Legal Form of Cyber Fraud Crime in the Jordanian and Comparative Legislation

Dr. Ibtisam Saleh
Dr. Hanan Al Daher
Assistant Professor
Amman Arab University

Dr. Mohamed Qudah
Associate Professor
Al- Ahliyya Amman University

Abstract

This paper addresses the legal form of a cyber fraud crime in the Jordanian and comparative legislation. The Jordanian legislator restricts the object of criminal protection to funds and overlooks, despite technology advancement and information revolution, protecting information funds from fraudulent seizure. There is a special provision in the Cybercrime Law, which is stated in general terms, that stipulates punishment of any person who commits a crime stated in any law if committed by technical means, by the penalty set in this Law. However, it does not cover data and information as an object of fraud. In order to achieve the envisaged objectives of the study, this study has initially looked into the object of cyber fraud to indicate whether information and data serve as an object of traditional fraud crime. The computer and IT fraud was then examined, and the legislation and jurisprudence perspective vis-a-vis this crime was illustrated. The material element of the cyber fraud crime was demonstrated next. This paper tackles cyber fraud means set forth in comparative legislation. It demonstrates the special nature of delivery in cyber fraud, as well as delivery by means of information systems. It concludes that data and information do not fit for physical delivery required by the legislator in the traditional fraud crime and that that there is a need for the legislator to intervene and deal with cyber fraud through an explicit provision.

Introduction

Crime is a social phenomenon that reflects reality, reacts with its variables, and responds to its developments. One of the most important and most useful inventions of the twentieth century is the emergence of computers, which have been accompanied by a revolution in information technology. It has led to the emergence of unusual criminal phenomena, including crimes committed through the use of computer systems and components, especially the internet. Therefore, the computer in these crimes acts as a tool in the hands of the offender, and it is used as he wishes to achieve many criminal and illicit purposes. Therefore, in these cases, the information crime does not exist through the computer or one of its components, but through the use of information systems and networks in order to achieve criminal ends. Perhaps the most prominent criminal act committed over the computer and its components is cyber fraud.

Cyber fraud crimes, in which data or information acts as the object of committing the crime or the means of committing it, are new forms of crime that are associated with scientific progress. In these crimes, the purpose of the offender is either to seize the information and the data itself because information has a financial value or to obtain data and information through fraud to obtain a financial value, e.g. access to documents of a financial value. While traditional fraud is seizure by the offender of money owned by others with the intention of its acquisition without the consent of the victim, cyber fraud creates many problems that have been addressed by jurisprudence. This includes the validity of information and data to be considered as an object of fraud and the possibility of fraud on computer and the information system, in addition to the special nature of delivery in cyber fraud. According to the above, this study will be divided into two sections as follows.

Section I: The Object of Cyber Fraud Crime

The Jordanian lawmaker has addressed the fraud crime in Article 417 of the Penal Law, which provides that**:1-** "Whoever makes another person deliver to him any moveable or immoveable property or any documents which include an undertaking or discharge, and takes control of this property or document by means of deception:

(a) through the use of fraudulent means that makes the victim falsely believe in the existence of a false project, incident, or matter, or raise the victim's hopes to gain profit or retrieve the amount of money taken by fraud, or the existence of a false debenture or forged discharge instrument, or (b) through the disposition of a moveable or immoveable property, while knowing that he has no right to do so, or (c) through the use of a false name or character, shall be punished by imprisonment ranging from three months to three years and a fine ranging from one hundred to two hundred Jordanian Dinars." By review of this provision, it is evident that the lawmaker does not define the fraud crime but only identifies the legal form of this crime, in terms of the items to which it is related and through the three forms of the material element of the crime. This is the same approach adopted by many Arab legislations such as the Syrian and Lebanese laws.

On the other hand, there are many legislations that have defined crime, e.g., Article 231 of the Kuwaiti Penal Law, as every fraudulent act by which the offender intends to bring a person to commit an unlawful act or maintain the unlawful act that he committed to force him to deliver a property in his possession and leads to submitting the property to the offender or to any other party. Fraud can be committed orally, in writing, or by sign.

As for criminal jurisprudence, fraud has been defined to be the seizure of money owned by another person by deceit and leading him to hand over his own money. It is, therefore, a crime in which the right to property is attacked. .[1] Electronic fraud has been defined by some as an intentional manipulation of information and data representing material values stored by the computer, unauthorized entry of correct information and data, tampering with instructions governing programming, or any other means that may affect the computer in order to obtain an illegal profit and to harm others.[2]

Division I: The Validity of Data and Information as an Object of Traditional Fraud

According to the Jordanian legislator's plan in Article 417, the fraud object is a property of a material nature owned by others. It is not fraudulent to use fraudulent means to obtain a benefit, even if it is evaluated for money. This property should be valuable. The absence of this value denies the thing the nature of money. The value of this money does not matter whether it is material or moral.[3] In terms of the nature of the money, Article 417 defines it as a movable property, real estate, or bonds that include an undertaking or discharge of any financial obligation or commercial papers. The question that has raised a legal dispute has centered around the validity of data and information as an object of fraud.

Branch I: Definition of Data and Information

Data are the inputs of the information system; some have defined it as "a set of facts that reflect certain attitudes and actions that have occurred in the past, present, or future, be it words, numbers, forms, or symbols."[4]Information is data analyzed and interpreted to increase the knowledge of decision makers and help them achieve specific goals and enable them to wisely judge phenomena and observations. In fact, there is a difference between data and information. Information is data processed; data is not yet processed, so the age, date of birth, study, or social status of a person is data, but when they are listed in a special form, they become information because they indicate the person's condition. Data are inputs, *i.e.*, raw or primary data that relate to a particular sector or activity. Information is the output, that is, the output of the data. It is organized and processed in a way that allows for the extraction of results. Therefore, computer systems are said to be information systems rather than data systems.[5] Despite the difference between information and data and that information is more important than data, this does not mean that data is not important because it is the source of information, so it is as important as information and both have the same legal protection. In Article 2 of the Cybercrimes Act, the Jordanian legislator defines data as figures, letters, symbols, shapes, sounds, images or drawings that are not self-explanatory. Information is defined as the data that have been processed and thus have become significant.

Branch II: The Extent to Which Data and Information are Considered as Money

There is no dispute over the validity of the programs and data to be the object of fraud if they contain a material support, considering that the latter is the object of this crime because of its physical nature. There has been a dispute between traditional and modern jurisprudence about the extent to which data and information are considered money. Money, from the traditional point of view, is only for the material things, which were most numerous in the past and the non-material things were few, so the definition of money in relation to money crimes was that everything material could be the object of a financial right. That is to say, the material things that are considered as money are things that are possess able.

Thus, the information that is presumed to be equivalent to a moral object is outside the scope of funds and is not fit to be money unless it is linked to materiality, that is, it must be registered on supports or discs. In addition, data and information cannot be described as movable because law requires that the movable money be of a visible financial tangible nature and information is not.[6] However, technical development, especially in the field of computers and the resulting emergence of new moral things, does not stop developing, so the economic value of these things has increased. This has prompted the modern jurisprudence to recognize data and information as money because it is of economic value and because they are put on market to start like any commodity and have a commercial market subject to market rules.[7]

This information is issued by its owner, *i.e.*, linked to his personality; it is he who thought of it, which means that it is close rights to the personality of the owner, and this information itself is the object of this right, and one of its characteristics is transition because transition is of its nature. This means that there is another party who receives information, be one or several people. Therefore, information and data are a mental energy, which accepts ownership and transfer, and it does move only with the approval of its holder. This approval is shown by the code number or secret number, which is the key that holds or releases it according to the will of the holder. This is not a departure from the principle of the legality of crimes and punishments.[8]

Branch III: Extent of Validity of Information and Data as an object ofFraud

From legislations that have expressly provided for the validity of information and data as an object of the crime of fraud, the Syrian legislator, in Article 21 / A of the law on the organization of communication on the network and the combat against electronic crime No. 17 of 2012, has punished those who seized, through the use of computers and network, movable money or real estate or information or programs of financial value or a bond that includes an undertaking, discharge or other financial privilege by deceiving the victim or deceiving an information system under the control of the victim by any means.

As for the validity of information and data to be the object of traditional fraud if it is independent of the physical support it contains, there are two trends. The first trend sees the lack of validity of data and computer information to be the object of this crime. Their argument is that there is no concrete physical activity in which receipt and delivery in the crime of fraud occur. Even if such delivery and receipt are assumed, they do not deprive the victim of possession of such programs and data that remain under his control concerning transfer and possession. This, though consistent with the nature of information and programs, does not conform to the nature of criminal activity in the crime of fraud.[9] The second trend, which is more acceptable, sees information as the object of a potential fraud because data and information are of the newly created financial values and thus can be the object of the crime of fraud as stipulated in Article 336/1 (Egyptian Penalties) as these texts give only examples of the object of this crime without requiring that the object be material or moral.[10]

The question that arises is whether data and information are money and an object of fraud according to the plan of the Jordanian legislator. It was argued that information and data are not money, since electronic data and information cannot be an object of the property right unless they are protected by intellectual property legislation. Even if data and information were protected by such legislations, aggression against them would form special crimes; thus, they cannot be an object of a fraud crime.[11]

Others believe that information and datacome under the description of money for several reasons. First, the texts related to money crimes did not define the meaning of money. However, the explanatory note to the Civil Law and the scope of clarification of Articles 53-54 concerning the definition of money has pointed out that there are two conditions for a thing to be money. The first condition is its use and it is recognized that the condition of the use of moral funds is available. The second condition is possession, whether material or moral, and the first form is achieved if the possession is material, and material is the tangible thing, so the components of the computer are money. The moral possession is if the owned is moral, *i.e.,* by its release from the owner and attribution to him, such as literary and artistic work. Therefore, data and information are considered money as long as they are possible to acquire morally and to benefit from them. Data and information have an innovative economic value, so they can serve as an object of fraud.[12]The researchers supports this jurisprudential direction.

Division II: Fraud on the Information System

The victim of the crime of fraud is the one who was deceived by the offender and who handed over his money, whether he is a natural or moral person. Corporations and public and private institutions are legal persons.

Since the computer and the internal networks of the enterprise constitute a branch of the institution, they are valid for the act of deception. But can fraud be practiced on a computer?

Branch I: Legislative Trends on the Extent of the Possibility of Leading a CC Computer into Error

The first Trend: Some Arab laws require that the offender has deceived another person like him, such as Article 417 (Jordanian Penalties), "whoever deludes others". This is the position of the Syrian legislator in Article 641 of Penalties and Article 366 of Egyptian Penalties, using the words "using fraudulent methods that deceive people." Therefore, the legislations which stipulate that fraud should occur on a natural person do not envisage deceiving the computer.[13]

The Second Trend: There are some legislations, such as those in the Anglo-Saxon countries, including Britain, Australia and Canada, the texts of which are more comprehensive and can be applied to the crime of electronic fraud. The First Article of the British Theft of 1978 punishes those who fraudulently obtained illegally a benefit from others. The English legislator has incriminated the computer fraud after having ratified the Computer Abuse Act of 1990.[14] Among the Arab legislations that have dealt with fraud on the information system is the Syrian legislation in Article21 /A of the Law on Organizing Communication on the Net and Combating Electronic Crime in Syria, which used the words: "by deceiving the victim or deceiving an information system under the control of the victim by any means."

Branch II: Position of Jurisprudence on This Issue

According to some jurisprudence, the crime of fraud does not occur if computer data and information systems are manipulated in order to seize money because for such crimes to occur, the offender and the victim must be natural persons. A person who is deceived must be in charge of monitoring the data and ,therefore, it is not imagined accordingly to deceive the information system as a machine, and the criminal text of fraud cannot be applied here due to the missing of an essential element.[15]

On the other hand, others believe that the deception of the information system to steal the money of others is achieved by fraudulent methods such as a lie supported by material works or external facts, where, in addition to lying, an external incident is available supported by the presentation or submission of documents or information that enters the computer.[16] French jurisprudence in favor of this opinion has been affected by the French judiciary, where the French Court of Cassation applied the penalty of fraud to a person who entered his car to the parking place and instead of placing the original money required for parking, he put useless pieces of metal, which operated the machine. The Court of Bordeaux ruled that the crime of fraud occurred if the accused person withdrew cash money from another person's account using the ATM card of that person or paid for his purchases using another person's card.[17] According to another opinion, the basic criterion for fraud is the fraudulent tactics, which are technical methods used by the offender during the operation of the device, which are the availability of technical expertise in deception of the information system through obtaining the identity card and assuming the character of its owner for replacing him in electronic operations and extracting information documents and results of automated operations.[18]

The position of the Jordanian jurisprudence on this issue is that the victim must be a human being because these crimes require a human mind that deceives the owner through tricks after an operation that did not reveal falsehood. Therefore, these crimes are called crimes of reason, and the computer is not similar to the human mind because the electronic mind either accepts or rejects, since its process is a physical operation, but the human mind does a rational process of a moral nature during which it reflects and thinks before rejection or acceptance. The researcher is in line with this jurisprudential trend because Article 417(Penalties) explicitly provides that the victim must be a natural person, and saying otherwise is expansion in criminalization.

In reference to the Jordanian judiciary, the illegal use of the ATM cards is considered a theft crime by the decision of the Amman Court of Appeal: "Where our court finds that the depositors and others have photocopied the ATM cards and confidential information of a number of customers while they are withdrawing via ATM, and then unloading such information on cards and reusing them to withdraw money from the account of the complainants without the element of illusion or falsity and without realizing the fraudulent methods since the offender in the crime of fraud can seize the money, transferred or not transferred, with the consent of the owner through cheating and fraud, which distinguishes the crime of fraud from the crime of theft. In fraud, the transfer of money from the victim to the offender occurs with his consent, although consent based on cheating is incorrect, while in theft the offender takes the money of the victim without his consent even if he knows it.

Since it is established in this case that the complainants did not give their money to the appellants who seized the funds without the consent of the owners of those funds, the consequent actions of the appellants in this case constitute all elements of the crime of theft contrary to Article 406 and in accordance with Article 76 of the Penal Code. Thus, we decide to amend the description of the offense assigned to the appellants as fraud in partnership contrary to Articles 417 and 76 of the Penal Code to the offense of theft in partnership contrary to Articles 406 and 76."[19]

Section II: The Physical Element of the Electronic Fraud Crime

In Article 15 of the Cybercrime Act, our legislator punishes anyone who committed an offense punishable under any applicable legislation using the Internet or any information system or website with the penalty provided in that legislation. Therefore, there is no legal obstacle to the use of computer and information systems as a means to commit the crime of traditional fraud, such as the offender's promoting for his fraudulent project through the Internet, which is an external manifestation supporting his lying.

There are much legislation that have criminalized fraud through the Internet or by means of information technology, including the Qatari Law of Combating Cybercrime No. 14 of 2014 in Article 11/2, Federal Law No. 2 of 2006 against IT crimes in Article 10, and the Kuwaiti Law No. 63 of 2015 in Article 3/5. It is noted that these legislations do not require that the purpose of fraudulent methods is those matters specified exclusively in Article 417 of the Penal Code. They are deceiving the victim with the existence of a false projector accident or creating a false hope to obtain a profit or the payment of the amount taken by way of fraud and support the illusion that there is a false bond or false quittance. Those legislations have focused on deceiving others without showing specific objectives.

Division I: Electronic Fraud Methods in accordance with the Comparatively Legislation
BranchI: Electronic Fraudulent Methods

In Article 417, the Jordanian legislator does not define fraudulent methods because any legal definition cannot cover all fraudulent methods, as they evolve with technical and technological progress. The Court of Cassation has defined it as "any lie accompanied by external facts or material acts that would make the victim believe the lie so as to lead him to hand over what he hasvoluntarily."[20] However, jurisprudence has defined fraud as any lying supported by external manifestations or physical acts leading the victim to illusions as specified by Law.

Fraud is based on cheating and cheating is based on lying, which is changing the truth by making a false incident in the form of a true incident, in order to inflict the victim in error to make him deliver his money, as a false doctrine leads to the truthfulness of a lie, but lying alone is not suitable for deceit and fraud on the victim, even if the offender exaggerates in his lying.These are some fraud methods in informatics framework.

First: Preparing Material Facts or External Manifestations

The information criminal must have a great deal of knowledge of computer technology, its systems and programs, and how to employ them to reach a result or have a place to practice fraud including a number of parts of computers, a set of screens, discs, hard discs, tapes, cables, fax, telephone, and a number of employees who understand the language of dialogue in this field. Or he uses any of the counterfeit cards or works at one of the famous computer companies or computer maintenance companies and other countless features which have made scholars include many such incidents under fraudulent methods.[21]

One of the Internet frauds is the e-mail fraud, where the victim is contacted through e-mail without any prior contact with him. The victim's address is not a specific address, but it is open so that the addressee is *undisclosed _recipents@yahoo.com*. One of the tricks is sending an e-mail to all the Internet users who have e-mail boxes which receive "Congratulations, you have earned $ 100,000 from a lottery company,"which randomly selects winners through the Internet and asks everyone to provide his bank account number, bank name, telephone number and beneficiary's name in case of death. The victim immediately provides them with what they asked for. The sender then confirms the profit by asking for a copy of his personal identity and his credit card number for the purpose of transferring a cash amount to him.

There are two criteria that determine the extent of illusion that must be available in order for fraudulent methods to be deceptive. First, there is the objective criterion under which fraudulent methods are to be so well prepared that they can deceive the average person with the minimum of care and caution.

If the offender succeeds in deluding the victim because of good skills, it means that the crime has been carried out, but if he is too naïve to deceive that person, the victim cannot be deceived. The second is the personal criterion, which determines the degree of illusion based on the personality of the victim and his intelligence, so that the lies supported by external manifestations are sufficient for the fraudulent methods to deceive the person whether or not they deceive others who are more intelligent than the victim is. This is the criterion adopted by our Jordanian legislator in Article 417 of the Penal Code. It uses the term "using fraud methods to deceive the victim" and the provisions of a number of special legislations dealing with cybercrime such as those in the Syrian Law.

Second: The Use of a Third Person to Support the False Claim

The use of another person to support the offender's claims and lies happens a lot in practical life, as it confers on the perpetrator's allegations a color of truth and makes the victim be fooled by false claims.

The offender must be the one who has arranged this means of deceiving the victim by bringing another person to support his lies under prior agreement. If that person has supported the lie of the offender on his own without prior agreement, the crime of fraud is no longer in place. It is also required that the support be issued by the same person and not a repetition of the lies of the offender or be a mere agent or a deputy of the offender transferring what he commissioned him to deliver to others. A person may have the good faith, but the offender uses him to carry out his crime. However, the crime remains when the elements of the perpetrator exist. The person mayhavea bad intention and colluded with the offender. Here he is a partner in the crime of fraud.[22] In the framework of informatics, the offender who claims to be the maintenance representative of a well-known company may be able to have access to the competing company's information systems to work with a third person to support the validity of his claims by taking possession of any of the maintenance tools of wires, cables, several screwdrivers, and other tools.

Third: Exploitation of the Offender of His True Character

Lying is not enough by itself to rise to the level of fraudulent methods, but lying or deception by a person who has a certain degree of confidence from people may generate confidence by the victim. This character must be true and not so different from the case of fraud by means of impersonation of the offender of an untrue identity. This method of fraudulent methods is often due to the type of work carried out by the offender and his connection to the nature of the field in which he exercises his tricks and actions, which leads to the difficulty of discovery and facilitates accepting them. An example of this is that a computer system analyst could use this role to facilitate his entry to the headquarters of any company to perform an untrue task and then manipulate their information systems or penetrate their own network to obtain data and information or manipulate them in order to obtain a benefit. Thus, we find that the character of the offender as a system analyst supports his lies and facilitates his entry to the headquarters of the company and then his fraud on the information system.[23]

Branch II: Taking a False Name or an Incorrect Character

The pseudonym is the non-real name, whether that name is attributed to a real person or a fictitious person and whether this designation includes the whole name or only a part of it such as a parent or family name. It is not required that the offender resorts to other fraudulent methods to commit the crime. Once a pseudonym is used, he has committed this crime provided that the false name would generate deception and mislead the victim to hand over his money. If the doer has a known name that is different from the name stated in the birth certificate and he is presented in this name to the victim, he is not considered to have committed the crime of fraud because the nickname is a real name and not a false name. The incorrect character was not defined by the Jordanian legislator in Article 417 of the Penal Code. However, the most correct thing is that it is defined as the prestige enjoyed by a person in the community by virtue of his birth, family relations, qualifications or work in a particular job, profession, craft or legal work. Through the definition of jurisprudence, it turns out that the incorrect character impersonated by the doer confers on him a special position in the eyes of others, who accept to deal with him with confidence as a result of this prestige, which leads to deliver to him the money of others, so it must be that the false character can meet the victim's need.[24]

The offender's taking a false name or an incorrect character is the most common means in the framework of informatics, since the offender deliberately impersonates others or adopts a false character in order to manipulate the data in order to achieve his desires. In addition, there is a variety of technical means used by the information criminal operating the device due to the special nature of the crime of e-fraud where the technical expertise of the offender is available to obtain the identity of other people and their status to replace them in electronic operations and to obtain the extracts and results of automatic processing of data.[25]

One practical application was the case of Thompson, a British subject who worked as a programmer at a Kuwaiti bank in 1948. He had designed his own program and was able to manipulate data related to the bank by transferring parts of customer accounts to a fictitious account that he had created for that purpose. He had suspended the transfer and left to work in Britain. He had already traveled to his country and sent a letter to the bank manager requesting the transfer of his entitlements, but he had been discovered and was tried by English courts.

Division II: The Delivery of Money in Electronic Fraud

Branch I: Extent of Validity of Information and Data for Possession by the Offender in accordance with Traditional Texts

The seizure of the property of others is the result aimed at by the offender. This is explicitly stipulated by the Jordanian legislator in Article 417 of the Penal Codes as well as the Lebanese legislator in Article 655 Penalties. This is what we can also see in the context of Article 336 (Egyptian Penalties) by saying "seizure". The victim is not required to hand over his money directly to the offender. The delivery may be made by a person who has received a direct order from the victim. It is not required that money is directly delivered to the offender, but delivery may go to a person working under the offender. However, if the other person is aware of the criminal intention and shares fraudulent roles with him, then he is a partner in the fraud. The intention of the victim to transfer the possession to the offender is pointless as to whether the transfer of possession is temporary or permanent or casual. The crime is committed once the money has been received by the offender in an intention to seize it. Thus, we find that the Jordanian legislator explicitly stipulates in the crime of fraud to have a physical activity in which delivery and seizure are made, *i.e.*, that delivery is hand to hand by the victim or someone else. The offender must have a physical possession of the money, which would also entail physical seizure by the offender. Accordingly, data and information are not suitable for the criminal activity of the crime of fraud in accordance with Article 417 Penalties.

Branch II: Delivery by Information Systems

There is no doubt that the nature of the delivered thing in informatics faces difficulties where penal legislations require that delivery be of material and movable objects. Thus, there was a legal dispute over the extent of the fraud crime if delivery was through information systems. The view was that the takeover resulting from fraud on the computer does not raise any problem if the object of seizure was money or any movable thing of a material value such as the manipulation of data entered or stored in the computer or its programs by someone so that the computer, in his name or in the name of his partners, would issue checks or invoices of undue amounts seized by the offender only or shared with his partners.[26]

According to another view, in many cases of information fraud, the victim contributes to the success of the fraudulent process, without being aware of the fraudulent means or the harmful effect it entails. In this case, the accused person will be punished for the crime of fraud rather than theft. The theft disappears if the victim surrenders the money to the offender for full possession regardless of whether delivery was made due to the victim's fault or not.[27]

But does the physical seizure of electronic money occur if the perpetrator manipulates the data stored in the computer to transfer the balances or benefits of others to his own account? Is this a takeover of money or not?

It is conceivable that someone manipulates the computer data in order to transfer some of the assets or benefits of others to his own account using fraudulent methods, which has prompted many state legislators to explicitly state the validity of electronic money to be the object of money crimes, despite their non-material nature. In the United States, several laws have been enacted to define money as "everything that represents a value." It is a definition that includes material or bank money.

Some legislations do not consider written money as material money, but as a debt, which is impossible to be a fraud object, such as the French legislation.[28] The French judiciary has invented the theory of equivalent delivery, which was adopted by the Court of Cassation in several rulings, which ruled that the payment made by a written entry is equivalent to the delivery of money.[29]"Material delivery is realized for crimes arising from the use of the computer as a positive tool. The victim of fake data pays the value of the invoices to the offender through money, which is a material transfer, or through a check.

Some believe that the solution decided by the French Court of Cassation can be applied in the case of interference with programming or data introduced to the computer which leads to the cancellation of the debt and rather burdening the account with undue creditor amounts whether the offender detained the transfer order to some person and then falsified it in his own name to be paid in his own account or he manipulated the program. Therefore, fund transfer from one account to another can be in writing without fund delivery to the offender.[30]The French Court of Cassation in its aforementioned decision considered the discharge of the payment of the fee, when the offender deposited a false coin instead of the required original money, as replacing material delivery although the offender did not receive anything material. The Court of Doual also applied the punishment of cheating on the person who placed a worthless piece of metal in a public telephone in order to phone others without paying the value of the call.[31]Thus, we find that the meaning of delivery in the crime of electronic fraud has a special indication different from the traditional meaning, where it often takes a special form that distinguishes it.

There is no doubt that the introduction of the equivalent of material delivery is a measure that finds its basis in the similarity that exists between the facts and, thus, runs counter to the principle of legality of crimes and penalties.

Conclusions

The spread of information technology and technological development has played a role in the emergence of new forms of fraud, where the object of the crime of fraud is a movable property owned by others. This has raised questions about the suitability of traditional texts to information money. Is the text of Article 15 of the Cybercrime Act sufficient to address this crime? After the researcher has finished the study we have found the following results:

1. The Jordanian legislator does not explicitly mention that data and information are money; thus, the matter has become controversial. The proponents of the traditional principle believe that information has a special nature and cannot be considered as money and cannot be the object of the traditional crime of fraud, whereas the proponents of modern concepts regard it as money of a financial value.
2. According to the Jordanian legislator's plan, fraud requires the delusion of the victim, who must be a human being, so one cannot imagine a fraud on a computer because this would be expansion of criminalization, which violates the principle of legality.
3. The delivery of money is the legal result in the crime of fraud, and it is a purely physical behavior, and this element is clear in its significance and does not accept the extension of its significance to data and information. Therefore, they are not subject to the criminal activity of fraud according to the Jordanian legislator's plan.
4. The positions of comparative legislations that have dealt with e-fraud have shown differences. Some of them have explicitly adopted the validity of data and information as an object of fraud, while some others have not addressed the subject, but they instead criminalized the fraud of seizing money through the information network or using the means of information technology.
5. It should be noted that the text of Article 15 of the Cybercrime Law can be subdued to cover the use of the computer or the information network to carry out the traditional crime of fraud.

Recommendations

1. The researcher wishes the amendment of the legal text that defines money so that money becomes "everything that has a financial value".
2. It is desirable if the Jordanian legislator introduces a special provision in the Electronic Crimes Law that deals with the crime of electronic fraud to include data and information as an object of the crime, and the means of commitment can be the Internet or any technical means.
3. The researcher wishes the addition of a text to the Electronic Crimes Law that criminalizes anyone who enters, by cheating or fraud, a system or data related to the Internet.
4. The researcher wishes that the legislator should add special provisions to punish the arbitrary use of the computer to seize information during its transfer for fraudulent purposes.

Footnotes

[1] Dr. Mohamed Said Nimour, *Explanation of the Penal Code Crimes against the Funds* (I 4), Dar al-Thaqafa for Publication and Distribution: Amman,
2004,p.234.
[2] Ali Adnan Al-Fil, *Cyber Crime, I 1, Zain Legal and Literary Library*, Beirut, 2011,pp.20-21.
[3] Dr. Nael Abdul Rahman Saleh, Al-Wakiz in *Crimes against Money, I 1,* Dar al-Fikr for Printing, Publishing and Distribution: Amman, 1996,pp.161-162.
[4] Dr. Hisham Mohamed Farid Rustam, *Penal Code and Information Technology Risks, I 1,* Typewriters Library, Assiut, 1995,p.26.
[5] Dr. Abdul Fattah Bayoumi Hijazi, *Combating Computer and Internet Crimes in Model Arab Law,* 1, University Thought House, Alexandria,2006,p.52.
[6] Ali Abdel Qader Al-Kahwaji, *Criminal Protection of Computer Programs, (I 1),* University Press and Publishing House, Beirut, 1999,p.81.

[7] Dr. Ghannam Mohamed Ghannam, *The Unsuitability of Traditional Rules in thePP Penal Code to Combat Computer Crimes, College of Sharia and Law,* UAEUU University, May 200, Vol. III, p. 10.
[8] Dr.Fattouh Al-Shazly, Dr. Afifi Kamel Afifi, *Computer Crimes, (2).* Halabi Publications, Beirut, 2007,p.141-142.
[9] Ali Abdel Qader Al-Kahwaji, Previous Reference , p.105.
[10] Dr.Fattouh Al-Shazly, Dr. Afifi Kamel Afifi, Previous Reference , p.164.
[11] Dr. Abd Elhil Al-Nawaysa, *Crimes of Information Technology, Explanation of Substantive Provisions in the Electronic Crimes Law,* 1, Dar Wael for Culture, Amman, 2017,p.91. See also Dr. Kamel Al-Saeed, *In-depth Criminal Studies in Jurisprudence, Law and Jurisprudence, 1,* Dar Al-Thaqafa for Publishing and Distribution, 2002. Amman,pp.50-51.
[12] Mohammed Amin Al-Shawabki, *Computer and Internet Crimes, Master Thesis, Faculty of Law,* Cairo University, 2002, pp.140-143. See alsoKhalid Ayad Al-Halabi, Investigation *and Investigation Procedures, Master's Thesis, Faculty of Law*, Middle East University, Amman. 2011,p.55.
[13] Dr. Jameel Abdul Baqi Al-Saghir, *Crimes Arising from the Use of Computers* (I 1), Dar Al-Nahda Al-Arabiya, Cairo,p.22.
[14] Dr. Kamel Al-Saeed, Previous Reference , pp. 24-25.
[15] Dr. Mohammed Sami Shawa, *The Information Revolution and its Implications for the Penal Code,* Dar al-Nahda al-Arabiya, 1994,p.120.
[16] CF. Bertrand،*La CriminaliteInformatique :LesDelitsRelatifts au MateRiel : Experteses*،Juin 1948,p.150.
[17] Crime 10 dec. 1970 . JCP.II.17277.D1972.p.155,Bordeaux, 25 mars 1987, D87 Juris,p. 424.
[18] Kyman, le resultat penal ,Rev .Scrim ,1968 ,1968 ,p .781.
[19] Amman Appeal Court Decision No468/2011 , Date 18/6/2011.
[20] Decision of Court of Cassation No 77/120, Lawyers Union Journal ,1977,Nos.7-8,p.1098.
[21] Bilal Amin, Crimes *of Automated Processing of Data and Information in Comparative Legislation and Islamic Law,* 1, University Thought House, Alexandria,p.131.
[22] Dr. Abdulrahman Tawfiq, *Explanation of the Penal Code / Crimes against Money, I 2, 2016*,p.156.
[23] Bilal Amin, Previous Reference, p.137.
[24] Dr. Nael Abdul Rahman Saleh, Previous Reference , p.188.
[25] Dr. Ahmed Hossam Taha Tammam, I, *Crimes Arising from the Use of Computer (I 1)*, Dar al-Nahda al-Arabiya: Cairo, 2000, p.523.
[26] Dr. Mohammed Sami Shawa, Previous Reference , p.126.
[27] Dr. Ahmed Khalifa Al-Malat, *Computer Crimes, I 2,* University Thought House, 2006.p.239. See also Dr. Ahmed Hossam Taha Tammam, I, *Crimes Arising from the Use of Computer (I 1)*, Dar al-Nahda al-Arabiya: Cairo, 2000,p.545.
[28] Dr.Fattouh Al-Shazly, Dr. Afifi Kamel Afifi, Previous Reference , p.165.
[29] Cass.Crim, 25 janvi67,B,17 october1967 B,C,252,G.P.1968,I,P1968,I,P 148 ,note blancher6 Fevrier no39 ,G.P.1967,I,p.229,note casson 65 ,I.C.p.1969 –II, 16116 note H.cuerin,19 December 1973,1969,B,C,no 48.
[30] Dr. Jameel Abdul Baqi Al-Saghir, Previous Reference, pp.115-117.

[31] Douain ,16 Juin 1972 ,2 .p.722.

References

General References

Dr. Abdulrahman Tawfiq, *Explanation of the Penal Code / Crimes against Money, I 2, 2016,*

Dr. Mohamed Said Nimour, *Explanation of the Penal Code Crimesagainst the Funds (I 4),* Dar al-Thaqafa for Publication and Distribution: Amman, 2004.

Dr. Nael Abdul Rahman Saleh, Al-Wakiz in *Crimes against Money, I 1,* Dar al-Fikr for Printing, Publishing and Distribution: Amman, 1996.

Specialized References

Bilal Amin, Crimes *of Automated Processing of Data and Information in Comparative Legislation and Islamic Law,* 1, University Thought House, Alexandria.

Dr. Ahmed Hossam Taha Tammam, I*, Crimes Arising from the Use of Computer (I 1),* Dar al-Nahda al-Arabiya: Cairo, 2000.

Dr. Hisham Mohamed Farid Rustam, *Penal Code and Information Technology Risks, I 1,* Typewriters Library, Assiut, 1995.

Ali Adnan Al-Fil, *Cyber Crime, I 1, Zain Legal and Literary Library,* Beirut, 2011

Dr. Abdul Fattah Bayoumi Hijazi, *Combating Computer and Internet Crimes in Model Arab Law, 1,* University Thought House, Alexandria.

Publishing House, Beirut, 1999.

Dr.Fattouh Al-Shazly, Dr. Afifi Kamel Afifi, *Computer Crimes, (2).* Halabi Publications, Beirut, 2007.

Dr. Kamel Al-Saeed, *In-depth Criminal Studies in Jurisprudence, Law and Jurisprudence, 1*, Dar Al-Thaqafa for Publishing and Distribution, 2002. Amman.

Dr. Abd Elhil Al-Nawaysa, *Crimes of Information Technology, Explanation of Substantive Provisions in the Electronic Crimes Law,* 1, Dar Wael for Culture, Amman, 2017.

Dr. Ahmed Khalifa Al-Malat, *Computer Crimes, I 2,* University Thought House, 2006.

Dr. Jameel Abdul Baqi Al-Saghir, *Crimes Arising from the Use of Computers (I 1),* Dar Al-Nahda Al-Arabiya, Cairo.

Dr. Mohammed Sami Shawa, *The Information Revolution and its Implications for the Penal Code,* Dar al-Nahda al-Arabiya, 1994.

CF. Bertrand ،*La CriminaliteInformatique: LesDelitsRelatifts au MateRiel : Experteses*،Juin 1948.

K yman ،le resultat penal ،Rev .Scrim،1968، 1968.

Master Theses

Khalid Ayad Al-Halabi, Investigation *and Investigation Procedures, Master's Thesis, Faculty of Law*, Middle East University, Amman. 2011.

Mohammed Amin Al-Shawabki, *Computer and Internet Crimes, Master Thesis, Faculty of Law*, Cairo University, 2002.

Research

Dr. Ghannam Mohamed Ghannam, *The Unsuitability of Traditional Rules in thePP Penal Code to Combat Computer Crimes*, College of Sharia and Law, UAEUU University, May 200, Vol. III, p. 10.