.escwa.un.org/Portals/0/Cyber%20Legislation/Regional%20Harmonisation%20Project/Directives/Directives-Full.pdf. (13/09/2012). (الاسكوا. *ارشادات الاسكوا للتشريعات السيبرانية: مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية*. بيروت، ٢٠١٢)
7. Grzegorz Kopczyński and Maciej Szostak, *"The Notion of The Document in The Polish Penal Code Of 1997," "Dokumento sąvoka 1997 m. Lenkijos*

*baudžiamajame kodekse," Jurisprudencija*, 2000, t. 18(10), available at: https://www.mruni.eu/lt/mokslo_darbai/jurisprudencija/archyvas/?l=103771. (10/03/2013).

8. Hussein Saeed Al-Ghafri, *"Legal Views on Fighting the Information Technology Crimes"*, Oman Daily, Monday 07/05/2012, an analytical essay was published on the former website of *Oman Daily*, available at: http://www.main.omandaily.om/node/94898. (22/10/2012)

حسين سعيد الغافري، *"رؤى قانونية حول مكافحة جرائم تقنية المعلومات"*، الاثنين/ ٠٧ مايو ٢٠١٢ ، مقال تحليلي نشر على الموقع السابق لصحيفة عُمان.

9. Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions

10. Lorenzo Picotti and Ivan Salvadori, *"within the framework of the Project on Cybercrime of the Council of Europe, Economic Crime Division and Directorate General of Human Rights and Legal Affairs",* Strasbourg – France, 28 August 2008, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf. (19/02/2013)

11. Michela Menting Yoell, *Research on Legislation in Data Privacy, Security and the Prevention of Cybercrime* (First Printing, Geneva: International Telecommunication Union, 2006)

12. Morocco Criminal Code

13. Moshtaq Talib Wahaib, *"Information Forgery as One of the Information Crimes in the Light of the Iraqi Law"*, University of Szczecin Faculty of Law and Administration, Doctor Dissertation, 2015.

14. Dr. Moshtaq Talib Wahaib Alnaimi, *"Information Forgery as One of the Information Crimes: Comparative Study",* Al-Halabi Legal Publications, Lebanon, Beirut, 1st Edition, 2018 د. مشتاق طالب وهيب النعيمي، *"تزوير المعلومات كأحد صور الجرائم المعلوماتية: دراسة مقارنة"*، مشنورات الحلبي الحقوقية، لبنان، بيروت، الطبعة الاولى، ٢٠١٨.

15. Mustafa Blassey, *"Features of the Cybercrimes Law (3-5)", a* series of analytic essays published by *Oman Daily,* available at: http://omandaily.om/?p=194033. (13/04/2015)

مصطفى بلاسي، *"ملامح قانون مكافحة جرائم تقنية المعلومات (٣-٥)."* سلسلة مقالات تحليلة نشرت في صحفية عُمان متاح على الموقع اعلاه).

16. Rizgar Mohammed Kadir, *"The Scope and the Nature of Computer Crimes Statutes – A Critical Comparative Study", Germany Law Journal*: Vol. 11 No. 1, June 2010, available at: https://www.germanlawjournal.com/. (10/01/2014)

17. Stein Schjolberg, *"The History of Global Harmonization on Cybercrime Legislation: The Road to Geneva"*, December, 2008, available at: http://www.cybercrimelaw.net/documents/cybercrime_history.pdf. (05/02/2011)

18. Sulaiman Ahmed Fadl, "*Legislative and Security Addressing of Crimes Arising from the Use of the International Information Network (Internet),* (Cairo: Dar Al Nahda Al-Arabia, 2007). فضل، سليمان احمد. *الموجهة التشريعية*

*والامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية – الانترنت*. القاهرة: دار النهضة العربية ، ٢٠٠٧).

19. The Council of Europe Convention on Cybercrime 'Budapest – 2001

20. The Criminal Code of Finland

21. The Criminal Code of the Republic of Croatia No. 110 of October 21, 1997

22. The Federal Law of UAE No. 2 of 2006 on the Prevention of Information Technology Crimes

23. The German Criminal Code

24. The Iraqi Penal Code

25. The Jordan Law Draft on Information Systems Crimes of 2009

26. The Penal Code of the French 1962

27. The Polish Criminal Code of 1997 "Kodeks karny"

28. The Portugal Cybercrime Law no 209/2009

29. The UAE Guiding Law to fight information technology crimes and related crimes

30. Unauthorized Computer Access Law of Japan no 128 of 1999

31. UNCITRIAL model laws on Electronic Commerce and also on Electronic Signature

32. Younis Arab, *"Laws and Legislations Concerning the Internet in the Arab Countries",* (Working paper submitted to the conference and exhibition of the international and Arabic banking technologies, Union of Arab Banks, Jordan – Amman, held from 28-29/10/2002)

يونس عرب ، *"التعاقد والدفع الالكتروني تحديات النظامين الضريبي والكمركي."* ورقة عمل مقدمة الى ندوة متخصصة حول التجارة الالكترونية – معهد التدريب والإصلاح القانوني ، الخرطوم ، كانون الأول ٢٠٠٢ ، ص ١ – ٢٠) .