UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

INTERNATIONAL DOCTORAL SCHOOL OF THE USC

Majed Falah Miqdad Alsarhan

PhD Thesis

CRIMINAL PROTECTION FOR ELECTRONIC TRANSACTIONS: COMPARATIVE STUDY, JORDANIAN AND IRAQI LEGISLATION

Santiago de Compostela, 2024

Doctoral Programme in Law

ESCOLA DE DOUTORAMENTO
INTERNACIONAL DA USC

DOCTORAL THESIS

CRIMINAL PROTECTION FOR ELECTRONIC TRANSACTIONS: COMPARATIVE STUDY, JORDANIAN AND IRAQI LEGISLATION

Author
Majed Falah Miqdad Alsarhan

Supervisor/s: Carlos Ruiz Miguel / Natalia Pérez Rivas

PHD PROGRAMME IN LAW

SANTIAGO DE COMPOSTELA
2024

Acknowledgments

I would like to extend my thanks to my supervisor, Professor Carlos, whose guidance and feedback helped develop the work, who did so much to bring this work into existence, and who was open to every question or inquiry. And to Dra. Natalia, who I always annoy her with my questions and inquiries, who was not slow in giving me directions, adjustments and comments, and who since then gave me a lot of time, the problems I was facing would not have been solved without Dra. Natalia's help. All the words of thanks in all the languages of the world will not fulfil your rights. And all the poets of the Arab desert, no matter how great their ability to express, will not fulfil your rights. To my father, whose spirit is still among us and I feel it, and which motivates us to work and succeed, as he did while he was alive, to the promise that exists between us, to every white rose that coloured your honourable head, my dear mother, to the one who was like a mountain, on whom I leaned and placed my head on her chest whenever life gets hard on me. To the source of kindness, I wish God for your recovery. To my dear wife who has always stood by my side and endured a lot, thank you very much. To the joy of the heart and the spring of the soul. The beautiful thing in my life, dear Mira. to my dear brothers all thanks my god protect you.

CONTENTS

Abstract

Abstract (ENGLISH)

The era in which we live is called the era of speed because of the great changes brought about by the information revolution that have made the world like a small village. Although its regions are far apart in reality, they have converged in the virtual world. Through the World Wide Web, one can access many websites and conduct many transactions. electronic transactions in short time, and since many electronic transactions have a contractual nature, it was necessary to provide legal protection for them so that those dealing with these electronic means are not exposed to fraud, and from here many countries enacted legislation through which they aimed to protect electronic transaction, the Jordanian legislator and the Iraqi legislator were not far from it. Therefore, both legislators decided to provide legal protection by enacting a legislation for electronic transactions in both countries with the aim of providing legal protection for electronic transactions in their civil aspect. This protection was not limited to the civil aspect in Jordanian legislation, but rather the protection included penal legislation as well through the enactment of a law for electronic crimes. Iraqi legislation was unable to extend criminal protection to electronic transactions, as the draft electronic crimes law has been stagnant for several years, and the Iraqi Council of Representatives has not been able to approve it due to the local and international criticism the draft has been subjected to, which has prevented its approval until the present time.

One of the features of electronic transactions is that they cross borders, and hence this matter may constitute a threat to the sovereignty of states. Therefore, many countries have worked to consolidate the concept of digital sovereignty by extending the state's authority over the digital space, by regulating access to this space and punishing those who violate the legislation regulating this. Digital space.

Due to the rapid development of electronic means of communication, this has resulted in many challenges related to the protection of data for individuals, groups, companies and countries. Perhaps the data of individuals, as it enjoys a kind of privacy, is the most important data that has been protected in many legislations, and the right to privacy is considered one of the rights that have been most subjected to. To the threat through the huge electronic revolution, even though a person lives in isolation from these means and can maintain the privacy of his data through traditional means, cyberspace knocked on his door and entered his home without his permission and made his data vulnerable to violation in light of this vast cyberspace that does not stop at A certain geographical limit and does not recognize the privacy of others

Hence, legislation has begun to confront this threat by adding more protection to the right to privacy so that it remains safe from this violation. However, the legislation in third world countries, including Jordan and Iraq, although they provide a protective cover for the right to privacy, this cover may be useful and effective in Confronting individuals with each other, but it does not provide this amount of protection against governments in third world countries in general, many of which continue to violate the right to privacy under the pretext of maintaining security, and therefore many international reports have criticized these violations.

The legal nature of an electronic transaction is based mostly on its contractual nature. Most contracts are rests the principle of consent, but there are some contracts that are considered contracts of adhesion. Electronic contracts can be considered consensual, but some of them are similar to contracts of adhesion.

Electronic contracts are also characterized by being named contracts. Contracts may be named contracts, which are given a special name by the legal legislation and regulated by the legislator within special provisions. They may be unnamed contracts, which are regulated under general legal rules and do not have a special name or special provisions.

The contract may be concluded in the presence of both parties, and this is common in contracts concluded by normal means, or it may be concluded between absent persons, and this is what characterizes electronic contracts.

Modern legislation has regulated electronic contracts within special provisions, and therefore they can be invoked between parties and against third parties, especially since the legislation has given authority to both the electronic signature and the electronic record.

In order for electronic transactions to be proven, the objective and formal dimensions must be taken into account in cases of proof.

The legal effects of electronic transactions do not differ from the legal effects of regular transactions

As for information crimes, they are crimes of a special nature, since these crimes take place in the electronic environment, and the special nature of these crimes is in terms of the scen in which the attack occurs.

Legal characterization has a role in consolidating the special nature of these crimes, because traditional texts are not sufficient for the purpose as they focus on material standards, while these crimes are committed against the person, money, and property.

Proving evidence is also considered one of the problems raised by electronic crime, as the data being searched for may be encrypted, and incriminating evidence can be erased and destroyed in a short time.

Given the special nature of electronic crimes, there must be special criminal protection against such crimes, which is what many legislations have worked to achieve, including Jordanian legislation and Iraqi legislation, although Iraqi legislation has not done enough.

Criminal protection is not limited to the substantive aspect of electronic transactions, but rather this protection extends to the procedural aspect as well. However, there are many procedural problems in electronic transactions, as they relate to electronic processing data and intangible entities, which makes it difficult to detect them on the one hand, and difficult to On the other hand, collecting evidence regarding them. What increases the difficulty of these procedures is the speed and accuracy of carrying out these crimes and the possibility of erasing their effects and concealing the evidence obtained immediately after the implementation of such crimes.

After the researcher completed his study, many things became clear to him that can be listed in the following points:

- Electronic transactions are defined as completing business and concluding contracts through an electronic format, and they include all activities and businesses related to the exchange of data and information, as well as goods and services via the Internet between consumers and companies, or between companies with each other, and they represent both parties to the contractual relationship in the electronic business environment.

- One of the positives of electronic transactions is that it breaks geographical borders, achieves the principle of abundance, is subject to the provisions of international law, relies on electronic means of proof, achieves the health dimension, and creates equality between ordinary individuals and people with special needs. Moreover, dealing with electronic transactions is one of the criteria for the progress and development of countries.

- The disadvantages of electronic transactions are that exposure to fraud is greater than fraud in regular transactions, and electronic fraud in electronic transactions is broader in scope than fraud in regular transactions. In addition, errors occur frequently in electronic transactions, and the perception of coercion is one of the defects surrounding electronic transactions.

- The electronic transaction is characterized by having an international dimension due to the cross-border nature of the electronic transaction. Also, the electronic transaction may be between states and sovereign states, so the rules of international

law are applied in this case, as the law of one state may not be governing another state. Also, through the law of will, resort may be made to the rules of international law and make it the governing law over electronic transactions.

- The law of will that governs the electronic transaction may be agreed upon between the parties, may be explicitly stipulated, or may be implicitly stipulated.
- Among the rules that the judge resorts to in determining the applicable law in the event of a dispute is the language in which the contract was written, the currency in which the payment will be made, the nationality of the contracting parties, the place where the contract was concluded, or the place of its entry into force.
- The Jordanian legislator is criticized for confining himself to stipulating that the objective scope of application of the law is that it is transactions carried out by electronic means, while the Iraqi legislator touched on the personal scope in the context of his presentation of the objective scope of electronic transactions by stipulating that an electronic transaction is carried out by natural or legal persons, as was the case. The dominance of will was present when explaining the objective scope of the Iraqi legislation. He explained that the application of the provisions of the law includes transactions that the parties agree to implement by electronic means, in addition to that the Iraqi legislation placed financial and electronic commercial securities within the objective scope of the application of the law, and these matters were overlooked by the Jordanian legislator and did not stipulate them. The researcher suggests that the text of the Iraqi legislator in determining the objective scope of electronic transactions was more comprehensive and general than the text of the Jordanian legislator.
- Personal data in electronic transactions is a right worthy of legal protection.
- The right to privacy has been recognized in, international treaties and charters, and the national constitutions of countries
- The call for developing unified global legislation to deal with electronic transactions conflict with the reality of criminalizing some transactions in countries and considering them permissible in other countries.
- The legislation for electronic transactions aims to protect information from the dangers of electronic means and to deter anyone who might tempt himself to use this information illegally.
- Financial data is considered personal data worthy of legal protection
- The threat to financial data is greater than threats to other personal data

- There are many and varied forms of threat to financial data, from electronic piracy to phishing to penetrating vulnerabilities and decoding codes to blowing up websites and many others.

- Financial data received the necessary legal protection in Jordanian legislation due to the importance of protecting this data. And we did not see this protection in Iraqi legislation

- The electronic contract is a contract characterized by a consensual character, not an adhesion character, as the method used in contracting does not change the nature of the contract, and most contracts are consensual contracts, and adhesion contracts remain adhesion contracts, whether they are concluded by normal means or through electronic means, the means used In contracting, the nature and reality of the contract do not change in any way

- Both Jordanian and Iraqi legislation recognized the authenticity of electronic transactions, and electronic contracts were given legal status as a contract in which both parties are committed to the content of the contract concluded between them by electronic means.

- To prove electronic transactions, certain conditions must be met in order for the electronic signature of its owner to be proven, and certain conditions must be present in the record or electronic document in order for it to be evidence in the event of disagreement between the two parties to the contract.

- The effects resulting from electronic transactions do not differ from the effects resulting from regular transactions, as the method used in concluding the contract between the parties does not change the reality of the contract in any way.

- electronic crimes are acrime of a special nature, but in order for criminal liability to arise for these crimes, the criminal act must exist, and the essence of the technical activity is that there must be a digital environment in which the perpetrator performs actions in order for this element to be achieved, and also the preparatory work falls within the criminal act, such as Purchasing the programs or equipment necessary to carry out the act. The criminal act also requires that the perpetrator be aware of how to use the computer and the programs necessary to carry out the act. Criminal intent must also be present, which is the planning and management of the perpetrator and his intention to commit his crime in the electronic environment, it also requires the availability of the elements of knowledge and will, and the Criminal intent is the mental state of the offender in which he was inclined to carry out this act. While knowing that the law criminalizes it, and there must be a causal relationship linking his crime. Artistic activity and its intention to cause crime in the electronic environment.

- Criminal intent in the electronic environment is rests three cases: -

  A- If the perpetrator wants to achieve a result resulting from his criminal behavior, such as if the perpetrator illegally enters the website while knowing that this access is illegal.

  B- the permissibility of intent, such as if one person sends a virus to another via computers, the intention being to reduce the speed of the device of the person to whom the virus is sent, and this virus works to destroy the device.

  C- The case of the enorm of the criminal result, in which a person hacks into another person's device in order to obtain a file containing personal photos of that person, then publishes it, and along with the personal photos of that person are financial data related to him.

- Many theories have been found to determine the criterion for verifying a causal relationship. These theories are:

  A- The theory of equivalence of causes. This theory cannot be applied in cyberspace.

  B- The theory of direct cause. An example of it in cyberspace is the seizure of a person's electronic funds. A weak password is not considered the reason for the seizure of electronic funds, but rather the act of theft is considered the direct cause of the seizure.

  C - The theory of appropriate cause, such as if a person sends a virus that is known to disrupt the device's system without destroying it, but after sending this virus, this person's device is destroyed. Here, the criminal liability is limited to disrupting the system without destroying it.

- One of the crimes committed on the website is the crime of illegal access or bypassing authorized access without making any change, as well as the crime of illegal access or bypassing authorized access in order to delete, add, modify, or hack information system data or information.

- The Jordanian legislator and the Iraqi draft criminalized illegal entry or exceeding authorized entry and imposed financial fines and imprisonment penalties for this crime.

- The aggravating circumstance is the crime of illegal entry or exceeding authorized entry if it harms national security, foreign relations, public safety, or the national economy.

- The Jordanian legislator and the Iraqi draft law criminalized illegal access or exceeding authorized access in order to delete, add, hack or modify data or information of the information system.

- The aggravating circumstance is illegal access to delete, add, modify or hack data if it targets money transfer or related to electronic payment services or any of the financial services provided by banks and financial companies.

- Criminal liability is punishing a person criminally for the crime he has committed by applying the rules of criminal law to him

- Criminal liability in the field of electronic transactions rests the service provider in two cases: -

  A- The case of being an accomplice in an electronic crime carried out by a person on the Internet.

  B- If he is aware of the electronic content and allows it to spread

- The European approach defines the service provider as any natural or legal person who provides Internet service in the information services community.

- The most important obligations of the service provider with regard to criminal liability are as follows: -

  A- The authorities must be informed in the event of publishing information related to a threat to the national or economic security of the state or publishing pornographic materials.

  B- The obligation of electronic service providers to respect the right to privacy and confidentiality of correspondence.

  C- Electronic service providers must monitor information that constitutes a crime that threatens the security and safety of the state.

  D- Commitment to block websites, links, or informational content upon the request of the investigating authorities and the court.

- There are three trends in determining the criminal liability of the electronic service provider, which are as follows: -

  A - The first trend: - It says not to impose criminal liability on electronic service providers because it is impossible for service providers to monitor all information via the Internet, in addition to their job being a technical job.

B - The second trend: - It calls for imposing criminal liability on electronic service providers, considering that failure to determine responsibility leads to a greater spread of illegal electronic information.

C- The third direction: He said that criminal liability is imposed on the electronic service provider in three cases:-

The first case: If it is proven that he is a source of illegal information and data.

The second case: the case of his failure to stop broadcasting illegal content despite his knowledge of it.

The third case: If he refuses to cooperate with the authorities if he is asked to do so.

- Criminal protection is not limited to the substantive aspect of electronic transactions, but rather this protection extends to the procedural aspect as well.
- The Electronic crime Unit was established in Jordan, affiliated with the Public Security Service, in 2008. This unit is a unit specialized in tracking electronic crimes. It consists of a group of specialists in tracking electronic crimes. This unit uses advanced tools, in addition to seeking the help of telecommunications companies that provide Internet services. This unit works to investigate, research and investigate crimes occurring through the Internet. In Iraq, there is a department called the Electronic Crime Control Department, affiliated with the police. Iraqi.
- The jurisdiction of the judicial police during the research and investigation stage is limited to two matters: receiving reports and complaints, preview
- The jurisdiction of the inspection mission in electronic crimes is limited to the information crimes unit located within the state and by judicial order, whose work is to investigate electronic crimes occurring within the borders of the state via the Internet, and the scope of the inspection is not limited, but rather broad in order to find all persons contributing to the investigation. Crime, even if it is a minor contribution.
- One of the special methods of combating electronic crimes is to intercept correspondence, record votes, and take pictures.
- Procedural protection at the trial stage consists of narrowing the scope of attendance at the trial resulting from a electronic crime, as its sessions are not open, which gives a kind of protection to the person of the perpetrator.

- A jurisprudential dispute arose over the conflict of judicial jurisdiction with regard to the criminal information crime. Jurisprudence was divided into three trends: the approach of criminal activity, the approach of where the result is achieved, and the mixed approach.

- Electronic evidence is defined as evidence taken from computers and in the form of electromagnetic or electrical pulses that can be collected and analyzed using special programs, applications and technology and can be presented in the form of evidence that can be approved before the court.

Modern procedures for seizing electronic evidence are carried out by controlling intercepting or monitoring electronic evidence.

- Means of proof, including electronic means of proof, are considered among the most important means that the legislator or regulator must pay attention to in various countries of the world because of the consequences of these means in proving the rights and obligations between members of society in their various legal positions.

Resumo

Resumo (GALISIAN)

A época na que vivimos chámase era da velocidade polos grandes cambios provocados pola revolución da información que fixeron que o mundo semellase unha pequena aldea. Aínda que as súas rexións están moi afastadas en realidade, converxeron no mundo virtual. A través da World Wide Web, pódese acceder a moitos sitios web e realizar moitas transaccións. transaccións electrónicas nun tempo récord, e dado que moitas transaccións electrónicas teñen carácter contractual, foi necesario dotalas de protección xurídica para que os que se ocupan destes medios electrónicos non se vexan expostos á fraude, e dende aquí moitos países promulgaron unha lexislación a través da que pretenden para protexer a información electrónica, e o lexislador xordano e o lexislador iraquí non eran inmunes. Por iso, ambos os lexisladores decidiron dotar de protección civil mediante a promulgación dunha lei para as transaccións electrónicas en ambos os países co obxectivo de ofrecer protección xurídica ás transaccións electrónicas na súa vertente civil. Esta protección non se limitaba ao aspecto civil na lexislación xordana, senón que a protección incluía tamén a lexislación penal mediante a promulgación dunha lei para os delitos electrónicos. A lexislación iraquí non puido estender a protección penal ás transaccións electrónicas, xa que o proxecto de lei de delitos electrónicos leva varios anos estancado e o Consello de Representantes iraquí non puido aprobalo debido ás críticas locais e internacionais que foi sometida ao proxecto.a o que impediu a súa aprobación ata o momento.

Unha das características das transaccións electrónicas é que traspasan fronteiras e, polo tanto, este asunto pode constituír unha ameaza para a soberanía dos Estados. Por iso, moitos países traballaron para consolidar o concepto de soberanía dixital ampliando a autoridade do Estado sobre o espazo dixital, regulando o acceso a este espazo e castigando a quen incumpre a lexislación que o regula. Espazo dixital.

Debido ao rápido desenvolvemento dos medios electrónicos de comunicación, isto deu lugar a moitos retos relacionados coa protección de datos para persoas, grupos, empresas e países. Quizais os datos das persoas físicas, ao gozar dunha especie de privacidade, sexan os datos máis importantes que foron protexidos en moitas lexislacións, e o dereito á intimidade é considerado un dos dereitos aos que máis se someteu. Ante a ameaza pola revolución electrónica masiva, aínda que unha persoa vive illada destes medios e pode manter a privacidade dos seus datos a través dos medios tradicionais, o ciberespazo chamou á súa porta e entrou na súa casa sen o seu permiso e fixo que os seus datos sexan vulnerables á violación. á luz deste vasto ciberespazo que non se detén nun certo límite xeográfico e non recoñece a privacidade dos demais

Por iso, a lexislación comezou a facer fronte a esta ameaza engadindo máis protección ao dereito á intimidade para que estea a salvo desta violación. Non obstante, a lexislación dos países do terceiro mundo, incluíndo Xordania e Iraq, aínda que proporcionan unha cobertura protectora para o dereito á intimidade, esta cobertura pode ser útil e eficaz para enfrontarse aos individuos entre si, pero non proporciona esta cantidade de protección contra gobernos dos países do terceiro mundo en xeral, moitos dos cales seguen vulnerando o dereito á intimidade co pretexto de manter a seguridade, polo que moitos informes internacionais criticaron estas violacións.

A natureza xurídica dunha transacción electrónica baséase principalmente na súa natureza contractual. A maioría dos contratos baséanse no principio de consentimento, pero hai algúns contratos que se consideran contratos de adhesión. Os contratos electrónicos pódense considerar consensuados, pero algúns deles son similares aos contratos de adhesión.

Os contratos electrónicos tamén se caracterizan por ser contratos denominados. Os contratos poderán ser denominados contratos, que reciben unha denominación especial pola lexislación legal e regulados polo lexislador dentro de disposicións especiais. Poderán tratarse de contratos sen nome, que están regulados por normas xurídicas xerais e non teñen denominación especial nin disposicións especiais.

O contrato pode celebrarse en presenza de ambas as partes, e isto é habitual nos contratos celebrados pola vía normal, ou pode celebrarse entre ausentes, e iso é o que caracteriza aos contratos electrónicos.

A lexislación moderna regulou os contratos electrónicos dentro de disposicións especiais, polo que poden ser invocados entre partes e contra terceiros, sobre todo porque a lexislación outorgou autoridade tanto á sinatura electrónica como ao rexistro electrónico.

Para que se acrediten as transaccións electrónicas, hai que ter en conta a dimensión obxectiva e formal nos casos de proba.

Os efectos legais das transaccións electrónicas non difiren dos efectos legais das transaccións habituais

En canto aos delitos informativos, son delitos de carácter especial, xa que estes delitos teñen lugar no entorno electrónico, e a especialidade destes delitos é no que se refire ao escenario no que se produce o atentado.

A caracterización xurídica ten un papel na consolidación da especialidade destes delitos, pois os textos tradicionais non son suficientes para o efecto xa que se centran en normas materiais, mentres que estes delitos se cometen contra a persoa, o diñeiro e o patrimonio.

A proba de probas tamén se considera un dos problemas que suscita a ciberdelincuencia, xa que os datos que se buscan poden estar cifrados e as probas incriminatorias poden borrarse e destruírse en pouco tempo.

Dada a natureza especial dos delitos electrónicos, debe haber unha protección penal especial contra estes delitos, que é o que conseguiron moitas lexislacións, incluídas a lexislación xordana e a lexislación iraquí, aínda que a lexislación iraquí non fixo o suficiente.

A protección penal non se limita ao aspecto substantivo das transaccións electrónicas, senón que esta protección se estende tamén ao aspecto procesual. Non obstante, existen moitos problemas de procedemento nas transaccións electrónicas, xa que se relacionan co tratamento electrónico de datos e entidades intanxibles, o que dificulta a súa detección, por unha banda, e, por outra banda, a recollida de probas ao respecto. O que acrecenta a dificultade destes procedementos é a rapidez e precisión na realización destes delitos e a posibilidade de borrar as súas pegadas e ocultar as probas obtidas inmediatamente despois da realización destes delitos.

Despois de que o investigador completou o seu estudo, quedaron claras moitas cousas que se poden enumerar nos seguintes puntos:

- As transaccións electrónicas defínense como a realización de negocios e a celebración de contratos a través dun formato electrónico, e inclúen todas as actividades e negocios relacionados co intercambio de datos e información, así como de bens e servizos a través de Internet entre consumidores e empresas, ou entre empresas con entre si, e representan a ambas as partes na relación contractual no ámbito dos negocios electrónicos.

- Unha das vantaxes das transaccións electrónicas é que rompe fronteiras xeográficas, logra o principio de abundancia, está suxeita ás disposicións do dereito internacional, depende de medios electrónicos de proba, alcanza a dimensión sanitaria e crea igualdade entre os individuos comúns e as persoas. con necesidades especiais. Ademais, tratar coas transaccións electrónicas é un dos criterios para o progreso e desenvolvemento dos países.

- As desvantaxes das transaccións electrónicas son que a exposición á fraude é maior que a fraude nas transaccións habituais e que a fraude electrónica nas transaccións electrónicas ten un alcance máis amplo que a fraude nas transaccións habituais. Ademais, os erros ocorren con frecuencia nas transaccións electrónicas, e a percepción de coacción é un dos defectos que rodean as transaccións electrónicas.

- A transacción electrónica caracterízase por ter unha dimensión internacional debido ao carácter transfronteirizo da transacción electrónica. Ademais, a transacción electrónica pode ser entre estados e estados soberanos, polo que neste caso aplícanse

as normas do dereito internacional, xa que a lei dun estado pode non estar rexendo a outro. Así mesmo, mediante a lei da vontade, pódese recorrer ás normas do dereito internacional e convertela na lei reguladora das transaccións electrónicas.

- A lei de vontade que rexe a transacción electrónica poderá acordarse entre as partes, estipularse de forma explícita ou demostrarse implícitamente.

- Entre as normas ás que recorre o xuíz para determinar a lexislación aplicable en caso de litixio figura a lingua na que se redactou o contrato, a moeda na que se realizará o pagamento, a nacionalidade das partes contratantes, o lugar onde se redactou o contrato. o contrato foi celebrado, ou o lugar da súa entrada en vigor.

- Critícase ao lexislador xordano por limitarse a estipular que o ámbito obxectivo de aplicación da lei é que se trata de transaccións realizadas por medios electrónicos, mentres que o lexislador iraquí tocou o ámbito persoal no contexto da súa presentación do ámbito obxectivo. de transaccións electrónicas estipulando que unha transacción electrónica é realizada por persoas físicas ou xurídicas, como foi o caso. O dominio da vontade estivo presente ao explicar o alcance obxectivo da lexislación iraquí. Explicou que a aplicación das disposicións da lei inclúe transaccións que as partes acordan executar por medios electrónicos, ademais de que a lexislación iraquí sitúa os valores financeiros e electrónicos comerciais dentro do ámbito obxectivo da aplicación da lei, e estes asuntos. foron pasados por alto polo lexislador xordano e non os estipulou. O estudo suxire que o texto do lexislador iraquí para determinar o alcance obxectivo das transaccións electrónicas era máis completo e xeral que o texto do lexislador xordano.

- Os datos persoais nas transaccións electrónicas son un dereito digno de protección legal.

- O dereito á privacidade foi recoñecido nas leis divinas, nos tratados e cartas internacionais e nas constitucións nacionais dos países.

- O chamamento a desenvolver unha lexislación global unificada para facer fronte ás transaccións electrónicas choca coa realidade de criminalizar algunhas transaccións en países e consideralas admisibles noutros países.

- Tanto a lexislación xordana como a iraquí proporcionaron protección legal aos datos persoais das persoas mediante unha lexislación especial para as transaccións electrónicas debido á incapacidade da lexislación tradicional para proporcionar esta protección.

- A lexislación sobre transaccións electrónicas ten como obxectivo protexer a información dos perigos dos medios electrónicos e disuadir a calquera que poida tentar utilizar esta información de forma ilegal.

- Os datos financeiros considéranse datos persoais dignos de protección legal
- A ameaza aos datos financeiros é maior que as ameazas a outros datos persoais
- Existen moitas e variadas formas de ameaza para os datos financeiros, desde a piratería electrónica ata o phishing, a penetración de vulnerabilidades e códigos de decodificación ata a explosión de sitios web e moitos outros.
- Os datos financeiros recibiron a protección legal necesaria tanto na lexislación xordana como na iraquí debido á importancia de protexer estes datos.
- O contrato electrónico é un contrato caracterizado por un carácter consensuado, non un carácter de adhesión, xa que o método empregado na contratación non modifica a natureza do contrato, e a maioría dos contratos son contratos consensuados, e os contratos de adhesión seguen sendo contratos de adhesión, tanto se son. celebrado por medios normais ou por medios electrónicos, os medios utilizados Na contratación, a natureza e realidade do contrato non cambian de ningún xeito.
- Tanto a lexislación xordana como a iraquí recoñecían a autenticidade das transaccións electrónicas, e os contratos electrónicos recibiron carácter legal como un contrato no que ambas as partes se comprometen co contido do contrato celebrado entre elas por medios electrónicos.
- Para acreditar as transaccións electrónicas débense cumprir determinadas condicións para que se acredite a sinatura electrónica do seu titular, así como determinadas condicións no rexistro ou documento electrónico para que sexa proba en caso de desacordo entre os dúas partes do contrato.
- Os efectos derivados das transaccións electrónicas non se diferencian dos efectos derivados das transaccións habituais, xa que o método empregado para celebrar o acordo entre as partes non modifica en ningún caso a realidade do contrato.
- Os delitos electrónicos son delitos de carácter especial, pero para que destes delitos se deriven responsabilidade penal é preciso que conste o elemento material, cuxo centro sexa a actividade técnica. Así mesmo, debe estar presente o elemento moral, que é a planificación e xestión do infractor e a presenza da súa intención de provocar o seu delito na contorna electrónica con Sabía que a lei o criminalizaba, e debe existir unha relación causal que vincule o seu delito. actividade técnica e a súa intención de provocar o delito na contorna electrónica.
- A intención criminal no ámbito electrónico baséase en tres casos: -

A- Se o agresor quere acadar un resultado derivado da súa conduta delituosa, como se o autor entra ilegalmente na páxina web sabendo que este acceso é ilegal.

B- Se a intención é permisible, como se unha persoa envía un virus a outra a través de ordenadores, a intención é reducir a velocidade do dispositivo da persoa á que se envía o virus, e este virus traballa para destruír o dispositivo.

C- O caso da gravidade do resultado delituoso, no que unha persoa piratea o dispositivo doutra persoa co fin de obter un ficheiro que contén fotos persoais desa persoa, despois publícao, e xunto coas fotos persoais desa persoa son datos económicos. relacionados con el.

- Atopáronse moitas teorías para determinar o criterio para verificar unha relación causal. Estas teorías son:

A- A teoría da equivalencia de causas. Esta teoría non se pode aplicar no ciberespazo.

B- A teoría da causa directa. Un exemplo diso no ciberespazo é a incautación dos fondos electrónicos dunha persoa. Un contrasinal débil non se considera o motivo da incautación de fondos electrónicos, senón que o acto de roubo considérase a causa directa da incautación.

C - A teoría da causa adecuada, como se unha persoa envía un virus que se sabe que perturba o sistema do dispositivo sen destruílo, pero despois de enviar este virus, o dispositivo desta persoa destrúese. Aquí, a responsabilidade penal limítase a perturbar o sistema sen destruílo.

- Un dos delitos cometidos na páxina web é o de acceso ilícito ou elusión de acceso autorizado sen realizar ningún cambio, así como o delito de acceso ilegal ou elusión de acceso autorizado para eliminar, engadir, modificar ou piratear datos do sistema de información. o información.

- O lexislador xordano e o proxecto iraquí penalizaron a entrada ilegal ou o exceso de entrada autorizada e impuxeron multas económicas e penas de prisión por este crime.

- A circunstancia agravante é o delito de entrada ilegal ou exceso de entrada autorizada se prexudica a seguridade nacional, as relacións exteriores, a seguridade pública ou a economía nacional.

- O lexislador xordano e o anteproxecto de lei iraquí penalizaron o acceso ilegal ou exceder o acceso autorizado para eliminar, engadir, piratear ou modificar datos ou información do sistema de información.

- A circunstancia agravante é o acceso ilegal para borrar, engadir, modificar ou piratear datos se ten como obxectivo a transferencia de diñeiro ou está relacionado

con servizos de pago electrónico ou calquera dos servizos financeiros prestados por bancos e empresas financeiras.

- A responsabilidade penal é castigar penalmente a unha persoa polo delito que cometeu aplicándolle as normas do dereito penal.
- A responsabilidade penal no ámbito das transaccións electrónicas recae sobre o prestador do servizo en dous casos: -

  A- O caso de ser cómplice dun ciberdelito realizado por unha persoa en Internet.

  B- Se coñece o contido electrónico e permite que se difunda
- O enfoque europeo define o provedor de servizos como calquera persoa física ou xurídica que preste servizo de Internet na comunidade de servizos de información.
- Tanto a lexislación xordana como a iraquí son criticadas por non definir o provedor de servizos electrónicos.
- As obrigas máis importantes do prestador de servizos en materia de responsabilidade punitiva son as seguintes: -

  A- As autoridades deberán ser informadas no caso de publicar información relacionada con unha ameaza para a seguridade nacional ou económica do Estado ou de publicar materiais pornográficos.

  B- A obriga dos provedores de servizos electrónicos de respectar o dereito á intimidade e á confidencialidade da correspondencia.

  C- Os provedores de servizos electrónicos deben controlar a información que constitúa un delito que ameaza a seguridade e a seguridade do Estado.

  D- Compromiso de bloquear sitios web, ligazóns ou contidos informativos a petición das autoridades instrutoras e do xulgado.
- Existen tres tendencias na determinación da responsabilidade penal do provedor de servizos electrónicos, que son as seguintes: -

  R - A primeira tendencia: - Di non impoñer responsabilidades penais aos provedores de servizos electrónicos porque é imposible que os provedores de servizos controlen toda a información a través de Internet, ademais de que o seu traballo é un traballo técnico.

  B - A segunda tendencia: - Demanda a imposición de responsabilidade penal aos provedores de servizos electrónicos, por considerar que a falta de determinación

da responsabilidade leva a unha maior difusión da información electrónica ilegal.

C- A terceira dirección: Dixo que a responsabilidade penal se impón ao provedor de servizos electrónicos En tres casos:-

O primeiro caso: Se se acredita que é fonte de información e datos ilícitos.

O segundo caso: o caso da súa incapacidade de deixar de emitir contidos ilícitos a pesar do seu coñecemento.

O terceiro caso: se se nega a cooperar coas autoridades se se lle pide que o faga.

- A protección penal non se limita ao aspecto substantivo das transaccións electrónicas, senón que esta protección se estende tamén ao aspecto procesual.
- A Unidade de Ciberdelincuencia creouse en Xordania, afiliada ao Servizo de Seguridade Pública, en 2008. Esta unidade é unha unidade especializada na persecución de delitos electrónicos. Está formado por un grupo de especialistas no seguimento de delitos electrónicos. Esta unidade utiliza ferramentas avanzadas, ademais de buscar a axuda das empresas de telecomunicacións que prestan servizos de Internet. Esta unidade traballa para investigar, investigar e investigar os delitos que se producen a través de Internet. En Iraq, hai un departamento chamado Electronic Crime Control Department, afiliado á policía. iraquí.
- A competencia da policía xudicial durante a fase de investigación e investigación limítase a dúas materias: recepción de denuncias, denuncias e vista previa.
- A competencia da misión de inspección en delitos electrónicos limítase á unidade de delitos informativos situada dentro do Estado e por orde xudicial, cuxo traballo consiste en investigar os delitos electrónicos que se produzan dentro das fronteiras do Estado a través de Internet, e o ámbito da inspección. non é limitado, senón máis ben amplo para atopar todas as persoas que contribúen á investigación. Delito, aínda que sexa unha contribución menor.
- Un dos métodos especiais de loita contra os delitos electrónicos é interceptar a correspondencia, rexistrar votos e tomar fotografías.
- A protección procesual na fase de xuízo consiste en estreitar o ámbito de asistencia ao xuízo derivado dun ciberdelito, xa que as súas sesións non son abertas, o que outorga unha especie de protección á persoa do autor.
- Xurdiu un litixio xurisprudencial polo conflito de xurisdición xudicial no que se refire ao delito penal de información. A xurisprudencia dividiuse en tres tendencias:

a doutrina da actividade criminal, a doutrina de onde se consegue o resultado e a doutrina mixta.

- As probas electrónicas defínese como as probas tomadas de ordenadores e en forma de pulsos electromagnéticos ou eléctricos que poden ser recollidos e analizados mediante programas, aplicacións e tecnoloxía especiais e que poden presentarse en forma de probas que poidan ser aprobadas ante o tribunal.

  Os procedementos modernos para controlar as probas electrónicas lévanse a cabo mediante a incautación, a interceptación ou o seguimento das probas electrónicas.

- Os medios de proba, incluídos os medios electrónicos de proba, considéranse entre os medios máis importantes aos que o lexislador ou o regulador debe prestar atención en varios países do mundo polas consecuencias destes medios para demostrar os dereitos e obrigas entre os membros da sociedade. nas súas distintas posicións xurídicas.

Resumen (SPANISH)

La era en que vivimos se llama la era de la velocidad debido a los grandes cambios provocados por la revolución de la información, que han hecho que el mundo se parezca a una pequeña aldea. Aunque sus regiones están muy alejadas en la realidad, han convergido en el mundo virtual. A través internet, uno puede acceder a muchos sitios web y realizar muchas transacciones. transacciones electrónicas en un tiempo récord, y dado que muchas transacciones electrónicas tienen carácter contractual, era necesario proporcionarles protección jurídica para que quienes tratan con estos medios electrónicos no se vean expuestos al fraude, y a partir de aquí muchos países promulgaron leyes con las que pretendían proteger la información electrónica, y el legislador jordano y el legislador iraquí no fueron inmunes. Por lo tanto, ambos legisladores decidieron proporcionar protección civil promulgando una ley para las transacciones electrónicas en ambos países con el objetivo de proporcionar protección jurídica a las transacciones electrónicas en su aspecto civil. Esta protección no se limitó al aspecto civil en la legislación jordana, sino que la protección incluyó también la legislación penal mediante la promulgación de una ley de delitos electrónicos. La legislación iraquí no ha podido ampliar la protección penal a las transacciones electrónicas, ya que el proyecto de ley sobre delitos electrónicos lleva varios años estancado y el Consejo de Representantes iraquí no ha podido aprobarlo debido a las críticas locales e internacionales de que ha sido objeto el proyecto, lo que ha impedido su aprobación hasta el momento.

Una de las características de las transacciones electrónicas es que traspasan las fronteras, por lo que este asunto puede constituir una amenaza para la soberanía de los Estados. Por ello, muchos países han trabajado para consolidar el concepto de soberanía digital ampliando la autoridad del Estado sobre el espacio digital, regulando el acceso a este espacio y castigando a quienes infrinjan la legislación que lo regula. Debido al rápido desarrollo de los medios electrónicos de comunicación, se han planteado numerosos retos relacionados con la protección de datos de individuos, grupos, empresas y países. Quizás los datos de los individuos, al gozar de una especie de privacidad, son los que más se han protegido en muchas legislaciones, y el derecho a la privacidad se considera uno de los derechos que más se han visto sometidos. A la amenaza a través de la revolución electrónica masiva, aunque una persona viva aislada de estos medios y pueda mantener la privacidad de sus datos a través de los medios tradicionales, el ciberespacio llama a su puerta y entra en su casa sin su permiso y hace que sus datos sean vulnerables a la violación a la luz de este vasto ciberespacio que no se detiene en un determinado límite geográfico y no reconoce la privacidad de los demás. De ahí que la legislación haya empezado a hacer frente a esta amenaza añadiendo más protección al derecho a la intimidad para que permanezca a salvo de

esta violación. Sin embargo, la legislación de los países del tercer mundo, incluidos Jordania e Irak, aunque proporcionan una cobertura protectora del derecho a la intimidad, esta cobertura puede ser útil y eficaz para enfrentar a los individuos entre sí, pero no proporciona esta cantidad de protección contra los gobiernos de los países del tercer mundo en general, muchos de los cuales siguen violando el derecho a la intimidad con el pretexto de mantener la seguridad, por lo que muchos informes internacionales han criticado estas violaciones.

La naturaleza jurídica de una transacción electrónica se basa sobre todo en su carácter contractual. La mayoría de los contratos se basan en el principio del consentimiento, pero hay algunos que se consideran contratos de adhesión. Los contratos electrónicos pueden considerarse consensuales, pero algunos de ellos son similares a los contratos de adhesión. Los contratos electrónicos también se caracterizan por ser contratos nominativos. Pueden ser contratos denominados, a los que la legislación jurídica da un nombre especial y que el legislador regula en disposiciones especiales. Pueden ser contratos innominados, que se rigen por normas jurídicas generales y no tienen una regulación específica. El contrato puede celebrarse en presencia de ambas partes, y esto es habitual en los contratos celebrados por medios normales, o puede celebrarse entre personas ausentes, y esto es lo que caracteriza a los contratos electrónicos. La legislación moderna ha regulado los contratos electrónicos dentro de disposiciones especiales, por lo que pueden ser invocados entre las partes y frente a terceros, sobre todo porque la legislación ha dado autoridad tanto a la firma electrónica como al registro electrónico. Para que las transacciones electrónicas puedan probarse, deben tenerse en cuenta las dimensiones objetiva y formal en los casos de prueba. Los efectos jurídicos de las transacciones electrónicas no difieren de los efectos jurídicos de las transacciones ordinarias.

En cuanto a los delitos informáticos, son delitos de naturaleza especial, ya que estos delitos tienen lugar en el entorno electrónico, y la naturaleza especial de estos delitos es en cuanto al escenario en el que se produce el ataque. La caracterización jurídica desempeña un papel a la hora de consolidar la naturaleza especial de estos delitos, ya que los textos tradicionales no son suficientes a tal efecto, pues se centran en normas materiales, mientras que estos delitos se cometen contra la persona, el dinero y la propiedad. La prueba también se considera uno de los problemas que plantea la ciberdelincuencia, ya que los datos que se buscan pueden estar encriptados y las pruebas incriminatorias pueden borrarse y destruirse en poco tiempo. Dada la especial naturaleza de los delitos electrónicos, debe existir una protección penal especial contra estos delitos, que es lo que muchas legislaciones han tratado de conseguir, entre ellas la jordana y la iraquí, aunque la iraquí no ha hecho lo suficiente.

La protección penal no se limita al aspecto sustantivo de las transacciones electrónicas, sino que esta protección se extiende también al aspecto procesal. Sin embargo, existen muchos problemas de procedimiento en las transacciones electrónicas, ya que se refieren a datos de procesamiento electrónico y entidades intangibles, lo que dificulta, por un lado, su detección y, por otro, la obtención de pruebas al respecto. Lo que aumenta la dificultad de

estos procedimientos es la rapidez y precisión con que se llevan a cabo estos delitos y la posibilidad de borrar sus huellas y ocultar las pruebas obtenidas inmediatamente después de la ejecución de tales delitos.

Después de completar la investigación, varios son los puntos que han sido clarificados:

- Las transacciones electrónicas se definen como la realización de negocios y la celebración de contratos a través de un formato electrónico, e incluyen todas las actividades y negocios relacionados con el intercambio de datos e información, así como de bienes y servicios a través de Internet entre consumidores y empresas, o entre empresas entre sí, y representan a ambas partes de la relación contractual en el entorno de los negocios electrónicos.

- Uno de los aspectos positivos de las transacciones electrónicas es que rompe las fronteras geográficas, logra el principio de abundancia, está sujeta a las disposiciones del derecho internacional, se basa en medios de prueba electrónicos, logra la dimensión sanitaria y crea igualdad entre las personas normales y las personas con necesidades especiales. Además, el tratamiento de las transacciones electrónicas es uno de los criterios de progreso y desarrollo de los países.

- Las desventajas de las transacciones electrónicas son que la exposición al fraude es mayor que en las transacciones ordinarias, y el fraude en las transacciones electrónicas tiene un alcance más amplio que el fraude en las transacciones ordinarias. Además, en las transacciones electrónicas se producen errores con frecuencia, y la percepción de coacción es uno de los defectos que rodean a las transacciones electrónicas.

- La transacción electrónica se caracteriza por tener una dimensión internacional debido a la naturaleza transfronteriza de la transacción electrónica. Además, la transacción electrónica puede ser entre estados y estados soberanos, por lo que en este caso se aplican las normas del derecho internacional, ya que la ley de un estado puede no regir en otro estado. Asimismo, a través del derecho de la voluntad, se puede recurrir a las normas del derecho internacional y convertirlo en la ley rectora de las transacciones electrónicas.

- La ley de la voluntad que rige la transacción electrónica puede acordarse entre las partes, estipularse explícitamente o demostrarse implícitamente. Entre las normas a las que recurre el juez para determinar la ley aplicable en caso de litigio figura la lengua en la que se redactó el contrato, la moneda en la que se efectuará el pago, la nacionalidad de las partes contratantes, el lugar de celebración del contrato o el lugar de su entrada en vigor.

- Se critica al legislador jordano por limitarse a estipular que el ámbito objetivo de aplicación de la ley son las transacciones realizadas por medios electrónicos, mientras que el legislador iraquí tocó el ámbito personal en el contexto de su presentación del ámbito objetivo de las transacciones electrónicas al estipular que una transacción electrónica la realizan personas físicas o jurídicas, como fue el caso. El predominio de la voluntad estuvo presente al explicar el ámbito objetivo de la legislación iraquí. Explicó que la aplicación de las disposiciones de la ley incluye las transacciones que las partes acuerdan realizar por medios electrónicos, además de que la legislación iraquí incluyó los valores financieros y comerciales electrónicos en el ámbito objetivo de aplicación de la ley, y estas cuestiones fueron pasadas por alto por el legislador jordano y no las estipuló. El estudio sugiere que el texto del legislador iraquí a la hora de determinar el ámbito objetivo de las transacciones electrónicas era más exhaustivo y general que el texto del legislador jordano.

- Los datos personales en las transacciones electrónicas son un derecho digno de protección jurídica. El derecho a la intimidad ha sido reconocido tratados internacionales y constituciones nacionales de los países. El llamamiento a desarrollar una legislación global unificada para tratar las transacciones electrónicas choca con la realidad de criminalizar algunas transacciones en unos países y considerarlas permisibles en otros. Tanto la legislación jordana como la iraquí prevén la protección jurídica de los datos personales de los individuos mediante una legislación especial para las transacciones electrónicas, debido a la incapacidad de la legislación tradicional para ofrecer esta protección.

- La legislación para las transacciones electrónicas pretende proteger la información de los peligros de los medios electrónicos y disuadir a cualquiera que pueda caer en la tentación de utilizar esta información ilegalmente.

- Los datos financieros se consideran datos personales merecedores de protección jurídica. La amenaza que pesa sobre los datos financieros es mayor que la que pesa sobre otros datos personales. Existen muchas y variadas formas de amenaza para los datos financieros, desde la piratería electrónica al phishing, pasando por la penetración de vulnerabilidades y la descodificación de códigos, la captura de sitios web y muchas otras. Los datos financieros han recibido la protección jurídica necesaria tanto en la legislación jordana como en la iraquí debido a la importancia de proteger estos datos.

- El contrato electrónico es un contrato caracterizado por su carácter consensual, no por su carácter de adhesión, ya que el medio utilizado en la contratación no cambia la naturaleza del contrato, y la mayoría de los contratos son contratos consensuales, y los contratos de adhesión siguen siendo contratos de adhesión, tanto si se celebran por medios normales como por medios electrónicos, el medio utilizado en la contratación, la naturaleza y la realidad del contrato no cambian en modo alguno.

- Tanto la legislación jordana como la iraquí reconocen la autenticidad de las transacciones electrónicas, y se otorga a los contratos electrónicos la condición jurídica de contrato en el que ambas partes se comprometen con el contenido del contrato celebrado entre ellas por medios electrónicos. Para acreditar las transacciones electrónicas, deben cumplirse determinadas condiciones para que la firma electrónica de su titular quede probada, y deben concurrir determinadas condiciones en el registro o documento electrónico para que sea prueba en caso de desacuerdo entre las dos partes del contrato. Los efectos derivados de las transacciones electrónicas no difieren de los efectos derivados de las transacciones ordinarias, ya que el método utilizado para celebrar el acuerdo entre las partes no modifica en modo alguno la realidad del contrato.

- Los delitos electrónicos son delitos de naturaleza especial, pero para que de ellos se derive responsabilidad penal debe estar presente el elemento material, cuyo centro es la actividad técnica. Asimismo, debe estar presente el elemento intencional, que es la planificación y dirección del delincuente y la presencia de su intención de causar su delito en el entorno electrónico, conociendo que la ley lo tipifica como delito. También debe existir una relación causal que vincule su actividad técnica y su intención de causar el delito en el entorno electrónico.

- La intención delictiva en el entorno electrónico se basa en tres casos: a) si el autor quiere conseguir un resultado derivado de su conducta delictiva, como por ejemplo si el autor entra ilegalmente en la página web sabiendo que este acceso es ilegal; b) si la intención es lícita, como por ejemplo si una persona envía un virus a otra a través de ordenadores, siendo la intención reducir la velocidad del dispositivo de la persona a la que se envía el virus, y este virus funciona para destruir el dispositivo; c) el caso de la gravedad del resultado delictivo, en el que una persona piratea el dispositivo de otra para obtener un archivo que contiene fotos personales de esa persona, luego lo publica, y junto con las fotos personales de esa persona hay datos financieros relacionados con ella.

- Se han encontrado muchas teorías para determinar el criterio de verificación de una relación causal. Estas teorías son las siguientes: a) la teoría de la equivalencia de las causas, que no puede aplicarse en el ciberespacio; b) la teoría de la causa directa: un ejemplo de ello en el ciberespacio es la incautación de los fondos electrónicos de una persona. Una contraseña débil no se considera la razón de la incautación de los fondos electrónicos, sino que el acto de robo se considera la causa directa de la incautación; c) la teoría de la causa adecuada, como si una persona envía un virus que se sabe que perturba el sistema del dispositivo sin destruirlo, pero después de enviar este virus, el dispositivo de esta persona se destruye. En este caso, la responsabilidad penal se limita a perturbar el sistema sin destruirlo.

- Uno de los delitos cometidos en la web es el delito de acceso ilegal o de sobrepasar el acceso autorizado sin realizar ningún cambio, así como el delito de acceso ilegal o de sobrepasar el acceso autorizado para borrar, añadir, modificar o piratear datos o información del sistema de información.

- El legislador jordano y el proyecto iraquí tipifican como delito la entrada ilegal o la superación de la entrada autorizada e imponen multas y penas privativas de libertad por este delito. El delito se agravará si perjudica a la seguridad nacional, las relaciones exteriores, la seguridad pública o la economía nacional.

- El legislador jordano y el proyecto de ley iraquí tipificaron como delito el acceso ilegal o la superación del acceso autorizado para borrar, añadir, piratear o modificar datos o información del sistema de información. El delito se agravará si su finalidad es la transferencia de dinero o está relacionado con servicios de pago electrónico o cualquiera de los servicios financieros prestados por bancos y empresas financieras.

- La responsabilidad penal consiste en castigar penalmente a una persona por el delito que ha cometido aplicándole las normas del derecho penal. La responsabilidad penal en el ámbito de las transacciones electrónicas recae sobre el proveedor de servicios en dos casos: a) el caso de ser cómplice de un ciberdelito cometido por una persona en Internet; b) si tiene conocimiento del contenido electrónico y permite su difusión.

- El enfoque europeo define al proveedor de servicios como toda persona física o jurídica que presta un servicio de Internet en la comunidad de servicios de información. Tanto la legislación jordana como la iraquí son criticadas por no definir al proveedor de servicios electrónicos.

- Las obligaciones más importantes del proveedor de servicios en materia de responsabilidad punitiva son las siguientes: a) informar a las autoridades en caso de publicar información relacionada con una amenaza para la seguridad nacional o económica del Estado o publicar material pornográfico; b) obligación de los proveedores de servicios electrónicos de respetar el derecho a la intimidad y la confidencialidad de la correspondencia; c) los proveedores de servicios electrónicos deben controlar la información que constituya un delito que amenace la seguridad y la protección del Estado; d) compromiso de bloquear sitios web, enlaces o contenidos informativos a petición de las autoridades investigadoras y del tribunal.

- Existen tres tendencias a la hora de determinar la responsabilidad penal del proveedor de servicios electrónicos, que son las siguientes: a) la primera tendencia: Dice no imponer responsabilidad penal a los proveedores de servicios electrónicos porque es imposible que los proveedores de servicios controlen toda la información a través de Internet, además de que su trabajo es un trabajo técnico; b) la segunda tendencia: Pide que se imponga responsabilidad penal a los proveedores de servicios

electrónicos, considerando que la falta de determinación de la responsabilidad conduce a una mayor difusión de la información electrónica ilegal; c) la tercera dirección: Señala que la responsabilidad penal se impone al prestador de servicios electrónicos En tres supuestos: i) el primer supuesto si se demuestra que es fuente de información y datos ilegales; ii) El segundo supuesto: el caso de que no deje de difundir contenidos ilegales a pesar de tener conocimiento de ello; iii) el tercer supuesto: Si se niega a cooperar con las autoridades si se le pide que lo haga.

- La protección penal no se limita al aspecto sustantivo de las transacciones electrónicas, sino que esta protección se extiende también al aspecto procesal. En 2008 se creó en Jordania la Unidad de Ciberdelincuencia, adscrita al Servicio de Seguridad Pública. Se trata de una unidad especializada en la persecución de delitos electrónicos. Está formada por un grupo de especialistas en el seguimiento de delitos electrónicos. Esta unidad utiliza herramientas avanzadas, además de solicitar la ayuda de empresas de telecomunicaciones que prestan servicios de Internet. Esta unidad trabaja para indagar, investigar y perseguir los delitos que se producen a través de Internet. En Irak existe un departamento denominado Departamento de Control de Delitos Electrónicos, adscrito a la policía iraquí.

- La competencia de la policía judicial en la fase de investigación e instrucción se limita a dos materias: recepción de denuncias, querellas y vista previa. La jurisdicción de la misión de inspección en los delitos electrónicos se limita a la unidad de delitos de información ubicada dentro del estado y por orden judicial, cuyo trabajo es investigar los delitos electrónicos que se producen dentro de las fronteras del estado a través de Internet, y el alcance de la inspección no es limitado, sino más bien amplio para encontrar a todas las personas que contribuyen a la investigación. delito, aunque se trate de una contribución menor. Uno de los métodos especiales de lucha contra los delitos electrónicos consiste en interceptar la correspondencia, grabar las votaciones y tomar fotografías. La protección procesal en la fase de juicio consiste en limitar el ámbito de asistencia al juicio derivado de un ciberdelito, ya que sus sesiones no son abiertas, lo que da una especie de protección a la persona del autor.

- Surgió una controversia jurisprudencial sobre el conflicto de competencias judiciales en relación con el delito de información criminal. La jurisprudencia se dividió en tres tendencias: la doctrina de la actividad delictiva, la doctrina de la obtención del resultado y la doctrina mixta.

- Las pruebas electrónicas se definen como pruebas obtenidas de ordenadores y en forma de impulsos electromagnéticos o eléctricos que pueden recogerse y analizarse utilizando programas, aplicaciones y tecnología especiales y pueden presentarse en forma de pruebas homologables ante el tribunal. Los procedimientos modernos de control de las pruebas electrónicas se llevan a cabo mediante la incautación,

interceptación o vigilancia de las pruebas electrónicas. Los medios de prueba, incluidos los medios de prueba electrónicos, se consideran entre los medios más importantes a los que el legislador o regulador debe prestar atención en diversos países del mundo debido a las consecuencias de estos medios a la hora de probar los derechos y obligaciones entre los miembros de la sociedad en sus diversas posiciones jurídicas.

Research Objectives and Research Methodology

RESEARCH OBJECTIVES AND RESEARCH METHODOLOGY

RESEARCH OBJECTIVES

Study hypotheses

Main hypothesis: criminal protection helps preserve electronic transactions.

Sub-hypotheses: In light of the main hypothesis, the researcher derived the sub-hypotheses, which are:

- The first hypothesis: The legislative systems are appropriate to protect electronic transactions.
- The second hypothesis: All forms of assault on electronic transactions.are subject to legal texts.
- The third hypothesis: The existing legislative solutions are considered sufficient to confront various forms of attacks on electronic transactions.
- Fourth hypothesis: Legislative texts related to the criminal protection of electronic transactions. Achieve a balance between the interests of transactions. Authors and other conflicting social interests.

Objectives of the study

The most important objectives of the study are the following points:

- Identifying criminal protection, its legal concept, and its nature in protecting electronic transactions from any harm.
- Identify all forms of assault on, electronic transaction and texts criminalizing and punishing or causing any harm to electronic transactions.

- Identify the existing legislative solutions to confront various forms of attacks on electronic transaction, and whether they are sufficient to preserve the rights of transaction owners, as well as protect electronic transactions.

- Identifying the legislative texts related to the criminal protection of electronic transaction with the aim of balancing the interests of transaction authors with other social interests that conflict with them, with the aim of protecting electronic transactions and preserving them from theft, hacking, damage or loss.

Study problem

The great abuse of electronic transactions and the illegal use of these tools made the researcher interested in the problem, and from here the problem of the study stems from the many uses of electronic means and their tools, as the researcher sensed the problem, which is what criminal protection is in light of electronic transactions.

The clear legislative deficiency that exists in Iraq, especially the failure to ratify the Iraqi electronic crime law, which is still rejected by the Iraqi Council of Representatives until this moment.

Study questions

The study answers a main question:

What is the criminal protection for electronic transactions?

From this, the sub-questions emerged:

- Are the legislative systems to criminally protect electronic transaction consistent with the legal nature of these transaction?

- Are all forms of assault on electronic transaction subject to criminalization and punishment provisions?

- Are the existing legislative solutions to confront various forms of attacks on electronic transaction sufficient to protect the rights of these transactions owners?

- Do the legislative texts related to the criminal protection of electronic transaction achieve a balance between the interests of electronic transaction authors and other social interests that conflict with them?

Importance of studying

The importance of the study was noted in the following points:

- The study contributes to ensuring criminal protection for electronic transactions, which leads to ease and speed of completion of commercial transactions and saving expenses.

- Electronic transactions have a close relationship with the right to confidentiality and privacy, and are also related to the protection of consumer rights, as they crystallize the rights of the two parties to the contract, as it is considered the reference for determining what the two parties agreed upon and determining their legal obligations, and the protection established for electronic transactions and at the same time guarantees protection for the consumer.

- Protecting electronic transactions leads to achieving stability and legal security. Protecting the electronic document, whether in terms of form or signature, protecting it from compromising its confidentiality, and revealing its content guarantees individuals reassurance and stability of transactions, and also leads to this document becoming evidence that stands on an equal footing with The paper document, which ultimately leads to the stability of the legal system and the lack of disputes.

Study tools

Legal texts, regulations, legislation and international documents related to the subject of study, especially Jordanian legislation and Iraqi legislation.

METHODOLOGY

Comparing laws is an ancient approach, as Aristotle compared 153 constitutions of Greek cities, and this comparison was the subject of his book “Politics.” Comparing customs also helped establish a unified civil code in France in 1804. Montesquieu also strove to extract the principles of good governance through comparison when He wrote his book "The Spirit of Laws" in which he compared political systems and classified them on the basis of the ways in which power is assumed and actually exercised

Comparative law is the science that deals with the comparative study between the main global legal systems, each of which includes a set of laws, with the aim of extracting common general origins between legislation and the differences between them in concepts, ideas and methods of legal drafting, and identifying the factors that influenced the emergence of each legislation. So that it has its own and distinctive character compared to other legislation, and in our study it became clear that the Iraqi Cybercrime Law was not ratified and that political reasons and sectarian differences led to its non-ratification.

The comparative approach enables one to know the national law well and demonstrate its originality and specificity. It also enables one to know its flaws and disadvantages and try to improve it. It also helps to imagine proposals for reforming and amending national legislation and clarifying the solutions contained therein, and in various legal systems by identifying and understanding the laws of various countries. It helps to develop international relations and prepare bilateral and multilateral agreements with the aim of legal and judicial cooperation. This was done in our study, where the shortcomings in Jordanian and Iraqi legislation were identified, as well as the issues that affected legislators, and this was pointed out, in addition to that in some places a comparison was made with legislation. Western, such as the Spanish, American, and European agreements. The recommendation to establish a unified global law to govern electronic transactions also appeared in this study, and the extent of the need for this recommendation was demonstrated through the use of the comparative approach in the study.

The comparative approach in the legal field deals with social and economic phenomena and facts and the legal rules that govern them. It necessarily aims to compare the legal rules that govern the same facts in different legal systems for the purpose of revealing the reasons for their emergence, development and the relationship between them.

Comparative law is currently considered an independent, self-contained science. It is necessary in historical or philosophical studies and research on law. It has its own goals, as comparative law jurists approach the legal systems being compared.

The analytical approach is also defined as dividing the elements of the study, studying each part of it, and commenting on each part, especially since the nature of the study is related

to legal texts, so it was necessary to use the analytical approach and explore the shortcomings in its formulation.

The use of the analytical method in the study was demonstrated through criticism of some legal texts, sometimes praise and interpretation of some texts, and sometimes also giving recommendations.

It is also necessary to point out the inductive approach, which is through studying a case and trying to reach answers to questions and aims to judge a specific piece of legislation and study studies related to this case.

- Based on the above, the study relied on the following research approach because these approach serve the subject of the study:

The comparative approach between Jordanian legislation and Iraqi legislation, and in some places Western legislation such as Spanish legislation and European agreements that regulate the issue of criminal protection for electronic transactions:

- The analytical approach to describing the situation, analyzing the content, diagnosing the problem and presenting it from all aspects.
- The inductive approach by referring to literature, research, studies, cultural bulletins, and university dissertations that are directly related to the subject of the study.

Introduction

INTRODUCTION

Modern technology makes it possible to do many things that were previously impossible to do. One of the things that technology has provided in the field of electronic communications is the possibility of achieving human communication and completing transactions with ease. Its use has made it possible to improve the provision of health care services, develop intellectual property, and other fields.

Information networks and electronic data interchange systems are an application of modern technological use in the field of communications and information transfer, and thus differ greatly from other traditional means of communication and media. This difference leads to two things: the first is the multiplicity and breadth of uses of these means, and the second is the need for legal regulation. It sets the framework for these uses, but this technology may be misused by threatening the national interest and the private interests of individuals. If modern means of electronic communication allow financial transactions to be completed quickly; The use of these methods is not without risks, as some criminals may exploit these methods to commit their crimes by fraud or compromising the privacy of these customers and the confidentiality of their transactions. If technical progress has attempted to combat crimes in the field of communications and has resorted to encrypting them in a way that preserves their confidentiality, these measures have led to perpetrators exploiting these established criminal procedures.

Terminology of Study

The scientific concept of computer programming: A computer program is defined as: “a list or series of commands placed in a specific order and in a special way to implement a solution or treatment of a problem. It is a written product resulting from the programming process.” In another definition, it is “successive instructions that describe the work required to be accomplished by the computer.”

-The concept of protection: Protection is a phrase composed of the words: protection, criminal, and therefore each word must be explained separately. As for protection, in language, from the verb (protection), it is said that he protected something so-and-so, and protection and protection: prevented him and defended from him, and it is said that he protected him from the thing and protected him from the thing. Protection also means a precaution that is based, as it responds to whoever protects it or what it protects, and the observer in general is a duty to the one who insures it to protect a person or property against

risks and ensure its security and safety through legal or material means. It also indicates both the work of protection and its system (measure, system). "It means prevention."

Brocedural Definitions

These definitions are from the researcher's point of view and are as follows:

-Electronic transactions: Electronic transactions are transactions that are concluded or implemented, in whole or in part, by electronic means or records. - Or it is a form of integrated use of all information and communications technologies, provided that the purpose of this combination is to facilitate and accelerate financial transactions, while ensuring high accuracy.

1- Al-Harash, Abdul Rahim (2005) study entitled "Criminal Protection for Computer Programs" is a comparative study. Amman Arab University.

This study aimed to identify the means of special protection for moral programs, work to preserve documents, papers and papers in light of the law, work to detect their forgery or theft, or work to change their features.

This study dealt with criminal legal matters in working to preserve electronic programs, as computer programs are considered intellectual works in accordance with the Jordanian Copyright Protection Law and the prevailing trend in comparative legislation. This trend is consistent with the nature of the program as it represents ideas that are expressed, and is consistent with obligations. International law under the TRIPs Agreement, which obligates member states to protect the program as an intellectual work.

A computer program can also be protected based on patent law, in addition to protecting it as an intellectual work in cases where the conditions for this protection are met, especially in light of legislation that does not require the availability of an industrial characteristic, such as American legislation, or legislation that takes a broad interpretation of this condition, such as Jordanian legislation. Computer programs are considered Movable intangible property in accordance with the Jordanian Copyright Protection Law. However, the data and information included in the program copy are considered moveable material property, and this result may pave the way for protecting it from the most important forms of assault within the scope of crimes against property.

Shams El-Din Tawfiq's study entitled "Criminal Protection of Electronic Documents".

This study aimed to identify crimes related to electronic transactions, and it is a study in Egyptian legislation, and since the consumer, while requesting goods and services via the Internet, or modern electronic media, enters into various electronic contracts with the professional, which includes all the legal conditions of offer and acceptance. And the place and cause, which generates obligations falling on the parties to it, which need to be written or recorded in the form of a document or document that is signed by the signatures of its parties in order for it to be authentic and produce its legal effects.

In view of the confidence and security that the electronic document provides to the consumer in electronic commercial transactions, the preservation of rights, and the clarification of obligations, comparative legislation has given it great importance, stipulated its regulation, given it legal authority, and provided it with the necessary criminal protection.

1

Electronic transactions

1. ELECTRONIC TRANSACTIONS

1.1 INTRODUCTION.

The age at which we live is called the era of speed, due to the great changes that the information revolution has brought about, making the world more like a small village, even if its diameters are in fact far apart, it has converged in the virtual world, through the web one can access many websites and perform many electronic transactions in record time and since that many electronic transactions are nodal in nature it was necessary to provide it with legal protection so that those dealing with these electronic means would not be subject to fraud. Hence, many countries have enacted legislation aimed at protecting electronic information. Jordanian legislators were not immune to this, so they enacted the electronic transactions law, which aims to provide legal protection for electronic transactions in both civil and criminal cases.

1.2 DEFINING ELECTRONIC TRANSACTIONS.

Transaction or almueamala in Arabic language : Eayn (the first letter) Mim (the second letter) and Lam (the third letter) one correct origin, which is general in every verb that serve it's intend, and it is the singular of mueamalat (transactions) which is derived from the verb eamala (treated) , meaning the language of dealing, and it is intended to behave from and toward selling, and treat the man in a way that bargained him at work [1] .Electronic in language: it's plural is electronics, derived from the electron from which the atom is composed and used when speaking to the virtual world by networks and means, an electronic network and an electronic device [2].

---

[1] Ibn Manzoor (1968), *Lisan Al-Arab*, Dar Seder for Publishing and Distribution - Beirut - Lebanon, 1st edition, page 474 The Arabic Language Academy in Cairo (1960), Al-Mojam Al-Waseet, Al Shorouk international Library for Publishing and Distribution – Cairo – Egypt, 1st edition, p 43.

[2] Omar, Ahmed Mukhtar (2008), , p 248.

1.2.1 Technical Definition of Electronic Transactions.

Electronic transaction is technically defined as: one of the use patterns and full use of all communication techniques and technologies in order to facilitate and accelerate transactions.[3] It has also been defined as processes through the automated data processing system, which is the basic method for performing various electronic transaction in order to ensure that there is an assault of electronic transaction data rules, there must be an automated treatment of the data associated with this type of transaction[4].

It is also defined as a component that is composed of a unit or a number of electronic processing units, which consist of memory, programs, data, input and output devices, and linking units that link the output devices with the input devices through a set of relationships through which a specific result is achieved for data processing, provided that this the component has a kind of technical protection [5]

1.2.2 Legal Definitions of Electronic Transactions.

Here we will study the issue of the legal definition of transactions by studying the legislation of more than one country and how the definition of electronic transactions was addressed.

The Jordanian Electronic Transactions Law No. (15) Of 2015 defines in its second article electronic transactions as transactions that are executed by electronic means. While transactions are defined as any procedure that takes place between one or more parties to create a one party obligation or a mutual obligation between two or more actors, whether this procedure is related to a commercial civil business or is with the government department[6] .

While the Iraqi law defines electronic transactions: applications, documents and transactions that are carried out by electronic means[7]. While the Syrian law defines transactions: a procedure or a set of procedures that take place between two or more parties that have a civil, commercial or administrative nature. And define electronic transactions: transactions carried out by electronic means[8]. As for Qatari law, it defines electronic transactions: any transaction, contract, or agreement that is concluded or executed, in whole

---

[3] Hashmi, Muhammad Ali Qasim (1993) , p 10.

[4] Hijazi, Abdel-Fattah Bayoumi (2001), p. 34

[5] http://www.mohamoon.com/montada/Default.aspx?Action=Display&ID=106198&Type=3
http://www.nabdh-alm3ani.net/nabdhat/t33913

[6] Article No. (2) Of the Jordanian Electronic Transactions Law No. (15) Of 2015.

[7] Article No. (1) Of the Electronic Signature and Electronic Transactions Law No. (87) Of 2012.

[8] Article No. (1) Of the Electronic Signature and Electronic Transactions Law No. (87) Of 2012.

or in part, through electronic communications[9]. As for the Kuwaiti law, it defines the electronic transaction: any transaction or agreement that is concluded or implemented in whole or in part by means of electronic means and correspondence[10]. While the UAE Federal Law defines the electronic transaction as any transaction, contract or agreement that is concluded or implemented in whole or in part by means of electronic correspondence[11]. As for Moroccan law, it defines electronic transactions as electronic transactions: any exchange, correspondence, contract, document, or any other transaction concluded or executed electronically, in whole or in part; As for the electronic method: every method associated with a technology that has electrical, digital, magnetic, wireless, optical, electromagnetic or any other similar capabilities [12].

And from our presentation of these definitions, the researcher finds that the most comprehensive of these definitions was the definition of the Moroccan legislation, as it considered correspondence, contracts, documents, and any transaction concluded or implemented by electronic means as an electronic transaction, whether the implementation of this transaction was done in whole or in part, and he defined it electronically in detail, which other legislations omitted. The electronic method is every means associated with technology that has electrical, digital, magnetic, wireless, optical, or any other similar capabilities. The transaction that takes place via a mobile phone is an electronic transaction, the transaction that takes place via a computer is an electronic transaction, and the transaction photographed on a photocopier is an electronic transaction. Thus, electronic transactions vary according to this definition.

1.2.3 Jurisprudential Definition of Electronic Transactions.

Since the issue of electronic transactions has emerged recently, it was necessary for jurisprudence to have an opinion on it, as we will analyze the jurisprudential opinions that were researched to define electronic transactions.

Some jurisprudence has defined electronic transaction: a pattern of transactions that take place via the Internet and are inclusive of parties, whether two or more parties, and this transaction varies according to the diversity of its essence. This kind of transaction has a diversity of parties to it[13]. While another aspect of jurisprudence defined it as transactions that

---

9 Article No. (1) Of the Qatari Electronic Commerce and Transactions Law No. (16) Of 2010.

10 Article No. (1) Of the Kuwaiti Electronic Transactions Law No. (20) Of 2014.

11 Article No. (1) Of the UAE Electronic Transactions and Commerce Law No. (1) Of 2006.

12 Article No. (1) Of the Electronic Transactions Law No. (20-43) of 2020.

13 Rashida, Booker (2017), p 34

take place through electronic means in whole or in part, and electronic means may be electric, magnetic, optical, or any other means suitable for exchange between dealers[14].

While another aspect of jurisprudence tended to define electronic transactions by saying that it is the completion of business and the conclusion of contracts through an electronic format, and it also includes all activities and works related to the exchange of data and information, as well as goods and services via the Internet between consumers and companies or between companies with each other, and it represents the parties to the contractual relationship in E-business environment[15].

Perhaps this definition is considered one of the most comprehensive definitions to explain what electronic transactions are. It is a definition that includes contracts, business completion, and all activities and private works, whether it is an exchange of data and information, or an exchange of goods and services, as long as these activities take place through electronic means.

1.3 THE PROS AND CONS OF ELECTRONIC TRANSACTIONS.

In light of the rapid spread of technology and its entry into all aspects of life, and it has become affecting the interests of individuals and institutions negatively and positively, there must be negative and positive aspects of it. And this will be discussed under these headings.

1.3.1 Advantages of Electronic Transactions.

1.3.1.1 Breaking Geographical Boundaries.

With the existence of technology and the transformation of transactions into electronic transactions, it became possible for individuals in two warring countries at the political level to communicate and deal electronically via the Internet[16]. Electronic transactions are characterized by the lack of material presence of the contracting parties in one place, as one of the contracting parties may be in Jordan and the other in Australia[17].

The electronic transaction does not recognize the spatial boundaries, as it penetrates the political boundaries. Technology has made the world a small village, so anyone in any place in the world can conduct a transaction with others in another place. A person may reside in

---

[14] Al-Roumi, Muhammad Amin (2004), p 49.

[15] Al-Hadithi, Ali Khalil Ismail (2011), p. 66.

[16] Abd al-Hamid, Tharwat (2001), p 43

[17] Khaled, Kawthar Saeed Adnan (2012), p 394.

the east of the world, while the other may be in the west of the world. Contracting, signing, paying, all of this is done by electronic means[18] . In electronic transactions, there is no material presence of the two parties to the transaction or contract in one place, but rather the will of the contract is expressed through electronic devices[19].

1.3.1.2 Achieving the Principle of Abundance.

The electronic transaction is an issue that does not recognize the place .Because the electronic transaction penetrates the spatial boundaries, it at the same time shortens the time limits as well as the effort and the cost. The electronic transaction takes place in a very short time and does not require a high cost, unlike regular transactions that may require movement or travel and require higher material costs and require a lot of effort[20].

Through electronic transactions, effort, money and time are saved for individuals. It is known that the speed of the Internet is very fast until it reached more than seventy megabytes per second. As for paper transactions, they may take days, weeks or even months from their parties in order to complete them in addition to He pointed out that it is possible for the parties to the transaction to incur money that can be dispensed with if this transaction is electronic, and this is one of the reasons that prompted many institutions to convert their paper transactions into electronic transactions in many countries of the world[21].

1.3.1.3 Subject To the Provisions of International Law in Resolving Disputes in Some Cases.

The electronic transaction is characterized as cross-border where it is possible take place between two people of different nationalities, each residing in a country different from the country of the other, therefore the transaction may be subject to the provisions of international law[22].

1.3.1.4 Reliance on Electronic Means of Proof.

It is natural that the methods of proving the electronic transaction differ from the normal transaction due to the different nature between them. it adopts electronic means of proof, such as the electronic signature and the exchanged electronic messages. If a legal dispute arises between two contracting parties, the establishment of evidence is available to

---

[18] Badr, Osama Ahmed, (2005), p 37

[19] Qadri, Fella (2017), p. 172.

[20] Ahmed, Amanj Rahim, (2006), p 48

[21] Suleiman, Abdullah (2006), p 2.

[22] Makhloufi, Abdel-Wahhab, (2012), p 59.

both parties by all ordinary and electronic means of proof, however, in order for the electronic means to be a source of proof in the electronic transaction, many legislations stipulated the possibility of verifying the identity of the person using the electronic means[23].

1.3.1.5 Achieving Interaction Between Individuals, Institutions And Countries.

Technology has not only broken down geographical borders, but has also expanded the scope of transactions that happen between real and legal persons, so that there are many electronic transactions that combine between a state and an individual, or an individual and a banking institution [24].

1.3.1.6 Create A Healthy Dimension.

Electronic transactions are healthier than paper transactions, especially in the era of Corona, which requires us to strive to reach health by many measures such as social divergence, which is already achieved in electronic transactions, unlike paper transactions, as electronic transactions do not require the presence of a person in the place of the transaction, but rather He can be treated while sitting in his home, away from mixing and overcrowding, unlike paper transactions that require their owners to be present at the place of the transaction in order to complete it, which causes overcrowding that amounts to not maintaining social distancing, which helps the Corona virus to spread [25].

Likewise, the electronic transaction activates the movement of digital money, which spread recently when the Corona virus appears, and this money in its use limits the spread of the Corona virus, because the use of paper money may very well be the cause of the spread of this virus through its circulation among people, which means the possibility Infection of individuals with this virus, which is contrary to what the countries of the world and the World Health Organization aim at, as the process of circulating paper money contributes to the spread of the virus [26].

1.3.1.7 Giving People With Special Needs The Ability To Carry Out Many Transactions Electronically, Equal To Normal People.

Electronic transactions have been able to serve people with special needs and the disabled more than others, due to their special circumstances and the difficulty of their

---

[23] Youssef, Amir Farag (2008),, p 44. Gharib, Zainab Abdel-Razzaq (2015), p 174 And Al-Basharatan No. 16, p 101

[24] Abdel-Hamid, Tharwat (2001), , Egypt, p 43.

[25] Al-Ayeb, Samia (2020), Volume 5, p. 35

[26] Siham, Musa (2020), Volume 4, p. 129.

movement and mobility, so that they can, in light of electronic transactions, complete their transactions without hardship, effort and trouble, as happens under paper dealing[27].

1.3.1.8 Electronic Dealing Is One of the Criteria For the Progress And Development of Countries.

Also, the country that deals electronically is a country that seeks to reach advancement and progress at the scientific and technological level, which makes it an important and prominent name among the countries of the world[28].

Through the foregoing, we extract many advantages of the electronic transaction, as it is a transaction that does not recognize geographical borders and works to save effort, time and money. It also takes into account health dimensions and is one of the criteria for the progress and sophistication of countries and the fact that the electronic transaction is subject to electronic means of proof. International law may be applied to the electronic transaction if the two parties to the transaction resided in two different countries and had two different nationalities, and it also made the legal positions equal between the parties, individuals and institutions.

1.3.2 Disadvantages of Electronic Transactions.

One of the disadvantages of electronic transactions is that exposure to fraud is greater than fraud in regular transactions. Electronic fraud is behavior related to computers, and the intention of the perpetrator through this behavior is to achieve illegal financial profit[29]., Impersonation process is a form of electronic fraud so it can take a false name or an incorrect capacity, and the aim is to obtain a certain economic benefit[30].

Among the defects that surround electronic transactions is electronic fraud, which is wider in scope than fraud in ordinary transactions. Also, fraud in ordinary transactions is domestic in scope, while electronic fraud may be domestic or international in scope. Therefore, when electronic dealings, the user must be sure of the fact that the site and the goods exist or the service as well, he must ascertain the legitimacy of what is presented on the site in terms of ownership of its materials[31].

---

27 Saad, Ahmed Mahmoud (1995), p. 50-51

28 Saad, Ahmed Mahmoud (1995), p. 50-51

29 Al-Moumni, Nahla Abdel-Qader (2007), p. 188.

30 Al-Issawi, Youssef Mazhar (2020), Volume 4, Issue 3, Part 2, p. 236

31 Al-Moumni, Bashar Talal (2003), p. 32.

In addition, the occurrence of a mistake and a large number of defects in electronic transactions, the offer of the commodity may be incomplete or characterized by lack of clarity or inaccuracy, which causes great difficulty if the claim is made by mistake, since the proof is difficult. The offer is made through a page on the Internet, and it is easy to change or replace it after that by electronic means[32].

The perception of coercion is also one of the defects surrounding the electronic transaction. An electronic form may be sent on the page of the buyer, through which this form will be informed of the terms of the contract. With the principle of consensual contracts, the seller may take a means to force the buyer with the goods or service[33].

1.4 THE ORIGIN AND DEVELOPMENT OF ELECTRONIC TRANSACTIONS.

Man, since the beginning of his existence on this earth, was in need of finding a language to communicate between him and his fellow human beings and groups, and man has striven to create this communicative language, so he invented writing in the stone ages, and then these means developed little by little with the passage of time until they reached to what it is today from the introduction of technology and the revolutions and transformations it caused in the field of communication more than it was the case in ancient times, as a person could only communicate with the people around him and those close to him, and then the communicative language developed at the geographical level, offset by a disruption of communication at the level that the personal communication of individuals was between each other, but technology made them communicate with countries and institutions. Technology broke geographical borders. Before the introduction of technology, there was a limitation and restriction of the movement of individuals in each country, which led to the difficulty of communication between two individuals in two different countries, or even to the complete absence of this communication. Especially if these two countries are in a state of war or a political dispute, and each of the two countries seeks to boycott everything that brings them together with the other country, so it was not way other than reconciliation between the two countries and restoring their relations to the communication of individuals in both countries[34].

In fact, the Internet was used in transactions from a relatively long time ago, that is, sixty years ago, and the use of this network was characterized by a military nature to carry out military transactions inside and outside the country, and this technology was the preserve of a few powerful countries familiar with the secrets of this network and the way it was used, such as America and the Soviet Union Britain and France, then these electronic transactions spread to most countries of the world, and with the geographical spread of this technology, there is a

[32] El-Gamal, Samir Hamed Abdel-Aziz (2006), p. 165.

[33] Al-Rashdi, Bisman Fathi (2008) p. 108.

[34] Raafat, Radwan (1999), p 35.

qualitative extension of the World Wide Web represented in its entry into many areas of life, including political, economic and social [35].

In the political field, countries have become able to complete many of their transactions electronically, and even in their relations with other countries, many of them have become electronically, which has achieved speed in completion and an abundance of effort and money[36].

On the military and security level, it has become possible to coordinate between military units in the event of war by electronic means, and as an example of the introduction of technology, security coordination in locating the person who wants to carry out a bombing operation. Through the electronic means that take place between the security services, this person can be located and arrested before carrying out his operation[37].

In the economic field, many economic institutions have websites and electronic services that save many customers the trouble of going to them. The electronic system also works to improve the movement of these institutions and their work. Electronic transactions have also expanded, so the buying and selling operations are done electronically, and the competition between markets has become electronic. Stores that deal electronically earn much more money than traditional stores that do not use technology. The Alibaba online store earns billions, and the same applies to Amazon, because these electronic markets cross geographical borders between countries, and electronic transactions have spread widely in the world, as they are no longer limited. States, authorities, and institutions, and not other people. Through the existence of markets, individuals are able to carry out buying and selling operations in a larger way in the virtual world than it is in the real world[38].

In the social dimension, there are social transactions between people through the web. Today, we see that there are social relationships that bring people together, which are done electronically, such as expressing condolences, congratulations, chatting, or what is known as chat rooms, all of which are done through social media [39].

The persons of electronic transactions differ according to their types. If these transactions are military or security, their persons are military or security institutions such as the armed forces, the intelligence apparatus, or the public security apparatus. And if these

---

35 Electronic services, a research published on the Internet on 7 / December / 2020, the date of the visit 19 / 11 / 2021.

36 1 – The Senate wanted to define a STAD as "any set composed of one or more automated processing units, memories, software, data, input-output and liaison devices which contribute to a determined result, this assembly being protected by safety devices » Rapp. J. Thyraud Doc. Senate 1987-88 n°3, page 52. 2

37 Rashida, Booker (2017), p 5. Al-Masirafi, Muhammad (2008), p 50.

38 Hegazy, Abdel-Fattah Bayoumi (2009), p 21.

39 Isabelle poitier,, 1996, p 4.

electronic transactions are of an economic nature, then their persons may be natural persons or legal persons usually represented in economic institutions, and as for electronic transactions of a social nature that are carried out through social media, their persons are mostly real persons from members of society [40].

In light of the global spread of these transactions on the Internet, there were increasing concerns about ensuring the right to these transactions, especially those that bring one person together with another, such as the buying and selling operations that take place through this Internet, in addition to the fear of the negative use of this network, both at the international level and which brings the state together. In other countries and persons of international law, such as organizations and people such as the UN Security Council and UNICEF, or at the internal level, which regulates relations between the state and individuals, or between individuals with each other. The negative use is mostly represented by either stealing data and financial or personal information in electronic transactions, and this is what many countries have mastered. Through its legislation, it sought to enact laws that regulate electronic transactions in order to establish confidence in these transactions in the hearts of people and eliminate the fear and anxiety lurking in their souls[41].

Among the countries that have pursued the enactment of legislation to protect electronic transactions, Jordan has enacted the Jordanian Electronic Transactions Law No. (15) Of 2015 and the Jordanian Electronic Crimes Law for a year Of 2023 AD. By surrounding these transactions with legal protection so that there is comfort in dealing with electronic transactions. Providing legal protection does not mean indifference on the part of individuals if the individual makes his passwords or financial information available to others because the law considers him in this case an idiot and the principle is that the law does not protect the dupes[42].

From the foregoing, it becomes clear to the researcher that electronic information and due to its wide spread, whether at the qualitative level or across the geographical extension, it was necessary for the intervention of international and domestic legislators to provide legal protection for these electronic transactions, especially since many of these transactions are considered cross-border

[40] Tawahir, Abdel Jalil (2012), Issue 2, p 98

[41] Al-Alfi, Muhammad (2008), p 144

[42] Ratib, Ahmed, Al-Sarayrah, Mansour Abdel-Salam (2008), Volume 23, Issue 5, p 84

1.5 CONCLUSION.

- The most comprehensive legal definitions of electronic transactions was the definition of the Moroccan legislation, as it considered correspondence, contracts, documents and any transaction concluded or executed by electronic means to be an electronic transaction. The transaction that takes place via a mobile phone is an electronic transaction, and the transaction that takes place via a computer is an electronic transaction, and the photographed transaction on the photocopier, it is an electronic transaction, and thus electronic transactions vary and multiply according to this definition.

- The most comprehensive jurisprudential definitions of electronic transactions, as it is defined as the completion of business and the conclusion of contracts through an electronic format. The parties to the contractual relationship in the electronic business environment. This definition is considered one of the most comprehensive definitions to indicate what electronic transactions are. It is a definition that includes contracts, business completion and all activities and private works, whether it is an exchange of data and information, or an exchange of goods and services as long as these activities take place through electronic means.

- One of the advantages of electronic transactions is that it breaks geographical borders, achieves the principle of abundance, is subject to the provisions of international law, relies on electronic means of proof, achieves the health dimension, and equality between ordinary individuals and those with special needs. Dealing with electronic transactions is one of the criteria for the progress and development of countries.

- The disadvantages of electronic transactions are that exposure to fraud is greater than fraud in ordinary transactions, and electronic fraud in electronic transactions is wider than fraud in regular transactions, in addition to the frequent occurrence of errors in electronic transactions, and the perception of coercion is one of the defects in electronic transactions

2

The Challenges Facing the Sovereignty of States Regarding Electronic Transactions and the Applicable Law

2. THE CHALLENGES FACING THE SOVEREIGNTY OF STATES REGARDING ELECTRONIC TRANSACTIONS AND THE APPLICABLE LAW

2.1 INTRODUCTION

Sovereignty is defined in the legal sense as: a characteristic of the characteristics that the state enjoys, and thanks to this characteristic, powers are formed in such a way that there is no higher authority than the authority of the state[43]. Since we are talking about digital (electronic) sovereignty, it is necessary for us to give a definition of this sovereignty. Digital sovereignty has been defined as: extending the authority of the state over digital space by regulating entry into this space and punishing those who break the legislation regulating this digital space[44].

Based on the foregoing, we will discuss the challenges facing the sovereignty of states regarding electronic transactions and the applicable law as follows: Electronic transactions between international and domestic.The applicable law in the event of a dispute

2.2 ELECTRONIC TRANSACTIONS BETWEEN INTERNATIONAL AND DOMESTIC.

Electronic transactions may take place between people or countries via the Internet, and they are either subject to the provisions of international law if they take place between countries, such as commercial transactions related to supplying one country to another country with a specific product. This transaction is subject to the provisions of international law, as each country has its own private sovereignty[45]. As for the transactions that occur between people via the Internet, they are subject to private law, whether it is the domestic law when they share the same country, as if there are two Egyptians who want to sign an electronic contract, here the Egyptian law regulates this contract[46]. Or that a law is applied to

---

43 Stripe, Al-Amin (2005), p. 75

44 Saadi, Muhammad (2013), p. 64

45 Moazeb, Abd al-Khaliq Saleh Abdullah (2019), p. 302.

46 Hammad, Tariq Abdel (2003), , p. 156

these transactions that the parties agree upon when their nationalities differ, such as if there is an electronic transaction between a Norwegian person and an Australian person, and they agree that this transaction will be subject to the provisions of Mexican law [47].

2.2.1 The International Framework for Electronic Transactions.

Most of the transactions are conducted via the Internet due to the speed and simplicity of this method[48]. Commercial transactions, like other things, required a lot of time, thinking, and effort to complete one transaction between two countries, as in the sales contract, for example, the buyer came from America to the seller in China to complete a commercial transaction, but at the present, commercial transactions are done through the Internet, so there is no need that the buyer leaves his country to complete a commercial transaction. Rather, it takes place through the Internet while he is sitting in his home or office through this Internet[49].

Article 1 of the UNCITRAL Law on Electronic Commerce ((This law was enacted through a committee established by the United Nations General Assembly with the aim of reducing obstacles to international commerce)). States: This law applies to any type of information in the form of a data message used in the course of commercial activities. However, the UNCITRAL Committee proposed the following provision for countries wishing to limit the application of this law to international data messages: This law applies to the data message as defined in Paragraph (a) of Article (2)[50], when the data message is related to international trade[51].

Many attempts have been made to define criteria for the law applicable to electronic transactions. Some have argued the need to find a unified objective law for electronic transactions, due to the special nature of the Internet, as it cannot be limited to a specific country whose law is invoked[52]. The electronic transaction is not restricted to a specific place due to the nature and privacy of electronic transactions. Therefore, the international dimension is what dominates the nature of electronic transactions, even if all its elements are met in one country[53].

---

47 Mostafa, Fahmy Khaled (2007) p. 82-83

48 Musa, Talib Hassan, p. 208

49 Yassin, Saad Ghaleb, Bashir Abbas (2006), p. 209

50 The aforementioned article stipulates the following: The term “data message” means information that is generated, sent, received or stored by electronic means

51 Article 1 of the UNCITRAL Law on Electronic Commerce 1996

52 Dannoun, Samir, 2012, p. 226

53 Salah El-Din, (2021) p. 35.

Electronic transactions are of an international nature and there are many applications for that. Through digital marketing, companies market their products to any place in the world. Since technology is cross-border, e-commerce is not defined by a specific geographical area, as goods or services can be offered through many websites in electronic space[54].

Some suggested the need to resort to international model contracts in electronic transactions, as these model contracts deal with many technical and legal issues that must be respected between the two parties, and are considered binding if the parties choose to deal with them explicitly or implicitly[55].

Some also went to consider the authority of the will, as the contract may be concluded between two parties residing in two different countries and holding the same nationality, or each of them may hold the nationality of the country in which he resides, and the two parties may agree to define a specific law, so the contracting parties have complete freedom in choosing the law applicable to The contracts concluded between them, and therefore the matter does not stop at the limits of internal law [56]

What is meant by the concept of the principle of the law of will is the recognition of the right of the parties to choose the law governing the contractual relationship concluded between them, The will is considered a control for attributing the law to be applied to this contractual relationship[57] The law of will is applicable in various legal systems, and this may be through an express clause in the contract, or through a subsequent agreement independent of the original contract[58].

In the field of law applicable to electronic contracts, some suggest concerted efforts at the international and regional levels in an effort to establish legal rules regulating these transactions, while ensuring that national rules are not circumvented, while observing legal and social systems[59].

However, the law of the will of the contracting parties faces difficulties in its application, especially in the case of an implied agreement, when it is difficult to determine

---

54 Hegazy, Abdel-Fattah Bayoumi, p. 22

55 Salama, Ahmed Abd al-Karim, 1989, p. 388

56 Manzolay, Salih, 2008, p. 272

57 Sylvette Guillemard, private international law facing the cyberspace sales contract, accessible on the site, http//:ww.these.ulalva.ca.

58 Salama, Saber Abdel Aziz, Electronic 2005, p. 87

59 Al-Jammal, Samir Hamid Abdel Aziz, 2006, p. 77

the direction of the will of the contracting parties in choosing the law that governs the contract[60].

In addition, one of the challenges facing the will law in electronic transactions is the issue of verifying the issuance of the will, the authority to dispose of the one from whom the expression was issued, and ensuring that the content of the electronic message is not tampered with, or that its content is not changed, in addition to the occurrence of malfunctions within electronic devices, which leads to the loss of stored data, and it will be very difficult to retrieve it, and this data is subject to manipulation [61].

2.2.2 The Domestic Framework for Electronic Transactions

In the domestic framework of electronic transactions, we find that they take place between two parties residing in the same country and belonging to the same nationality. The contract may be concluded between two parties residing in the same country, but each of them has a different nationality than the other.

If one of the dealers resides in one country and the other dealer resides in another country, then here the international law governing such an electronic transaction, but if both dealers in the electronic transaction reside in the same country and the transaction fulfills its elements in the same country, then here the law of the state is the ruler. On this transaction[62].

The law of the domicile of the contracting parties may be the applicable law, since the domicile law is the law that is recognized among the contracting parties more than others, except that in electronic transactions the real addresses of the parties may not be used, which does not give a clear indication of the real address[63].

In the case of a difference in the domicile of the contracting parties, the law of the country in which the contract was concluded applies, and this trend has received many criticisms because it entails the development of national solutions that were developed mainly for contracts concluded within a specific country, while electronic commerce contracts are dominated by the international character[64].

Some went to apply the criterion of the nationality of the contracting parties to the electronic transaction, but this criterion was criticized due to the difficulty of verifying the identity of the parties and their nationalities at the date of concluding the contract in electronic

---

60 Al-Ali, Youssef, ,2003, p. 238

61 Badawi, Bilal Abdel-Muttalib, 2003, p. 1972

62 Salah Al-Din, Kazan Zain Al-Abidin 2021, , Issue 1, p. 216. Moazeb, Abdel-Khaleq Saleh (2019), , p. 35.

63 Al-Hawari, Ahmed Muhammad, 1995, p. 155

64 Manzalawi, Applicable Law, p. 271

space, and in that contract, fictitious names may have been resorted to complete the electronic process[65].

In talking about the domestic framework for electronic transactions, this calls for an explanation of how both Jordanian and Iraqi legislation regulated electronic transactions. Commercial transactions must stem from a free will based on consent represented by offer and acceptance. And consent is the agreement of the wills of the two parties, meaning that the offer is converged by one of the parties with the acceptance of the other, in order to bring about the legal effect resulting from this transaction, and in order for the contract to be valid, it must be free from the defects of consent that the Jordanian Civil Law considered as defects represented in by coercion, error, and deception associated with outrageous unfairness[66].

The expression of the association of offer with acceptance in light of electronic transactions takes place through the electronic information message, and this is what was stipulated in the Electronic Transactions Law No. 15 of 2015 in Article 9 of it, which states: "The information message is considered a means of expressing the legally accepted will to express Offer or acceptance with the intent to create a contractual obligation. In Article 2 of the Electronic Transactions Law, the Jordanian legislator defined the information message as: "Information that is generated, sent, received, or stored by any electronic means, including e-mail, short messages, or any electronic exchange of information.[67]

The Jordanian legislator considered the information message as a means of expressing the legally accepted will to express an offer or acceptance with the intention of establishing a contractual obligation[68]. The electronic information message is the method of linking between the seller's will to sell the commodity and obtain money from the buyer in return for the delivery of the sold commodity to him, and the buyer's will, which is represented in buying the commodity that the seller has, owning it and paying the money instead of this possession of this commodity[69].

While the electronic information message was not defined in the Iraqi legislation, but the electronic contract was defined in Article 1 of the Iraqi Electronic Signature and Electronic Transactions Law No. (87) For the year 2012 as: linking the offer issued by one of the contracting parties to the acceptance of the other in a way that proves its effect on the contracted upon, which is done by means electronic[70].

---

65 Al-Manzlawi, Applicable Law, p. 333

66 Al-Otaibi, Muhammad Dhaar (2013), p. 52.

67 Article 2 of the Jordanian Electronic Transactions Law No. 15 of 2015.

68 Article 9 of the Jordanian Electronic Transactions Law No. 15 of 2015.

69 (Dudin, Bashar (2006), 1st Edition, p. 106.

70 Article 1/11 of the Iraqi Electronic Signature and Electronic Transactions Law No. (87) of 2012

As for the place where the offer is met with acceptance in the electronic transaction, it is the Internet, and as for the time of convergence of the two wills under this contract, it is the time of receiving the electronic message and its approval by the parties to the electronic transaction[71].

In order for the electronic transaction subject to implementation to be sound, there must be satisfaction or consent on the part of its parties to complete this transaction, and for satisfaction there are conditions, the most important of which is eligibility, if the parties to the transaction must meet the eligibility conditions, and eligibility conditions are to be the one who wants to conclude the transaction a sane adult should not be demented or young. If the electronic transaction is defective, then this transaction becomes defective and voidable[72].

However, there is a problem that may appear clearly in the light of electronic transactions, which is how to verify the eligibility of the two parties, the seller and the buyer, especially since this contract is concluded between absentees. Cause it may be that each of them is from a different country, A part of jurisprudence[73] in this case preferred the theory of the apparent case, that is, it is possible to distinguish one of the parties to the transaction, especially if the other party performs irresponsible behavior in this transaction, but if this party has fulfilled his will and he is aware of the signature of the electronic transaction, Meaning that both parties must be fully aware of their actions, so that they must both have full liability. Otherwise, the contract will be invalid [74].

With regard to the scope of application of electronic transactions, the Jordanian legislator did not overlook to specify the transactions to which the Electronic Transactions Law applies and the transactions to which this law does not apply.

The provisions of this law must be applied to all transactions that take place by electronic means. However, here the legislator excluded some transactions whose nature requires the opposite, and among thes:

Creating and amending a commandment. In addition to Creation of the endowment and modify its conditions .and Transactions of disposing of immovable and movable funds whose registration is required by legislation, including the agencies related to them, title deeds and the establishment of in-kind rights over them, with the exception of lease contracts for these funds .also Agencies and transactions related to personal status .aside from Notices related to the cancellation or termination of contracts for water, electricity, health and life insurance .as well services.Case regulations, pleadings, judicial notification notices, and court decisions.

---

71 Michel, Tony Issa 2010, 1st edition, p. 76.

72 Abu Aqleen, Ahmed Fawzi 2012, p. 41.

73 Abdel-Rahman, Khaled Hamdi 2008, p. 145. Abu Al-Haija, Muhammad Ibrahim (2017), , p. 101.

74 Idrisi, Rashida Muhammad 2005, p. 104.

Beside guarantees, except for what is stipulated in special instructions issued by the competent authorities based on the Securities Law or any other legislation[75].

When we go to the Iraqi legislator, we find that it is very similar to the Jordanian legislator, as he excluded some transactions from being applied electronically. While Article 3 of the Iraqi Electronic Signature and Electronic Transactions Law clarified: The provisions of this law apply to:

Electronic transactions carried out by natural or legal person's and.Transactions whose parties agree to implement them by electronic means .Securities and electronic trading.

Among the transactions that the Iraqi legislature excluded, and the provisions of this law do not apply to them:

Transactions related to personal status matters and personal items. Also creating a will and an endowment and amending their provisions .Moreover Transactions related to the disposal of immovable funds, including agencies related to them, their title deeds, and the creation of real rights over them, with the exception of lease contracts for these funds .inadditionTransactions for which the law drew a certain formality. Aside from Court procedures, judicial announcements, attendance announcements, search warrants, arrest warrants, and judicial rulings. And any document required by law to be authenticated by a notary public[76].

Through the foregoing, it is from my point of view that it is well done by the Iraqi and Jordanian legislators in that they excluded some transactions from being subject to the laws of electronic transactions, since the nature of these transactions has a certain privacy and must take place according to a certain formality

[75] Article 3 of the Jordanian Electronic Transactions Law No. 15 of 2015.

[76] Article 3 of the Iraqi Electronic Signature and Electronic Transactions Law No. (87) of 2012

2.3 THE APPLICABLE LAW IN THE EVENT OF A DISPUTE.

The attribution controls in private international law in the applicable law in the event of a dispute are not suitable for application to electronic commerce, as it depends on the spatial attribution control, and this is not compatible with electronic commerce, which is considered transitory[77].

As for the law of will, there was a disagreement among the jurists about the basis on which to choose the applicable will law, and this disagreement was embodied between the subjective theory and the objective theory[78].

The owners of the personal theory looked at the freedom of the individual, which they made a source of rights and obligations. They said that the parties have the right to choose the law in their contractual relations, based on the principle of the authority of will. They also said that there is no requirement for a relationship between the contract and the law of will. More aware of the law that will bring them safety, In addition, the contract applies to the provisions of the law in force at the time of his choice without being affected by the amendments that occur to the law thereafter. Arrows of criticism were directed to this theory because the will is not considered a source of rights except with legal authorization[79].

On the other hand, the objective theory is not based on the principle of absolute freedom in choosing the law that the contracting parties want to apply to their contractual relations, but rather it is based on the principle of attribution, which gives the will this right. Here, the law is applied as a law and not as a condition included in the contract. It is not permissible for the contracting parties to work to exclude peremptory legal provisions[80].

Electronic transactions that take place between countries via the Internet are subject to the provisions of international law, such as commercial transactions related to providing one country to another country with a specific product. This transaction is subject to the provisions of international law, as each of the two countries has its own sovereignty[81]. And as for the transactions that take place between people via the Internet, they are subject to private law, whether it is the domestic law when they share the same country, as if there are two Egyptians who want to sign an electronic contract, here the Egyptian law regulates this contract[82]. Or that a law is applied to these transactions that the parties agree on when their nationalities differ, such as if there is an electronic transaction between a Norwegian and an

---

77 Sadiq, Hisham, Issue 1, 2004, p. 20

78 Pierre Mayer, P 455

79 Suleiman, Ali Ali, 5th edition, 2008, p. 110

80 Yaqout, Muhammad Mahmoud, 2000, p. 95

81 Moazeb, Abd al-Khaliq Saleh Abdullah 2019, 1st edition, p. 302.

82 Hammad, Tariq Abdel-Al 2003, p. 156

Australian person, and they agree that this transaction will be subject to the provisions of Mexican law[83].

It has become necessary in electronic commerce contracts to include a clause that includes the applicable law that is most responsive to the requirements of the legal security required for dealing via the Internet[84].

Therefore, in this topic, we present to both cases, respectively, in the event of an agreement, what is the applicable law, and the other case in the absence of an agreement, and what is the applicable law in such a situation.

2.3.1 If There Is An Agreement.

There may be an agreement between the two parties to the electronic transaction about the law to be applied, which is called the law of the will, meaning that there is a convergence between the will of the two parties in choosing the law whose provisions apply to the electronic transaction, so the existence of an agreement between the will of the two parties is based on personal attribution, which is an original attribution rule That is, these two parties can assign the subject of the electronic transaction that they have collected to a specific law upon which their wills agree. The Jordanian law has recognized the rule of personal attribution, as stated in Article No. (36) of the Jordanian Arbitration Law: "A- The arbitral tribunal shall apply the legal rules agreed upon by the two parties to the subject matter of the dispute [85].

And the law of will is the law on which the will of the two parties to the transaction agree upon by meeting the will of the two parties on a law. It is possible that the applicable law in this electronic transaction is different from the law of the country in which the electronic transaction took place. For example, if the electronic transaction takes place in Sweden between a Chinese person and another Swede, then in this case the will of both parties, that is, the Swedish person and the Chinese person, is determined to choose the law whose rules govern this transaction, even if this law is not the Swedish law, given that Sweden is the country of conducting the transaction, so they can To choose French law, for example, if their will agrees with it, Therefore, we call the French law the law of will, meaning that it would not have existed in this case had it not been for the agreement of the will of the two parties to the transaction to choose its provisions and rules to apply to this transaction, and this process of selection means choosing the French law to apply its

[83] Mostafa, Fahmy Khaled 2007, p. 82-83

[84] Xavier van overmeire, vol 3, 2008, P4

[85] Article No. (36/a) of the Jordanian Arbitration Law No. (31) of 2001 AD and its amendments

provisions to this transaction that is between a Swedish person and a Chinese person Which occurred in Sweden, it follows a legal rule called the attribution rule [86].

The jurist Demolan justified the rule of attribution as an embodiment of the principle of will power on the one hand, and on the other hand it is an expression of the philosophy of individual freedom that he (Kant) established and that the French Revolution believed in, which led to the stability of the will law in many countries in the nineteenth century. The rule of the law of will in the contract that brings together the two parties has become a traditional rule advocated by many jurists such as Mancini and Santini, which led to its application in the judicial authority, and this necessitated that there be codification of this rule in order for the approval of the judiciary and its reliance on the provisions of law and legislation, and indeed this is what was The French state has codified it, as well as Egypt, which was the first Arab country to codify this rule [87].

It is also permissible for the two parties to the electronic transaction, if each one holds the nationality of a country different from the other, to agree on a specific law whose provisions and rules apply to this transaction,[88].

As for the Iraqi legislator, he was not far from the Jordanian legislator

Unless the two contracting parties agree otherwise or it appears from the circumstances that another law is intended to be applied, the contractual obligations shall be subject to the law of the state in which the co-citizens of the two contracting parties are located if they take a domicile, and if they differ, the law of the state in which the contract was concluded shall apply"[89].

The legal text emphasized the supremacy of the principle of the agreement of the will of the two parties, as the will plays a very important role in the process of choosing the law whose provisions and rules will be implemented on the subject of the electronic transaction. Nevertheless, it should be adhered to that there is nothing in the subject matter of the transaction that could disturb public order and morals within the country in which the subject matter of this transaction will apply[90]. The contract must not violate the general order in force within the country in which the subject matter of the contract will take place, such as the contract being an American person handing over to a Finnish person the amount of four million dollars in Jordan if he beats him in a gambling game in a public place inside Jordan, here this contract cannot be executed, This is because the subject matter of this contract is

---

86 Gul, Halima, Mayhoub, Ali 2020, , Issue 1, p. 52

87 Al-Masry, Hosni (2006), p. 342.

88 Article No. (20) Of the Jordanian Civil Law No. (43) Of 1976 AD and its amendments.

89 Article No. (25) Of the Iraqi Civil Law No. (40) Of 1951 and its amendments.

90 Sheikh, Mahmoud Muhammad 2015, p. 3

contrary to the public order applied in Jordan, which is the country of execution of the contract [91].

The parties to the contract may agree to apply a law other than the law of the country of origination or implementation of this transaction, or the law of their common home, if their will agrees on that, in accordance with the rules of private international law[92]. The will of the parties to an electronic transaction may be expressed either explicitly or implicitly, but the express will in electronic contracts prevails over the implicit will, as the parties to electronic contracts express their will explicitly through the Internet and carry out their obligations through this network. Examples of transactions the electronic process that takes place in this field is the buying and selling process within electronic markets such as Amazon and others[93].

The issue of defining the law whose provisions apply to electronic transactions is characterized by flexibility, due to the special nature of the principle of will powers, which is natural to be determined in a balanced and reasonable manner. However, such type of contracts and transactions are flawed by the difficulty of completing negotiations freely between the parties[94].

We must point out in this regard that expressing the will in the applicable law explicitly is better and raises the dispute in this matter, and what helps in choosing the applicable law is the existence of model contracts in electronic commerce that contain a clause through which individuals must establish the law of the country Which will govern this relationship, and it can be expressed explicitly in the way of electronic messages that occur between the parties to the contract or transaction [95].

The explicit choice of the applicable law is a guarantee of the success of commercial relations between the contracting parties, because they have chosen the law that serves their interests and secures a legal solution in the event of any possible dispute between the parties[96].

The choice of the applicable law may be either through the exchange of electronic messages through e-mail, or through web pages, and this model of contract for some

---

91 Arshour, Haitham Suleiman 2017, p. 18-19

92 Al-Masry, Hosni 2006, p. 341

93 Khlifi, Samir 2010, p. 27

94 Salem, Abdul Karim 2018 , p. 71

95 Al-Fadl, Munther 1996, p. 91

96 Patrick, thieffrx, 2002, p.228

companies may include a clause that includes the applicable law on the transaction that takes place between the company and its customers[97].

And when the parties agree explicitly to choose a specific law explicitly, it is required that there be a link between the law that was chosen and the contract, since the right to choose the law was based on the rules of attribution, and the purpose is to resolve the conflict between laws [98].

On the other hand, the implicit will is extracted by the judiciary based on the reality of the situation and the behavior of the parties, and the judge extracts it from the reality of the situation by knowing the direction of the will of the two parties, and this research is based on previous contracts and transactions of these two parties in which a specific law was stipulated that applies to that transaction, or Through the language in which the contract was written, if the German language is the language in which the contract was written, here the German law is applied to this contract, and this may be done through the currency in which the two parties agreed to fulfill the obligation arising under this contract or the place of implementation and conclusion of the contract [99]. In the event of an implicit agreement on the law of will, the judge must focus on the contractual bond and attribute it to the law most closely related to the contract[100].

2.3.2 The Case of No Agreement.

The objective attribution rule is applied in the absence of an agreement between the two parties, and this rule is one of the alternative or backup attribution rules, and it exists in the event that the two parties did not express their will explicitly in choosing the law applicable to the transaction and the judiciary was unable to derive the direction of the will of these two parties in the case being a victim[101]. In this case, the judge cannot abstain from performing his duty and refuses to consider this matter, and he also has no right to apply the law of the country in which he considered this matter to the provisions of this transaction.[102]

Here, the judge must continue the search until he reaches the determination of the applicable law, by attributing these links that he reached through the research to specific controls that are determined by a competent authority in this matter, and then resorting to indications and factors that work to indicate To the law applicable to this transaction, which is

---

97 Zouina, 2011, p. 16

98 Yakut, , p. 114

99 Zahran, Hammam Muhammad Mahmoud 2004, p. 72

100 Sadiq, Hisham Ali, 2001, p. 227

101 Mohamed, Diaa El-Din Nasser Ismail 2018, p. 13

102 Ibrahim, Khaled Mamdouh 2008, p. 192

linked in terms of its provisions and rules with the subject matter and provisions of this transaction[103].

The controls that the judge relies on in determining the law applicable to this transaction when there is no agreement are represented in the law of the country in which the contract was formed, or the law of the country in which the contract was executed [104]. Or the joint nationality law in the event that the two parties hold the nationality of the same country, or the common home law in the event that the two parties reside in the same country[105]. There is a difficulty facing the judiciary in determining the law applicable to this transaction in this case, as this type of transaction takes place through the Internet, which is governed by rigid controls in most of them, but there is a flexible regulation which works to facilitate this matter for the judiciary, and this regulation called Distinguished Performance Regulation of the Contract[106]. This control is the performance according to which the cash consideration for the commodity or service to be obtained is placed in the electronic transaction[107].

Among the things that the judge relies on in determining the applicable law during a dispute is the parties' reliance on a model contract whose provisions are in conformity with a specific legal system, or that it is drafted by an institution belonging to a particular country. This is considered a presumption indicating the direction of the implied will of the parties to subject the contract to the law of that country[108].

Before we finish this part, we must explain the role of the implementation of public order in international electronic commerce contracts, because the implementation of public order in international electronic commerce contracts is possible, as some electronic transactions that take place through cyberspace are available in some countries, while they are In other countries subject to invalidity, some countries allow betting and gambling transactions, while others prohibit it. Hence, such electronic transactions are subject to invalidity in countries that prohibit such type of transactions, and therefore the law of the country that prohibits such type of transactions is excluded when a dispute arises between the parties[109]

---

[103] Abu Al-Haija, Muhammad Ibrahim Irsan 2005, p. 93

[104] Abdullah, Izz al-Din, 1965, p. 404

[105] Ibrahim, Ahmed Ibrahim, 1997, p. 345

[106] Al-Hindawi, Hassan 2005, p. 191

[107] Al-Masry, Muhammad Walid 2002, p. 352

[108] Taklett, Applicable Law, p. 20

[109] Burhan, Samir, 2007, p. 64

2.4CONCLUSION.

- The electronic transaction is either characterized by the domestic dimension or characterized by the international dimension.
- As for those who went to say the international dimension in the electronic transaction, looking at the nature of the cross-border electronic transaction, just as the electronic transaction may be between states and sovereign states, then the rules of international law are applied in this case, as it is not permissible for the law of one state to be ruling over another state. Also, through the law of will, the rules of international law may be resorted to and made it the governing law on electronic transactions.
- As for those who went to say the domesticity of electronic transactions, he looked at the place of conclusion of the contract, the place of its implementation, the nationality of the contracting parties, and even the authority of the will of the parties in the event that they wanted to resort to the rules of domestic law in their electronic transactions.
- The law of will that has been agreed upon between the parties may be stipulated explicitly or implicitly implied.
- Among the rules that the judge resorts to in determining the applicable law in the event of a dispute is the language in which the contract was written, the currency in which the payment is made, the nationality of the contracting parties, the place of concluding the contract or the place of its enforcement.
- In my opinion, the Jordanian legislator was not successful in presenting the objective and personal scope of electronic transactions, and that he limited himself to stipulating the objective scope of the application of the law as being applied to transactions conducted by electronic means, and did not address the personal scope of electronic transactions. While the Iraqi legislator touched on the personal scope as part of his presentation of the objective scope of electronic transactions by stipulating that an electronic transaction is one that is carried out by natural or legal persons.
- The autonomy of the will was also present when dealing with the objective scope of the Iraqi legislation, because it stipulated that the application of the provisions of the law includes transactions that the parties agree to implement by electronic means, in addition to that the Iraqi legislator included electronic financial and commercial documents within the objective scope of the application of the law, and these matters were overlooked. The Jordanian legislator did not stipulate it, which the researcher believes is that the text of the Iraqi legislator that defined the scope of electronic transactions is more comprehensive and general than the text of the Jordanian legislator.

3

Electronic Communications, Privacy Rights and Confidentiality of Personal Data

3. ELECTRONIC COMMUNICATIONS, PRIVACY RIGHTS AND CONFIDENTIALITY OF PERSONAL DATA.

3.1 INTRODUCTION

Due to the rapid development of electronic means of communication, this has resulted in many challenges related to the protection of data for individuals, groups, companies and countries. Perhaps the data of individuals, as it enjoys a kind of privacy, is the most important data that has been protected in many legislations, and the right to privacy is considered one of the rights that have been most subjected to. To the threat through the massive electronic revolution. After a person lives in isolation from these means and can maintain the privacy of his data through traditional means, cyberspace knocked on his door and entered his home without his permission and made his data vulnerable to violation in light of this vast cyberspace that does not stop at... A certain geographical border that does not recognize the privacy of others. Hence, legislation has been established to confront this threat by adding more protection to the right to privacy so that it remains safe from this violation. However, the legislation in third world countries, including Jordan and Iraq, although they provide a protective cover for the right to privacy, only This cover may be useful and effective in confronting individuals with each other, but it does not provide this amount of protection against governments in third world countries in general, many of which continue to violate the right to privacy under the pretext of maintaining security, and therefore many international reports have criticized this. Violations. Hence, in this chapter, we present the challenges related to data protection and the criticisms directed at these violations.

3.2 Recommendations and comments of the Human Rights Council and the Human Rights Committee on the right to privacy in Jordan and Iraq, and the two countries' responses to these criticisms

The United Nations paid great attention to privacy, so a special rapporteur was appointed at the United Nations on the right to privacy. This position was created in 2015 by the United Nations Human Rights Council resolution No. 16/28. The aim of creating this position was to:

- Reviewing government policies related to the interception of digital communications and the collection of personal data.
- Identifying procedures that intrude on privacy without convincing justification.
- Helping governments develop best practices for subjecting global monitoring to the rule of law.
- Contributing to ensuring that national procedures and laws are compatible with international obligations in the field of human rights[110].

In its resolution on the promotion and protection of human rights on the Internet in July 2012, the Human Rights Council affirmed that the same rights that people enjoy offline must also be protected on the Internet, especially freedom of expression[111].

Since then, massive revelations regarding the scope of widespread monitoring of private communications via online and mobile platforms have sparked an international debate regarding the right to privacy versus national security.

Serious issues are raised by the possibility of exaggerating national security without controls to protect against violations[112].

In the report on privacy in the digital age issued by the United Nations General Assembly at its sixty-eighth session on November 20, 2013. It affirmed the human right to privacy, which does not allow any person to be subjected to arbitrary or unlawful interference with his privacy, family affairs, home, or correspondence, and his right to enjoy the protection of the law from such interference. Exercising the right to privacy is important for the

[110] https://www.ohchr.org/ar/special-procedures/sr-privacy

[111] https://www.ohchr.org/ar/stories/2013/11/right-privacy-digital-age

[112] https://www.aaup.edu/sites/default/files/Publications/

realization of the right. Freedom of expression and the right to hold opinions without harassment is one of the pillars on which a democratic society is built[113]

An Amnesty International report stated that the phones of five human rights defenders were hacked using the Pegasus spyware between August 2019 and December 2021. According to a Front Line Defenders investigation affiliated with the University of Toronto, the Jordanian government is likely behind this hack[114].

Recommendation 15-136 issued by the Human Rights Council at its fortieth session between 25-2to22-3-2019 It included providing all members of society with uncomplicated access to the Internet, by ensuring the security of cyberspace and the safe flow of information without violating freedom of expression or the right to privacy.

Jordan responded to this recommendation by saying that Jordanian legislation regulated the freedom to use the Internet in light of the wide spread of social networking sites and electronic blogs, within a balance that takes into account freedom of opinion and expression and limiting some aspects such as character assassination, violation of privacy, and the promotion of terrorism. Electronic governmental platforms were also created to receive complaints and suggestions. Citizens and refute rumours, including the Your Right to Know platform, at your service[115]

A report of the Human Rights Council at its seventeenth session, held in Geneva on 21/10 to1/11 \2013, stated that the law in Jordan forces websites to self-censor their contents, as there is arbitrary interference with the right to freedom of expression that comes from the obligations stipulated in The law stipulates that website managers do not publish user comments whose authenticity cannot be verified, and that after the suppression of websites and online news coverage, users moved to social media to express their opinions and organize demonstrations. Jordan responded to these criticisms by stating that theJordanian legislation grants freedom of opinion and expression in all its forms and freedom to practice journalistic work is within a system of laws that guarantees this freedom, but at the same time preserves the balance of freedoms among individuals, so that no individual infringes upon the rest of the individuals in his freedom of expression, or in any way that disrupts the security of the nation[116].

It was also stated in a report of the Human Rights Council at its thirty-first session in the period between 5to16-11-2018 that there is an increase in reliance on monitoring, including

---

[113] https://news.un.org/ar/story/2013/12/193452

[114] https://www.amnesty.org/ar/latest/news/2021/07/pegasus-project-apple-iphones-compromised-by-nso-spyware/

[115] https://www.ohchr.org/ar/hrbodies/hrc/home

[116] https://www.ohchr.org/ar/hrbodies/hrc/home

the suppression of the opposition, as more charges are brought against activists as a result of being placed under monitoring.

Jordan's response was that with regard to violations of the right to privacy in Jordan, there is only a very small amount of scrutiny and monitoring carried out by the authorities in Jordan, for reasons of maintaining national security[117].

A report of the Human Rights Council at its seventh session, held in Geneva from 8-19-2010, praised the Iraqi Constitution for guaranteeing the right to personal privacy and the inviolability of homes in accordance with Article 17 thereof. The report also praised the formation of a Ministry for Human Rights, which took place in 2003, which aims to spread the culture of human rights and education on it to be a basis for respecting human dignity and working to protect human rights and promote their goals. The report also praised the formation of committees and human rights units in 2006, whose tasks include creating the appropriate environment for exercising human rights. Human rights in various ministries, as well as spreading the culture of human rights. The report also praised the tangible improvement in the human rights situation in the Kurdistan Region. The report also praised the Constitution's guarantee of freedom of expression of opinion by all means, as exercising the right to freedom of opinion and expression represents a basic pillar in democratic construction. The report indicated that the use of satellite receivers and mobile phones has become Dealing with the Internet is not subject to any restrictions.

The report criticized the presence of a number of cases of assassination of homosexuals in Iraq, and that there is a fear of not reporting these incidents due to the unwillingness of families to acknowledge that the targeted individuals are homosexuals for fear of being exposed to other attacks[118].

Amnesty International also stated that the Iraqi government is unable to provide adequate protection for men who consider themselves gay, as many of them were mutilated and their bodies were thrown in the streets, while many others were forced to flee Iraq after receiving death threats.

The report also criticized mentioning a person's religious affiliation in official identity documents, as this entails the risk of misuse of that data or subsequent discrimination on the basis of religion or belief.

Iraq responded to some of the recommendations submitted to the Human Rights Council that they do not enjoy Iraq's support, including the recommendation of Norway and Canada, which includes investigating all allegations of persecution based on gender or sexual orientation and bringing charges against those behind these crimes. Likewise, Australia's

[117] https://www.ohchr.org/ar/hrbodies/hrc/home

[118] https://www.ohchr.org/ar/hrbodies/hrc/home

recommendation, which includes ensuring that all allegations of persecution are investigated, was not received. Reports related to human rights violations, including reports concerning religious minorities and homosexuals, and the prosecution of those responsible for these violations. France's recommendation to the Human Rights Council was not supported by Iraq, which included removing homosexuality from the list of crimes, and ensuring that those who practice violence against homosexuals are brought to justice.

Iraq also made clear that such recommendations are inconsistent with the nature of conservative Iraqi society, and are also inconsistent with the teachings of the true Islamic religion and other indigenous religions[119].

In a report to the Human Rights Council at its thirty-fourth session, held from 4-15-11-2019, it was shown that a number of current Iraqi laws constitute a threat to freedom of expression in general and to gains in the field of freedom of the press in particular. The Iraqi media law related to publications does not prohibit the exercise of freedom of expression. Expression only, but it can be punished by death or life imprisonment, which is the harshest form of punishment. The draft law on electronic crimes also raises concern because of the broad and non-specific definition, and therefore it poses a threat to the right to freedom of expression. The draft law also raises concern because It imposes a maximum of two years in prison for defamation and slander, and recommended that the Human Rights Council keep the Internet open, and amend the Electronic crime Project and the Freedom of Expression Law to ensure that they support rights rather than restrict them.

Iraq responded to these recommendations by saying that the Media and Communications Commission issued a number of regulations that regulate broadcasting and transmission media in Iraq, including codes of professional practice for the media, and a list of media broadcasting rules and systems. There are general directives about balance in broadcasting news and not inciting violence and hatred. Parliament is studying a draft law on freedom of expression, in addition to the possibility of revising legislation that requires legal legislation, noting that the law currently in force effectively meets the requirements of the current stage in terms of journalists performing their duties and meeting their needs[120].

119 https://www.ohchr.org/ar/hrbodies/hrc/home

120 https://www.ohchr.org/ar/hrbodies/hrc/home

3.3 ELECTRONIC TRANSACTIONS AND CONFIDENTIALITY OF PERSONAL DATA.

Some define private life as the right to a person's family, personal, interior and spiritual life when he lives behind his closed door[121]. There is a difference in the concept of privacy between narrowing its scope and making it limited to material privacy and what is meant by the right of isolation, while others expand its concept to include in addition to material privacy moral privacy, and even include every aspect of interference, whether it is in controlling personal information (any information related to a specific person). His identity or can be identified directly or indirectly, whether then identifying his identity by reference to his personal number or by reference to anything belonging to him.[122] As well as the right to isolation and confidentiality[123].

The right to respect for private life is one of the rights attached to the personality that proves to man, and is enjoyed by all persons without discrimination [124]The right to privacy has been protected in international agreements and national constitutions of most countries of the world, and the violation of the sanctity of privacy is a crime punishable by criminal legislation, but the protection of personal data does not enjoy this legal protection in many legislations, especially since the threat to personal data has become the dominant image in Threatening the principle of privacy with the spread of electronic transactions. Therefore, criminal legislation came to protect this right, especially with the proliferation of electronic means and the negative use by some to attack the right to private life of individuals[125].

After the tremendous development of means of communication and the use of computers and cell phones, information has become increasingly circulated on the World Wide Web, and it has become possible to conduct technical operations quickly and effectively. Awareness of the danger of electronic devices to private life has begun since the sixties of the last century, with many countries issuing laws aimed at protecting life. Own informational risks[126]. With the development of the concept of the right to a private life, this right includes the informational privacy of individuals, including personal data that may be transferred through electronic and other means [127]

But this fact is not absolute, as some jurisprudence says: The right to protect personal data is closely related to the right to privacy, but it is distinguished from it that the right to privacy is referred to in the constitutions of most countries of the world. As for the protection

---

[121] Qayed, Osama Abdullah 1994, p.8

[122] Muqresh, Ahmed Samer 2018, p. 14

[123] Nayel, Ibrahim Eid, p. 125

[124] Mughabghab, Naim 1998, p. 100

[125] Al-Manasah, Osama Muhammad, Al-Zoubi, Jalal Muhammad 2017, p. 241.

[126] Al-Husseinawi, Ali Jabbar 2009, p. 78.

[127] Muqresh, the Effects of Using the Internet, p. 15.

of personal data, some countries have recognized this right and others Many countries still do not consider the right of personal data as a right as privacy, and despite that, the protection of personal data is of paramount importance in this digital society, and in this cyberspace, especially due to its speedy flow, so it deserves legal protection, and this protection has been recognized in many countries. Countries, whether at the national, regional or international level[128].

The methods and forms of access to personal data vary. It is possible to access the data without making any changes to that data. This is done by hacking into someone's electronic system, whether this system is protected or unprotected, and access can also be made by making modifications to the data.[129].

To view and deal with data and information that would violate the right entrusted to him by law to protection, eavesdropping, collecting data and storing it illegally, attacking the confidentiality of communications and correspondence, disclosing data and information about a person and making it available to everyone in a way that harms its owner, viewing and spying on correspondence of an electronic nature and giving false and inappropriate information In the field of operations and transactions of an electronic nature, all of these forms are a violation of the principle of privacy [130].

However, it must be noted that electronic information is required in order for it to be considered of a personal nature and a secret that deserves protection, that it be related to the person, and that its owner be keen to keep it within the scope of confidentiality and far from the knowledge of others, and in attacking its confidentiality there is a possibility of material or moral harm. Returns to its owner [131].In modern societies, this right is considered one of the most important rights because it is closely related to individual freedom[132]. The reason for the importance of the right to privacy is that it is a guarantee of human security, comfort, tranquility and individual freedom[133].

The right to private life finds its many applications in international covenants.As for the international covenants, it was stated in the Universal Declaration of Human Rights:No one may be subjected to arbitrary interference with his private life, family affairs, home or

[128] Access Nader 2018 p. 2.

[129] Al-Manaasa and Al-Zoubi, p. 244.

[130] Saeedani 2013, previous reference, p. 25 Saeedani, Naeem, 2013, p. 24 Momanip. 174-178.

[131] Taha, Mahmoud, Ahmed 2017, p. 9.

[132] Al-Moumani, Nahla Abdel-Qader 2010, p. 164

[133] Hussein, Sami Jalal 2011, p. 69

correspondence, nor to campaigns affecting his honor and reputation, and every person has the right to be protected by law from such interference or attacks[134].

International conventions and conferences have also taken care of this right, as it was stated in the European Convention on Human Rights: Every individual has the right to respect for his private and family life, his home, and his correspondence, and that the public authority cannot interfere in the exercise of this right, unless such interference is provided for by law. And that it constitutes in a democratic society a measure necessary for national security, public security, or the economic well-being of the state, or to protect order, and to prevent crimes, and to protect health and morals, or to protect the rights and freedoms of others[135].

The Montreal conference convened in 1968 recommended several recommendations, including the need to take care of the dangers that threaten private life, such as electronics and audio-visual means that technology has reached, and combating their damage to the private life of individuals[136].

Constitutions and laws in various countries of the world have entrusted this right with protection, due to the high status that privacy and personality enjoy in the same individual as one of those rights that he enjoys by virtue of his human being and its connection to the dignity of the individual and his moral and material values[137].

In Jordanian legislation, the Jordanian constitution emphasized the protection of private life, as Article Seven of the constitution stipulated: Personal freedom is inviolable, and that every assault on public rights and freedoms or the sanctity of private life is a crime punishable by law[138].

The Iraqi constitution also affirmed the sanctity of private life, as it came in the first paragraph of Article 17 of the constitution as follows: Everyone has the right to personal privacy in a way that does not contradict the rights of others and public morals[139].

In confirmation of this principle represented in the protection of private life, Article (56) of the Jordanian Telecommunications Law stated: Telephone calls and private

---

[134] Article 12 of the Universal Declaration of Human Rights adopted by the United Nations General Assembly in 1948

[135] Article 8 of the European Convention on Human Rights, which was approved in 1950

[136] Bahr, Mamdouh Khalil, p. 98.

[137] Ayoub, Julius Antios 2009p. 219.

[138] Article Seven of the Jordanian Constitution.

[139] Article Seven of the Iraqi Constitution

communications are confidential matters that may not be violated, under penalty of legal responsibility[140].

Jordanian penal legislation imposes an appropriate penalty on anyone who violates the sanctity of private life and doubles it in the event of recurrence,:[141].The Iraqi legislator explicitly stated in the Iraqi Penal Code that it is not permissible to eavesdrop by ear or otherwise, or to divulge secrets..[142]

taking into consideration that personal data deserve legal protection, we must recognize the inability of traditional legislation to provide the legal protection required to keep pace with technological development in light of technical proliferation. [143]

Given the existence of technology and the widespread use of the digital world, several attacks on an individual's privacy have occurred in a variety of forms, such as capturing and tampering with data through the means of technology, which has led to many problems, often amounting to a crime. [144].

So most countries in the world have tended to secure information systems by enacting electronic crimes legislation that encroaches on one's privacy. Stealing information and data, modifying or tampering with it, and spying on individuals through the Internet, or through threats, extortion, and piracy the crimes that disrupt information systems in order to attack data and information contained within information system and transmitted through networks of a global nature[145].

The aim of setting these special legislations is to protect that information from the dangers of using electronic means[146], and deterring and disciplining the criminal, as electronic crimes has increased and its types and methods differ according to the widespread use of this space among people and their use of its equipment and tools[147].

It also required the development of special legislation to preserve privacy in cyberspace, and an international agreement was necessary to protect privacy on the World Wide Web because the electronic infringement of this privacy transcends and breaches those spaces and borders between countries due to the globality of the world wide web as it is not an institution

---

[140] Article 56 of the Jordanian Telecommunications Law No. 13 of 1995 and its amendments.

[141] Article 348 bis of the Jordanian Penal Code No. 16 of 1960 and its amendments

[142] Article 438 of the Iraqi Penal Code No. 111 of 1969 and its amendments.

[143] Al-Abadi, Muhammad Hamid 2015, p. 333.

[144] Sassi, Toshin, Abu Bakr, Soleimani 2013, p. 6.

[145] Al-Malt, Ahmed Khalifa 2005, p. 178.

[146] Al-Jubouri, Salim Abdullah ,p. 381.

[147] Al-Talawi, Ahmed Abes Nehme 2016, , p. 58.

that is legally located within the boundaries of a particular State and is governed by its provisions. A means has to be found to limit this aggression and preserve privacy as it is known[148].

But a valid question arises: Can we enact unified global legislation to combat electronic crimes and preserve privacy at the same time because cyberspace is extensive and privacy violations through it are characterized by global reach as well?

In answer to this question, we say that, because of the difference in legislation between States, not all criminal acts in one country are themselves criminalized in another, so the provisions of any law in the world cannot be applied to crimes committed on the Internet, and that is why it is difficult to find the means and method for preventing the electronic infringement of human privacy. [149]

In addition, some legislation still surrounds private life with protection while not doing the same with personal data. Many legislation has tended to protect privacy by creating obligations and responsibilities for personal information and maintaining transparent data processing. And creating special protection for sensitive data and establish enforcement rights and effective control over the processing of personal data[150].

Personal data is protected by the right to privacy in international human rights instruments. Protected data includes phone data, emails, internet usage, and data stored on computer servers. Data protection also includes the creation, collection, storage, analysis, use and sharing of personal information.[151].

The cross-border nature of the Internet requires a cross-border regulation for data protection that extends beyond the national and legal framework Examples include the African Union Convention on Electronic Security and the Protection of Personal Data of 2014 and the Economic Community of West African States (ECOWAS) Supplementary Act on the Protection of Personal Data within ECOWAS.[152].

As for the European Union, it drafted a regulation with the aim of protecting personal data in 2018, which aims to protect the data of all European citizens in all countries, and it will be applied to any party that deals with data of European citizens to protect the data of its

[148] Ayoub, Julion, Anthony 2009, previous reference, p. 219.

[149] Hijazi, Abdel-Fattah Bayoumi 2007, p. 45.

[150] Fikri, Ayman Abdullah, p. 851.

[151] Fikri, Information Crimes, p. 851.

[152] lhttps://www.unodc.org/e4j/ar/Electronic crimes/module-10/key-issues/data-protection-legislation.html

citizens, especially with regard to the processing of personal data. The aim of this regulation is the following: [153]

- Protection of normal persons regarding the processing of their personal data, their fundamental rights and freedoms, regardless of nationality or place of residence, in particular their right to protection of personal data.
- Contributing to the realization of freedom, security, justice, and economic union for economic and social progress, and for the consolidation and convergence of economies within the internal market, and the well-being of natural persons.
- Contribute to the establishment of a protection system supported by strong enforcement to create confidence that allows the support and development of the digital economy of the European Union countries, given the significant risks of protecting people's data especially with regard to various activities on the internet.
- Ensure an adequate and high level of protection and remove obstacles to personal data flows within the European Union.
- Work to ensure a homogeneous and consistent application of laws related to the protection of basic rights and freedoms of natural persons with regard to the processing of personal data in all European Union countries.
- Define the data holder's rights and the obligations of controllers and handlers of personal data, as well as similar privileges to monitor and ensure adhesion with laws on the protection of personal data

In the German federal state of Hesse, the first data protection law was passed in 1970, and then many countries developed laws to protect personal data[154].

To combat the crime of privacy and data protection, Jordanian legislators enacted the Jordanian Electronic crimes Law in 2023 and added legal materials to keep abreast of events occurring within the network in the Jordanian Telecommunications Law No. (17) For the year 1995, to reduce this infringement on privacy within the borders of Jordan.[155]

In Iraq, there is a draft Electronic crimes law, which has not yet been ratified, and the Iraqi Communications Law, which does not clearly stipulate the protection of personal data.

---

[153] Features of personal data protection under the European Directive GDPR Mohamed Ghazi, https://ae.linkedin.com

[154] Access Now, Lessons Taken from the European Union's Personal Data Protection Law, p. 2.

[155] Abdullah, Abdul Karim Abdullah 2007, p. 60.

3.4 ELECTRONIC TRANSACTIONS AND PROTECTION OF FINANCIAL DATA.

Among the personal information that deserves protection is the protection of financial data, such as the credit card number or the bank cloud number. When a person opens an account in a bank, this account has a special number, and the bank account number is one of the personal data that deserves protection[156].

Many States do not wish and fear the principle of confidentiality, particularly concerning people's financial matters and information, for fear of money laundering or terrorist financing. In this regard, before granting any facilities to the customer, banks conduct searches about the money that person wants to deposit in this bank as their knowledge of the source of such funds and how to obtain them.[157]

Infringement of financial data means violating customer privacy by obtaining and exploiting their electronic information, and this is done through several stages, including the survey stage: which is the stage of collecting information and indefinite search for some financial data of users, then followed by the survey stage, which includes scanning ports and network maps and the security vulnerability to obtain a special type of information, to discover gaps in the operating system that are relied upon to access the financial data [158].

Credit card data used in electronic payment may be obtained through illegal hacking of the global communications trunk system, as hackers use software that allows them to access data and information about companies, banks and individuals.[159]

After the scanning stage comes the stage of entering the system, and the system may be entered either by breaking the password, or exploiting the gaps and weaknesses that were discovered in the operating system, then comes the stage of maintaining ownership of the entry, and in this stage he downloads and uploads files and deals with programs and applications, and then the aggressor tries to hide his access to the system by erasing the trace, by changing certain files and hiding the login data [160].

The French judiciary has considered it a matter of privacy to publish anything that would disclose a person's financial disclosure.[161] The French Court of Cassation therefore

---

[156] Sophie PENA PORTA Abness and their treatment, art available bile sar http://www.cridibe/pdf/arid paris,2005

[157] Hegazy, Abdel-Fattah Bayoumi p. 40

[158] Abdul Hakim, Ibrahim , p.6

[159] Al-Husseini, Ammar Abbas, , 2017, p. 255

[160] Abdul Hakim, Information Crimes, p. 6

[161] Mahut, Mohamed Thamer, 2015, p. 71

held that investigations and inquiries into a person's financial situation constituted a violation of the right to privacy.[162]

Among the forms of financial data worthy of protection within electronic transactions is the electronic payment card, through which the obligation arising from one of the parties to the electronic transaction may be implemented. During the electronic payment process, the person using the electronic payment card records data about this card, which means that it is possible retaining the process and the data and information included in this process, such as the customer's balance, his creditworthiness and the income of this individual, and even this process may include data and information related to this person's financial actions prior to this process, and this information is considered confidential information of the individual, where this data can be exploited by the other party while fulfilling the obligation arising from it under this electronic transaction [163].

What helps to provide financial information to the bank in this case is that this person is obligated to provide data and information to the merchant or the bank, which are financial data for this person, or the bank obtains this information when this person provides data for the cards that he stopped using for any reason seen by the customer or the bank, such as theft or loss of data or cards whose owner is negligent or bankrupt, in this case we reach a quantity of data and information that is specific to this type of card is available in the hands of the bank or the merchant, which allows this entity to use it in a way that contradicts the principle of privacy, This means that it is possible to commit a crime of violating a person's private life, and that this type is common among merchants, not with banks, because this matter destroys the bank's reputation among people, which means that it can lose many customers due to this act [164].

The violation of consumer data by the supplier or merchant takes place through some suppliers resorting, during the consumer's fulfillment of his obligations through electronic payment, to exploit customer numbers and accounts by withdrawing amounts from them without providing any service or commodity in exchange for obtaining these funds[165].

The information obtained by the supplier or dealer may include information on bank accounts and electronic payment card numbers, so it is important that this information be

---

[162] Cass, cil.mai 2000 Jupis, 2000 Bull, cive.2000 RTD. Civ 2000, P801

[163] Fathi, Bin Jadeed 2012, Protecting the right to privacy during contracting via the Internet, a research published in the Law Journal, the third issue,

[164] Habib, Adel Jabry Hamid 2003, p. 62-63

[165] Al-Dasouki, Ibrahim, 2003, p. 38

kept, that there be trust between the consumer and the supplier and that there be guarantees that this information will not be exploited and may be subject to theft and piracy [166].

For this, it is necessary to keep the personal and financial information of the parties to the electronic transaction entrusted with confidentiality through the debt settlement process, and this matter is available in the electronic money payment system, especially the electronic wallets system, as these wallets allow maintaining the financial secrecy of the person who uses them[167].

Enhancing transparency by providing consumers with basic information on benefits, risks and product or financial service conditions, including information on conflicts of interest, is the cornerstone of many financial consumer protection regimes.[168]

Although the privacy of financial data is rarely violated by banks, this is not denied at all, as bank employees are informed by virtue of their jobs of the secrets of consumer financial data, and these data are confidential and must not be disclosed, but some employees may be dismissed from these banks and as a retaliatory factor from this employee of the bank, he may exploit the financial data that he knew, hacking and manipulating accounts, affecting consumers' confidence in this bank as a result of these operations, which exposes the bank to losses, and exposes consumers to violations of their financial data [169].

The consumer's financial data may be violated by a third party, through various means, such as deception and the creation of fake websites on the Internet that resemble the websites of original companies and commercial institutions, so the consumer, in order to obtain a specific service or commodity, submits his financial data related to the credit card.Which is exploited by such sites, and he may withdraw money from the consumer only to discover later that he has been deceived by these sites, and some may resort to flooding the site with thousands of e-mails from the perpetrator’s device. Which leads to the loss of data stored in this target device, and the mainframe computers of banks and financial institutions are targeted in order to obtain the largest possible number of credit card numbers. [170].

Among the forms of infringement of financial data is infringement of balances and bank accounts, through one of the authorized employees entering the system or customer accounts, and then transfers are made through electronic payment cards or credit cards[171].The

---

[166] Makki, Hasan, 2019, p. 363

[167] Awad, Ali Gamal El-Din 2000, p. 221

[168] Targetig Scan ,s , Report of the Acc anscams activity 2017 , Australian competiton and consumer commis ssion ,may 2018

[169] Qayed, Osama Abdullah, 2003, , p. 168

[170] Fadl, crimes related to the use of credit cards, www.pdicemc.com

[171] Najm Al-Din, Najwa, 2017, p. 529

infringement of the financial data may be through phishing, by obtaining the secret numbers of credit cards and electronic payment cards and purchasing with them, through the establishment of fake websites for certain companies and institutions in electronic shopping,[172].

The infringement of financial data may be through the penetration of security gaps by hacking the bank's systems by decoding the system, one way to capture sites is to exploit gaps through the use of a dedicated program or by blocking the service, which is the flooding of networks with data and messages that are not important in order to prevent them from functioning, or through mass search through a collective agreement to encroach on certain sites simultaneously or by finding the password by guesswork or certain possibilities.[173]

Threats to financial data include fraud and password theft by using third-party credit cards to purchase goods online, or a person may use a person's account to mount fraudulent attacks. Passwords may be stolen by claiming that those requesting them are computer security experts, or by guessing, for example, first-name letters or their date of birth, or by checking information that is posted online and enabling them to know and use passwords.[174]Financial data may be penetrated through the technical compass known as cookies, where cookies can know the Internet IP address, the method of Internet connection, the sites visited, and the type of device, the type of processor, and the data that the user is required to enter, such as name, email, credit card number, and other data.[175]Phishing may take place via social networking sites, as phishing hackers create a fake registration page, and special e-mail messages are used in order to obtain funds by fraudulent means and collect confidential information, most of which was transferred from e-mail messages with the aim of attacking and stealing confidential information related to the password and the number of the credit card[176].

Financial data has been given legal protection through the same provisions that guarantee the right to privacy for personal and individual data. As for the protection of financial data, it has been guaranteed by the Jordanian legislator. The Jordanian legislator imposed strict penalties on anyone who accesses an information network with the intention of viewing or obtaining financial data for another person. As stated in the Jordanian Electronic

---

172 Al-Shibl, Abdul Aziz, PhD thesis, 2010, p. 270

173 Al-Shibl, p. 263

174 Al-Moussawi, Mona Turki, Fadlallah, Jean Cyril, 2013, p. 17

175 Bakr, Othman, p. 14

176 Fahmy, Dina Abdel Aziz, Criminal responsibility arising from the misuse of social networking sites, Fourth Scientific Conference on Law and Media, Tanta University, 23-24-4-2017, p. 15

crimes Law, a penalty is imposed on the person who infringes on the financial data of another person,[177]

While in Iraqi legislation we do not find any reference to protecting financial data except in the draft electronic crime law, if it is implemented, as the Iraqi legislator indicated penalties for those who attempt to attack financial data.

3.5CONCLUSION.

- Personal data in electronic transactions is a right worthy of legal protection.
- The right to privacy has been recognized in divine laws, international treaties and conventions, and the national constitutions of countries.
- The call for a unified global legislation to deal with electronic transactions collides with the fact that some transactions are criminalized in some countries and considered permissible in other countries.
- Jordanian legislation provided legal protection for individuals' personal data through legislation specific to electronic transactions, due to the inability of traditional legislation to provide this protection.
- Legislations for electronic transactions aimed to protect information from the dangers of electronic means and to deter those who tempt themselves to use this information illegally.
- Financial data are considered personal data that deserve legal protection.
- The threat to financial data is greater than other threats to personal data.
- There were many and varied forms of threat to financial data, from electronic hacking to phishing to penetrating loopholes and decoding codes to blowing up websites and many others.
- The financial data received the necessary legal protection in Jordanian legislation, due to the importance of protecting these data

[177] Article No. (6) Of the Jordanian Electronic crimes Law 2023

4

Legal Characterization, Authoritative, Proof and Legal Effects of Electronic Transactions

4. LEGAL CHARACTERIZATION, AUTHORITATIVE, PROOF AND LEGAL EFFECTS OF ELECTRONIC TRANSACTIONS.

4.1 INTRODUCTION

The legal nature of an electronic transaction is based mostly on its contractual nature. Most contracts are based on the principle of consent, but there are some contracts that are considered contracts of adhesion. Electronic contracts can be considered consensual, but some of them are similar to contracts of adhesion.

Contracts may be named contracts, which are those that received a special name from the legal legislation and were regulated by the legislator within special provisions. They may be unnamed contracts, which are regulated under general legal rules and do not have a special name or special provisions.

The contract may be concluded in the presence of both parties, and this is common in contracts concluded by normal means, or it may be concluded between absentees, and this is what characterizes electronic contracts.

Modern legislation has regulated electronic contracts within special provisions, and therefore they can be invoked between parties and against third parties, especially since the legislation has given authority to both the electronic signature and the electronic record and to prove electronic transactions in two dimensions, an objective dimension and a formal dimension, and both dimensions must be taken into account in cases of proof. There are many legal effects resulting from these electronic transactions, which are no different from the effects resulting from regular transactions. In this chapter, we explain the legal framework for electronic transactions, and then we talk about how to prove electronic transactions. We conclude this chapter by explaining the legal implications of electronic transactions..

4.2 LEGAL CHARACTERIZATION OF ELECTRONIC TRANSACTIONS.

The electronic transaction in its legal characterization is based on a contractual basis, because the electronic transaction is a procedure that takes place between one person and another on the Internet, and this procedure is bound by conditions in its subject matter, whatever it is, and on its parties, regardless of whether the persons can be, which means that The electronic transaction is legally adapted due to its nature and essence[178].

For example, the legal characterization of the sale contract differs from the legal characterization of the contracting contract. The electronic transaction in its legal characterization is based in its essence on sale adapts according to this contract, and the electronic transaction based on contractual nature is legally adapted according to this contract. However, the difference here is the environment that creates the contract. The electronic transaction originates in cyberspace while the normal transaction originates in the ordinary space[179].

Which means that it is possible for there to be an electronic transaction between two parties that do not know each other except through the World Wide Web, and this means that the space for conducting an electronic transaction is much larger than the space for conducting a regular transaction, because the normal transaction is between two people present in the same place[180]. Although there are points of difference between the ordinary transaction and the electronic transaction, its legal characterization does not differ, because both of them are binding contracts for both parties[181].

Among the points of similarity also between the ordinary contract and the electronic contract is that both contracts must be documented and written in order for it to be an argument on proof, except that the difference in this is in the form and manner of writing, as there is no specific form for the electronic contract, as is the case with the ordinary contract that adheres to one form in writing and manner, this writing may include the legal evidence that stipulates the validity of the electronic transaction in the event of the death of one of the dealers or the occurrence of disputes between the two parties, This writing also contains all documents, whether they are on papers or material supports, and for this reason, writing is one of the basic conditions in electronic transactions, which means that this condition is similar to the ordinary contract [182].

---

[178] Al-Sada, Abdel Moneim 1958, Part 1, p. 91

[179] Abu Salah, Wadah Mahmoud 2021, Volume 2, Issue 4, p. 84

[180] Salhab, Lama Abdullah Sadiq 2008, , p. 32

[181] Muhammad, Nermin 2003, p. 666

[182] Al-Morsi, Abdel Aziz 2005, , p. 10

4.2.1 Electronic Transaction as Contractual Between Consent and Adhesion.

Some jurisprudence has gone to the fact that electronic contracts are contracts of adhesion, so the dealer in an electronic transaction has two options, as for the option of acceptance or the option of rejection, and the emergence of adhesion in the electronic transaction is also due to the lack of equality between the will of the two contracting parties. One of the contracting parties may have strong influence, while the other has a weaker position, especially if his need for contracting is necessary.[183]And others justified the consideration of the electronic transaction as a contract of adhesion as a result of the standardization of the contract, as one of the parties to the transaction prepares the contract in advance, and unilaterally presents the condition, Where the other party's role is limited to accepting these conditions without having the right to discuss or amend them, thus lacking the principle of choice and consent in contracts.[184]

from the other hand some of them has considered adetermine the characterization of the electronic transaction as consensual or adhesion due to the manner in which it is carried out, if this transaction is concluded through websites, then it is a transaction of adhesion, and if this transaction is concluded by e-mail, then it is characterized by the consensual character.[185]

The description of some jurisprudence of the nature of the electronic transaction as a transaction of adhesion is a description that suffers from a lot of accuracy, because the electronic transaction is mostly negotiated between its two parties. The offeror may offer a specific commodity indicating in his offer the price of this commodity, so the price may be approved or the price may not be approved, and when the price is approved, it may be approved on certain conditions, and at that time negotiation takes place between the parties to the transaction, which contradicts the principle of adhesion as the nature of the electronic contract [186]

The opinion that went to say that the nature of the electronic transaction is based on the principle of consensual, finds its application in practice because the customer has many options in front of him in the product he wants, whether it is a commodity or a service, so he is not forced to a specific product, but the authority of his will is achieved, and there is nothing to compel him to conclude an electronic transaction that he does not want.[187]

---

[183] Momani, Omar Hassan 2003, p. 34.

[184] Ibrahim, Khaled Mamdouh 2006, p. 63.

[185] Al-Moumni, electronic signature, p. 35

[186] Ibrahim, conclusion of the electronic contract, p. 63.

[187] Al-Moumni, electronic signature, p. 35.

If we express consent in the nature of electronic transaction, then this is a ground for affirmative action [188] and acceptance [189] in electronic transaction [190], the affirmative is the will that gave rise to the contract and the affirmative applies by offering it to the electronic means, whether it is a website, email, chat rooms or through a message via social media, while acceptance must include the categorical intention to contract through assertive formulas, not hesitation, and this may be done verbally or in writing, or by clicking twice on the "OK" box. [191].

In my opinion, I believe that electronic transactions are consensual contracts because the contractor has the option to accept or reject, and it is possible to choose from more than one product offered. In some cases, it is possible for negotiation to occur between the two parties, as happens when correspondence between companies, between individuals and companies, and even between countries and companies.

4.2.2 Electronic Transaction Between Designation And Non-Designation.

Contracts may be named, they are those which have been privately awarded by legal legislation and regulated by the legislature under special provisions, and they may be unnamed contracts, which are regulated under general legal rules and have no special name or provisions. Unnamed contracts do not have a specific legal organization and it is difficult to predict their vocabulary, and general rules are used to regulate them, but if the contracts are

---

[188] Article 91 of the Jordanian Civil Code stipulates:

1. Offer and acceptance are both expressions used by convention to create the contract. Any expression issued first is an offer and the second is an acceptance.
2. The offer and the acceptance are in the past tense, and they are in the present tense or the imperative if the case is intended. While Article 77 of the Iraqi Civil Code stipulates:

1- The offer and the acceptance are both expressions used by convention to create the contract, and any expression issued first is an offer and the second is an acceptance.

2- The offer and the acceptance are in the past tense, and they are in the present tense or the imperative if they are intended to be adverbial.

[189] Article 9 of the Jordanian Electronic Transactions Law stipulates: The information message is considered a means of expressing a legally acceptable will to express an offer or acceptance with the intent of establishing a contractual obligation. While the eleventh paragraph of Article One of the Iraqi Signature and Electronic Transactions Law stipulates: Electronic contract: The offer issued by one of the contracting parties is linked to the acceptance of the other in a way that proves its effect on the contracted upon, which is done by electronic means. While Article eighteen of the Iraqi Signature and Electronic Transactions Law stipulates: First, the offer and acceptance of the contract may be done by electronic means.

[190] Al-Moumni, electronic signature, p. 35.

[191] Mahmoud, Ban Saif Al-Din 2019, , Volume 27, Number 7, p. 9.

The electronic offer: It is a firm and complete offer in accordance with certain conditions that a person directs to a specific other person or to non-specific persons themselves or to all. electronic acceptance: - It is the expression of the will of the one to whom the offer is addressed, and it is required that it be identical with the offer in all its aspects

regulated within special provisions and are codified, then they are named contracts. Named contracts are contracts that the legislator singled out for a specific name and regulated their provisions with special texts, due to their widespread use in practical life, and we find that the Jordanian legislator has singled out the electronic contract with a special name and organized its provisions with special texts, Therefore, the electronic contract is one of the named contracts[192]. The matter in Iraqi legislation is no different from that in Jordanian legislation, as electronic contracts were regulated within special legislation, and the Iraqi legislator organized them within special provisions[193].

4.2.3 The Electronic Transaction Takes Place Between Absentees.

The electronic transaction, in its legal nature, takes place via the Internet, where technology is used in order to complete this contract. Examples of these means by which the electronic transaction can take place are the mobile phone, computer or other electronic devices[194].

An electronic transaction takes place between two persons or two absent parties, that means between two parties who have not been brought to a particular place to complete such a transaction, and one of the dealers may be in one state and the other in another state, it's a transaction that transcends geographical boundaries.[195]

Legal legislation alerted early to the issue of contracting between absentees. Both Jordanian civil legislation and Iraqi civil legislation considered contracting by telephone or by methods similar to telephone as a contract between people absent in place and present in time[196].

Through these legal texts, we see that

- the electronic transaction is considered as a contract that takes place between contractors who are absent in place, meaning that there is no place that brings together the contractors or dealers to complete this transaction in presence
- it is a transaction like the transaction that takes place between those present in terms of time, as its time in presence does not differ from its time electronically, which is represented in both cases by the time in which two wills converge, one of which is

---

[192] Moazeb, the Legal Framework for Transactions, p. 115. Al-Obaidi, Ali Hadi 2009, Named Contracts, , p. 7.

[193] The Electronic Signature and Electronic Transactions Law No. (87) Of 2012 was issued in Iraq on 10-18-2012 and was published in the Official Gazette on 11-5-2012 and was considered effective from the date of its publication in the Official Gazette.

[194] Boudi, Hassan Mohamed 2009, p. 50.

[195] Al-Otaibi, Muhammad Dhaar 2013, p. 44.

[196] The article102 is from the Jordanian Civil Code and the article88 is from the Iraqi Civil Code

represented by affirmation, and the other will is embodied through acceptance, this is the time in which any contract is concluded, whether it is electronic or in presence,

- the essential matter represented in all electronic contracts, which is that it is a contract that is not concluded except by using an electronic means of communication that brings together the dealers[197].

4.3 AUTHENTICITY OF ELECTRONIC TRANSACTIONS.

Electronic transactions stem from the presence of laws governing the operations that take place on the Internet in different ways. The state's approval of the use of individuals on the Internet requires the enactment of a law that gives legal character to the actions of individuals within this network. Therefore, legislation has been enacted to regulate these operations[198], and in Jordan, the Jordanian Electronic Transactions Law was issued in the year (2015) to regulate the matters of electronic transactions, and The Jordanian Cybercrime Law of the year2023 .In Iraq, the Electronic Signature and Electronic Transactions Law No. (87) For the year 2012 was issued on 10/18/2012 and was published in the Official Gazette on 5-11-2012 and it was considered effective from the date of its publication in the Official Gazette in order to regulate the matters of electronic transactions [199]

4.3.1 Authenticity of the Electronic Signature.

A signature is considered to be the instrument or instrument that gives the holder the power and legal value of the contract that he or she enters into. A person is not obligated to perform his obligation under this contract until after he or she has made the signature, even if the signature forms are different. A signature may be in writing, in the form of a seal, or in the form of a thumbprint. However, all of these images require the signatory to fulfill their obligation under the contract that he or she signed.[200]

An electronic signature is a statement that may take multiple forms, whether letters, numbers, symbols, or other forms. These forms are inserted electronically, and its purpose is

---

[197] Al-Moumani, Bashar 2004, p. 54.

[198] Abd al-Mawla, Muhammad al-Sayyid, Evidence in Electronic Documents, a research published on the Internet, the date of the visit 9/19/2022

[199] Abu Al-Haija, Muhammad Ibrahim 2011, , 2nd edition, p. 84

[200] Mamdouh, Khaled 2006, 1st edition, p. 72

to determine the identity of the owner of the signature, his unique use of it, and distinguish him from others[201]

Some jurisprudence has defined it as: a number of specific data that are visible in a form of an electronic nature in order to be considered evidence of the integrity and validity of other data related to it that are clear in electronic form [202].

It was also defined as: a set of electronic and technical procedures that give its user the ability and ability to produce a relationship through which he can distinguish his electronic messages and attribute them to himself as a party to this contract through the use of electronic symbols, letters or codes[203].

Anyone looking into the issue of the electronic signature and making it a cornerstone for completing electronic contracts and producing their impact on the ground knows very well that if it were not for this signature, many problems would have been created under these contracts, which This negatively affects the movement of electronic commerce, because the spread of many electronic contracts without an electronic signature that obliges the parties to the contract to fulfill the obligations arising from them is a matter that raises concern in the souls, so the conduct of electronic contracts is avoided, especially since the Internet brings together all the parties of the world, therefore, electronic signature has been a cornerstone of all Internet contracts and computer-mediated devices such as telephones, computers and other such devices through which electronic contracts are made.[204]

There are many types of electronic signature and its forms, including the simple electronic signature, and this signature is done by simply clicking on the keyboard as evidence of approval, and some of them are what is done by writing the signer's name at the end of the electronic editor, and some of them are what is done by photographing the handwritten signature and transferring it to the electronic document required to be approved by scanning device[205].

---

[201] Article (2) of the Jordanian Electronic Transactions Law No. (15) of 2015 defines the electronic signature as: data that takes the form of letters, numbers, symbols, signs, or other things and is included electronically or by any other similar means in the electronic record. Or it may be added to or linked to it with the aim of identifying the owner of the signature, making him unique in using it, and distinguishing him from others. While the fourth paragraph of Article One of the Iraqi Electronic Signature and Electronic Transactions Law No. (87) of 2012 defines the electronic signature as: a personal mark that takes the form of letters, numbers, symbols, signs, sounds, or other things, and has a unique character that indicates its affiliation to the signatory and is approved by an authority. Ratification

[202] Abu Al-Haija, Muhammad Ibrahim 2002, 1st Edition, p. 72.

[203] Obeidat, Lawrence 2009, p. 170.

[204] Abu Maria, Ali 2010, Volume 5, Issue 4, p. 86.

[205] Tawakul, Fadi Emad El-Din, 2010, p. 164

Including the secured electronic signature, which is done through signing using magnetic cards associated with the password, or credit card signature, or through signing using self-characteristics, biometric signature, or bio monitoring signature (such as a signature that depends on analyzing the material characteristics of a person), Which may be physiological, behavioral or congenital characteristics and is based on monitoring and measuring the vital properties of a person such as fingerprints, retinas, tone of voice or facial features [206].

A secure electronic signature is the digital signature, which is a set of numbers installed to make it a secret code to sign. and this digital signature is based on encryption, which ensures signature confidentiality credit card with a confidential number known only to the client, and this type of signature is used in electronic transactions between traders or between companies, and this type of signature is considered a safe way to identify the person who signed through the computer [207].

Among the forms of the signature is the electronic fingerprint, which is made up of data that has a fixed form. This fingerprint can distinguish the original message and identify it accurately and distinguish it from other forged messages in the event of any change in the message and the electronic fingerprint, which is either the voice print, the fingerprint, or the iris of the eye.[208].

The legal authority of an electronic signature is crucial to electronic authentication, thus ensuring protection for users through electronic media.[209] A digital signature is efficient, fast, secure and confidential. [210]

The authenticity of the electronic signature is represented by identifying the identity of the person signing, showing his satisfaction with the content of the signed document and his commitment to it, and evidence of the presence of the parties to the act at the time of signing or the presence of their legal representatives, and to ensure the credibility of the persons and information sent[211].

As for the conditions that must be met in the electronic signature in order for it to be an evidence in proof, they are as follows:

---

[206] Rida, Legal Controls for the Validity of the Electronic Signature, p. 245

[207] Rida, Legal Controls for the Validity of the Electronic Signature, p. 246

[208] Al-Mutalaqa, Muhammad Fawaz, 2006, p. 184

[209] Salah, Yasser Wajih, Issue 50, 2020, p. 387

[210] Salah, the digital signature, p. 389

[211] Reda, Avan Abdel Aziz, Volume 2, Issue 2 , 2019, p. 235

- That the signature be specific to its owner and known to him in order to achieve his role in the proof[212].
- That the signature be readable through the use of an electronic method, as well as that this signature remains until it is used as an evidence in proof[213].
- Linking the electronic signature to the electronic document until it performs its function of proof[214].

We note the Jordanian legislator's keenness to explain in detail when an electronic signature is authentic and can be relied upon as evidence

If the signatory is unique to it in order to distinguish it from others .and If it identifies the owner of the signature. Also it should be private key was under the control of the signatory at the time the signature was made. Furthermore it should linked to the electronic record in a way that does not allow an amendment to be made to that electronic record after signing it without making a change to that signature.[215]

Here, too, the legislator talks about when an electronic signature can be considered authenticated, as he mentions that if it fulfills the conditions mentioned in the preceding paragraph, and that it is linked to an authentication certificate at the time of its creation issued by one of these entities.

A licensed electronic authentication entity in the Kingdom .and accredited electronic authentication .as well entity. Government entity, whether it is a ministry, a public official institution, a public institution, or a municipality approved by the Council of Ministers, provided that the requirements of the Telecommunications Regulatory Authority are fulfilled. Likewise the Ministry of Digital Economy and Entrepreneurship. And The Central Bank of Jordan in connection with electronic banking or financial activities. [216]

And when we look at the Iraqi legislator, we find that he was not far from the Jordanian legislator in how he formulated all issues related to the electronic signature, as he dealt with them as follows

An electronic signature is valid and issued by the signatory if there are means of identifying the signatory and indicating its consent to what is stated in the electronic

---

[212] Abu Al-Haija, Muhammad Ibrahim, 2005, p. 130

[213] Abu Al-Haija, Trade Contracts, p. 127

[214] Abu Al-Haija, Trade Contracts, p. 127

[215] Article (15) of the Jordanian Electronic Transactions Law No. (15) of 2015

[216] Article (16) of the Jordanian Electronic Transactions Law No. (15) Of 2015.

document and in accordance with the signatory's and addressee's agreement on how to conduct the electronic transaction.

An electronic signature within the scope of civil, commercial and administrative transactions that are authoritative for a written signature shall be subject to the conditions provided for in article 5 of this Law.[217]

We also note here that the Iraqi legislator explicitly states, as did the Jordanian legislator, about the conditions so that the electronic signature is considered authoritative in evidence.

The electronic signature is only linked to the signatory. And the electronic intermediate must be under the sole control of the signatory. In addition to any modification or change in the electronic signature must be detectable. Aside from it shall be established in accordance with the procedures established by the Ministry with instructions issued by the Minister [218]

4.3.2 Authenticity of the Electronic Record.

The Jordanian legislator defined the electronic record as an information message that contains a record, a contract, or any document or document of another type, any of which is created, stored, used, copied, sent, communicated or received using the electronic intermediate [219]

In addition the Iraqi legislator defined electronic documents as documents that are created, merged, stored, sent or received, in whole or in part, by electronic means, including electronic data exchange, e-mail, telegram, or telecopy, and have an electronic signature[220].

The electronic document requires several conditions in order for it to be an evidence of proof, as follows:

- Writing in an electronic document must be readable, clear and understandable.[221]
- Electronic writing remains and does not go away by keeping it on an electronic pillar such as computer memory, CD-ROMs or flashers to facilitate reference to it when needed.[222]

---

[217] Article (4) of the Iraqi Signature and Electronic Transactions Law No. (87) Of 2012.

[218] Article (5) of the Iraqi Signature and Electronic Transactions Law No. (87) of 2012

[219] Article (2) of the Jordanian Electronic Transactions Law No. (15) Of 2015.

[220] Article (1) of the Iraqi Signature and Electronic Transactions Law No. (87) Of 2012.

[221] Nassif, Elias,p. 212

- The inability of the electronic document to be amended, so that in order for it to be authoritative, the electronic document must not be subject to modification. If an amendment or addition occurs, it should be visible on the electronic support[223].

The Jordanian legislator has given the electronic record authenticity and considered it to be evidence of proof, but it distinguished between the electronic record linked to an electronic signature and not linked to an electronic signature, granting the electronic record linked to an electronic signature the same authority granted to ordinary documents, while making electronic records not signed electronically the same status as regular, unsigned papers. In proof. The Jordanian legislator also did not consider electronic records linked to a signature to the same degree of proof. Electronic records that are not linked to an electronic authentication certificate are invoked between the parties to the transaction, while electronic records authenticated by an electronic authentication certificate are invoked between their parties and third parties.[224]

According to a decision of the Jordanian Court of Cassation: "Certified or signed computer outputs shall have the power of normal proof unless it is established that they have not been used or certified by the attributable person or that no one has been charged with sending them in support of the provisions of article 13 of the Law on Evidence.[225]

On the other hand we see the Iraqi legislator summarized the details that the Jordanian legislator resorted to regarding the validity of electronic records, he explained that electronic records have the same validity as their paper counterparts, but it is required that the information in the electronic records be capable of preservation and storage, with the possibility of retrieving it at any time, and it must be kept in the form in which it was created or Sending or receiving it, the information contained in these records must include an indication of its originator or recipient and the date of its sending and receipt.[226].

---

[222] Al-Zibari, Mikael Rashid Ali, 2012, p. 238

[223] Homsi, Hassan Abdel Basset, 2000, p. 36

[224] Article (17) of the Jordanian Electronic Transactions Law No. (15) Of 2015.

[225] Cassation of Rights No. 356 of 2021 dated 2-3-2021.

[226] Article (13) of the Iraqi Signature and Electronic Transactions Law No. (87) of 2012 stipulates: First: Electronic documents, electronic writing, and electronic contracts shall have the legal authority of their paper counterparts if they meet the following conditions:

A - The information contained therein must be able to be saved and stored so that it can be retrieved at any time.

B - The possibility of keeping it in the form in which it was created, sent, or received, or in any form that facilitates proving the accuracy of the information contained in it when it was created, sent, or received, in a way that does not accept modification by addition or deletion.

C - That the information contained therein indicates who created or received it, and the date and time of its sending and receipt.

4.4 PROOF OF ELECTRONIC TRANSACTIONS.

Many transactions and contracts have moved from ordinary space to cyberspace, due to the cheap cost and short time in cyberspace[227].Therefore, it is necessary to prove the electronic transaction and find means for that in order to preserve the rights of dealers electronically.

4.4.1 The Objective Dimension in Proving Electronic Transactions.

Electronic transactions are not of a single degree of importance, including simple and unloading transactions due to the simple obligation they entail, such as transactions in taxi orders or the purchase of a simple meal, in other words, the transaction may be conducted without a voiding in the contract between the parties because of the simplicity of the electronic transaction[228].

Electronic transactions, if the obligation they entail is of high value, must be under a contractual framework, such as a purchase of a car transaction, unloaded in the contractual framework until such transaction has been proven and the rights and obligations of the parties have been stated. [229]

It must be noted here that the electronic contract is a form of electronic documents that prove the validity of the electronic transaction and the rights of each party to this contract, also, the necessity of the process necessitated the existence of a law regulating the

---

Second: The conditions stipulated in Clause (First) of this Article do not apply to the information accompanying documents whose intention is to facilitate their sending and receipt.

Third: The signatory or the addressee may prove the authenticity of the electronic document by all legally prescribed methods of proof.

While Article Fourteen of the same law stipulates: The copy copied from the electronic document shall have the status of the original copy if it meets the following conditions:

First: The information and data of the copied image must be identical to the original copy.

Second: The electronic document and electronic signature must be present on the electronic means.

Third: The ability to save and store the information and data of the copied image so that it can be referred to when needed.

Fourth: The possibility of saving the copied image in the form in which the original copy of the electronic document was created, sent, or received.

Fifth: The copied image contains information indicating the location, the recipient, and the date and time of sending and receiving.

[227] Barham, Nidal Ismail 2005, p. 78

[228] Dudin, Bashar 2006, p. 82

[229] Sharaf El-Din, Ahmed 2010, 1st Edition, p. 114

transactions that take place through cyberspace without the parties to the document being in one council[230].

The Jordanian legislator has excluded some transactions from the scope of electronic transactions, including some transactions related to wills and endowments, transactions related to the disposition of immovable property, some transactions related to the disposition of movable property, agencies, transactions related to personal status, notices related to the cancellation or annulment of water and electricity service contracts, health insurance, and regulations. Suits, pleadings, judicial notification notices, court decisions, securities, and court decisions, except what is excluded according to special instructions[231].

The Iraqi legislator did not deviate much from the Jordanian legislator in excluding some transactions from the scope of electronic transactions and applying the electronic signature law to them[232].

---

[230] Bayoumi, Abdel-Fattah Hijazi 2005, p. 82

[231] Paragraph (A) of Article No. (3) of the Jordanian Electronic Transactions Law No. (15) of 2015 AD and its amendments stipulates: "A. The provisions of this law apply to transactions conducted by electronic means.

While it stipulates that the scope of electronic transactions does not apply to some transactions, as paragraph (b) of the same article stipulates:

- The provisions of this law do not apply to the following unless any other law stipulates otherwise: -

1- Creating and amending a will.

2- Establishing the endowment and amending its conditions.

3- Transactions for the disposition of immovable and movable property whose registration is required by legislation, including the agencies related to them, their title deeds, and the establishment of real rights over them, with the exception of lease contracts for these funds.

4- Agencies and transactions related to personal status.

5- Notices related to cancellation or termination of contracts for water, electricity, health and life insurance services.

6- Regulations of cases, pleadings, judicial notification notices, and court decisions.

7- Securities, except as stipulated in special instructions issued by the competent authorities based on the Securities Law or any other legislation.

[232] The first paragraph of Article Three of the Iraqi Electronic Signature and Electronic Transactions Law No. (87) of 2012 stipulates: First: The provisions of this law apply to:

A - Electronic transactions carried out by natural or legal persons. B - Transactions whose parties agree to implement them by electronic means.

C - Financial and electronic commercial securities.

While the second paragraph of the same article excluded some matters that cannot be proven by electronic means in the second paragraph of Article Three of Iraqi legislation, which stipulated: Secondly, the provisions of this law do not apply to the following:

A- Transactions related to personal status matters and personal matters

B - Creating the will and endowment and amending their provisions

In my opinion that both the Iraqi and Jordanian legislators did well to exclude these transactions since they are between members of the same family and it is easy to violate electronic privacy between people who reside in the same house.

And the reason for preventing these transactions in order to arrange proof of them is their need for the presence of the parties and the presence of contact between them in the real world[233].

4.4.2 The Conditions That Must Be Met In the Electronic Signature In Order For It to Be Provable.

The electronic signature has many functions, including identifying the signatory, expressing the will of the signatory on the document, and proving the integrity of the contract[234].

America is considered one of the first countries to issue legislation that considers the electronic signature as a complete proof of proof, as the Electronic Signature Law was passed in 1995. This law added the authoritative proof of the electronic signature, as long as it was done through the public key cipher and was authenticated by electronic authentication, and then the law abandoned the certificate Electronic ratification the electronic signature itself was considered an argument of proof[235].

The electronic signature is mediated by an intangible electronic intermediate, and it also requires a specific mechanism that includes the attributed of the signature to its owner, and it is often a third element such as a bank or an official entity, and the electronic signature is considered safer than the manual signature, especially if you use the feature of signing with the secret number or the magnetic card, The electronic signature possesses legal authority and does not differ in that from the ordinary signature[236].

In order for it to be provable, the electronic signature must:

- That the signature be distinct and related to the person of its owner, and this condition aims to ensure that no other person creates the same signature so that this

---

C - Transactions related to the disposal of immovable properties, including the agencies related to them and their title deeds, and the establishment of real rights over them, with the exception of lease contracts for these properties.

D. Transactions for which the law has established a certain formality

233 Al-Mutalaqa, Muhammad Fawaz 2006, 1st edition, pp. 19-20

234 Shawabkeh, Hazem Salem, Volume 11, 2019, p. 32

235 Al-Shammari, Saad Ghaleb Ali, 2018, p. 56

236 Ibrahim, Khaled Mamdouh, , 2010, p. 201

signature is unique and closely linked to the person concerned, morally and materially[237].

- It should be sufficient to identify the owner of the person, by referring to the authorities issuing the electronic signatures and the accredited certification certificate, including the signature with the PIN number in the automated teller machine[238].
- To be created by the means of the person and under his control, and that the owner of the electronic signature is alone with it, as no one can know the decoding of his signature or enter it[239].
- That the signature be linked to the record to which it relates in a way that does not allow an amendment to be made to the contract after signing it without making a change in the signature[240].
- Documentation[241].

In Jordanian legislation, in order for an electronic signature to have the authority to prove ordinary evidence and be used as evidence between the parties to the transaction, it must be characterized by being protected, and this requires the availability of conditions, namely that its owner be unique in it and through which the identity of its owner can be determined, and that the private key is subject to the control of the owner of the signature at the time the signature is made, and it must The signature is linked to the electronic record in a way that does not allow for modification to the electronic record after its signature. Moreover, a protest may be made between the parties to the transaction and third parties if it is notarized if it meets the conditions of protection in addition to its link to an electronic authentication certificate[242].

---

[237] Nuseirat, Alaa Muhammad 2005, p. 130

[238] Obeidat, Lawrence Muhammad, proof of the electronic editor, p. 130

[239] Obeidat, Lawrence Muhammad, proof of the electronic editor, p. 130

[240] Nuseirat, Alaa Muhammad, The Authenticity of the Electronic Signature in Evidence, p. 136

[241] Obeidat, Lawrence Muhammad, proof of the electronic editor, p. 130

[242] Article No. (15) of the Jordanian Electronic Transactions Law No. (15) of 2015 AD and its amendments stipulates: An electronic signature is considered protected if it meets the following conditions together: -

A- If the person who signed the signature is unique to him to distinguish him from others.

B- If it identifies the person who signed the signature.

C- If the private key is under the control of the signatory at the time the signing is made.

D- If it is linked to the electronic record in a way that does not allow for making an amendment to that electronic record after signing it without making a change to that signature.

Article (16) of the Jordanian Electronic Transactions Law stipulates:

As for Iraqi legislation, the electronic signature is considered evidence of proof if it is approved by an accredited certification authority, even if the electronic signature is linked exclusively to the signatory. Any modification or alteration in the electronic signature must be detectable, and the electronic intermediary must be under the control of the signatory. Alone and no one else[243]

4.4.3 Conditions To Be Met In the Electronic Document Or Record.

A trend of jurisprudence has gone that it is permissible to consider the electronic document as an official bond, especially in light of the modern technological capabilities, as some developed countries deal through these electronic bonds, and there is an authority called the Electronic Ratification Authority that grants digital certificates to verify the identity of the contracting parties via the World Wide Web. It also certifies electronic signatures, in addition to the appearance of an electronic notary who certifies these documents, making them official bonds issued by an authority recognized by law, and does not need the authentication of other parties as they are issued mainly by an internationally recognized authority[244].

The electronic document is considered a complete written evidence that enjoys the specifications enjoyed by the regular document, in terms of the availability of confidence that the signature is attributed to the signer and that the electronically edited paper has been placed in a manner that achieves a close link between them and indicates his acceptance of what is contained therein[245].

The electronic documents extracted from the Internet are a principle of legal proof from the principle of proof by writing. The presence of information on electronic supports or

---

The electronic signature is considered authenticated if all the conditions mentioned in Article (15) of this law are met and it is linked to an electronic authentication certificate issued in accordance with the provisions of this law and the regulations and instructions issued pursuant to it, at the time of creating the electronic signature by any of the following entities: -

A- An electronic authentication body licensed in the Kingdom.

B- An accredited electronic authentication body.

[243] Article Five of the Iraqi Electronic Signature and Electronic Transactions Law No. (87) of 2012 stipulates: The electronic signature is authentic in proof if it is approved by the certifying authority and the following conditions are met:

First: The electronic signature is linked to the site alone and no other.

Second: The electronic medium is under the control of the site alone and no one else.

Third: Any modification or change in the electronic signature must be detectable.

Fourth: It should be established in accordance with the procedures determined by the Ministry through instructions issued by the Minister

[244] Bakr, Ismat Abdel Majeed, 2015, p. 364

[245] Bakr, The Role of Scientific Technologies in the Development of Contracts, p. 365

extracting a copy of them by means of a printer can constitute evidence of the issuance of writing by the defendant, which can confer on them the principle of proof by writing that brings the possibility of the validity of the right closer. The plaintiff is the subject of the contract[246].

Conditions for accepting the electronic document as proof:

They consist of the following matters:

- The readability of the electronic editor in order to understand its content and understand what it contains[247].
- Preserving the integrity of the data, by recording on a intermediate that allows writing to be stable and continuous so that it can be referred to at the time of need[248].
- Non-penetration, which means the inability to access it in illegal ways so that it is not subject to modification or modification[249].

The Jordanian legislator considered the electronic record to produce the same legal effects produced by a registration, contract, instrument, or document submitted in written form, but the information contained in this electronic record must be accessible, and the possibility of storing the electronic record and referring to it at any time without Make any change to it[250]

When we look at the Iraqi legislator, we find that: he stipulated that the electronic record should produce its legal effects if it was signed during the validity of an approved certificate of authentication and was matched with the identification code shown in that certificate [251]

[246] Qandil, Saeed, , 2004, p. 32

[247] Tabor Michel , , 2003 , p50

[248] Verhest Thibauh, 2002 , p.80

[249] Kamel Mehadi , 2010, P .44

[250] Article (6) of the Jordanian Electronic Transactions Law No. (15) of 2015

[251] Article Seventeen of the Iraqi Electronic Signature and Electronic Transactions Law No. (87) of 2012

4.5 Legal Effects of Electronic Transactions.

Despite the difficulty of the many challenges facing electronic transactions in terms of the difficulty of determining the identity of the contracting parties in the absence of a direct relationship between the two parties, due to the spatial separation between the parties to the commercial operations that take place through the Internet.[252].In the absence of material supports and paper documents, the procedures and correspondence between the parties to the transaction are done electronically[253].

Also, collective interaction takes place between several parties at the same time, as one of the parties to the transaction can send the electronic message to an unlimited number of recipients at the same time[254].And the need for an electronic intermediant through which the will of the contracting parties is expressed[255]. Despite all these challenges, the effects of electronic transactions do not differ from the effects of regular transactions in terms of the functional equality of the electronic transaction with the paper transaction and the adoption of the electronic signature and giving it the full argument if it is protected and reinforced. And the authoritative electronic editor in the proof [256].So that if the receiver treated the electronic message addressed to him from the originator as an offer issued to him, and he agreed to this offer with an identical acceptance, in this case the contract is concluded.[257].

Electronic transactions do not differ in the generation of legal effects from ordinary transactions, the difference in the generation of effects is due to the different subject and nature of the electronic transaction itself. The electronic transaction that is a sale and purchase contract entails legal effects represented in obligating the seller to deliver the sold item to the buyer and obliging the buyer to pay the value of the sale to the seller[258], the effects that combine all types of electronic transactions are represented by the binding force of what was stipulated in this transaction [259] Electronic transactions do not differ in their legal effects from regular transactions[260].

The legal effects that result from the transactions do not differ according to the nature of the transaction, whether it is electronic or ordinary, because there is a legal regulation of the

---

[252] Burhan, Samir, Concluding the Contract in Electronic Commerce, a research presented to the Conference on Legal Aspects of Electronic Commerce, Cairo, 12-13/1/2002.

[253] HOPNE (R) Electronic controlling part 5 Electronic contracts and Evidence p2

[254] SMEDINGHOFF (T) –2005 , vol 9 , issue 4 , p.311

[255] Musa, Khaled Al-Sayed Muhammad, , 1st edition, 2014, p. 58

[256] Khalifa, Muhammad Ahmed Kasib, 2019, p. 309

[257] Al-Mabadi, Jihad Mahmoud, , 2016, p. 86

[258] Momani, Bashar Talal 2004, , p. 128

[259] Abu Al-Haija, Muhammad Ibrahim 2011, , p. 115

[260] Al-Otaibi, Muhammad Dhaar 2013, , p. 57

contract between the parties, whether in a normal or electronic form, In all cases, they arrange the binding force for the implementation of obligations for the parties to the electronic or regular contract, and both contracts are similar in the rules for interpreting transactions, guarantee provisions, and guaranteeing hidden defects. And the validity of the transaction on both parties, and the rules of general succession and special successor, and the rules that govern the relationship of creditor and debtor under this contract, in addition to the obligations and rights stipulated in the contract in terms of the parties in it[261].

If we want to apply the effects of electronic transactions to the electronic sales contract as a form of electronic transactions, we find the following effects:

- The seller's obligation to deliver the sold item in electronic contracts, and that is that the item sold is placed at the buyer's disposal so that he can possess it and use it without obstacle or hindrance. If the item sold is digital, then it is delivered through the Internet itself, so its delivery is by downloading and uploading it directly to the computer of the buyer or service applicant and enabling it. From accessing and benefiting from it according to the contract or by sending it through e-mail if it is computer programs or e-books, but if it is non-digital goods, it shall be delivered by traditional methods[262].

- The guarantee contracted in electronic contracts via the Internet, information must be provided to the consumer about the conditions of commercial guarantees and after-sales service and the seller's responsibility for the risks that the seller may be exposed to in the event of a sale with experience in accordance with the basic conditions of this guarantee[263].

- The obligation of the buyer to pay the price in electronic contracts, so the payment of the price is the main obligation on the buyer and the performance of a price that may be done via the Internet and may be done by electronic means [264].

[261] Michel, Tony Issa 2010, p. 72

[262] Arbab, Youssef Zakaria Issa, Volume 10, Issue 1, 2019, p. 6

[263] Arbab, Legal Effects, p. 7

[264] Arbab, Legal Effects, p. 7

4.6CONCLUSION

- We conclude from the foregoing that the electronic contract is a contract that is characterized by consensual character and not by adhesion, as the means used in contracting does not change the nature of the contract, and contracts are mostly consensual contracts. And Adherence contracts remain contracts of consent, whether they are concluded by ordinary means or through electronic means. The means used in contracting does not alter the nature and reality of the contract in any way.

- The conclusion of the contract by electronic means does not change the nature of the contract in any way, whether it is a consensual contract or a contract of adhesion, and the electronic contract is one of the named contracts for its regularity within special legal rules.

- Both Jordanian and Iraqi legislation recognized the authoritative of electronic transactions, Electronic contracts have been legalized as a contract that binds both parties to the content of the contract concluded between them by electronic means.

- To prove electronic transactions, certain conditions must be met in order for the electronic signature of its owner to be proven. Also, certain conditions must be met in the electronic record or document in order for it to be an evidence in the event of disagreement between the two parties to the contract.

- The effects of electronic transactions do not differ from the effects of regular transactions. The method used in concluding the agreement between the parties does not change the reality of the contract in any way.

5

Substantive Criminal Protection for Electronic Transactions

5. SUBSTANTIVE CRIMINAL PROTECTION FOR ELECTRONIC TRANSACTIONS

5.1 INTRODUCTION

Electronic crime are of a special nature, since these crimes take place in the electronic environment. The special nature of these crimes also lies in the scene of the assault. Legal characterization also plays a role in consolidating the special nature of these crimes, as traditional texts are not sufficient since they are based on material standards, while these crimes affect a person's identity, money, and property. Moreover, proving evidence is one of the challenges posed by electronic crimes, as the data being searched for may be encrypted, and incriminating evidence can be erased and destroyed in a short period of time[265]."

In view of the special nature of electronic crimess, there must be criminal protection from such crimes. Therefore, we will present successively in this part the crimes that occur on the website, and then we will present after that the criminal liability of the electronic service provider, while we dedicate the third section to the criminal protection of the recipients of the electronic service.

Crimes related to electronic transactions are not organized under one heading, but rather have multiple headings, including illegal entry or exceeding authorized access, including the crime of forging information, including the crime of destroying information, and including the crime of stealing information. Electronic service providers are responsible for many obligations, and if these obligations are violated, they are subject to criminal accountability. Legislation has provided a series of protections for service recipients, whether by providing protection for information and data, websites, or the information network. The protection also included protection from By impose criminal penalties for electronic crime perpetrators.

[265] Qashqoush, Hoda Hamed, , 2001 , p. 4.

5.2 CRIMES OCCURRING ON THE WEBSITE

Before talking about the crimes committed on the website, we must talk about the elements of the crime in general, whether it is a regular or electronic crime, so that we can then proceed to talk about the crimes committed on the website in particular.

5.2.1 Criminal Act

The criminal act is the most important element upon which any crime is based in order to be punished by law. The law does not punish a crime for which there is no criminal act[266].

It is possible to define the criminal act as: the external activity that shows criminal behavior in existence, and according to the limit or amount that the legislator considers it a criminal behavior[267].

Or it is the behavior or activity that leads to the occurrence of the crime[268], or it is an activity characterized by a material nature and it appears through the perpetrator's practice of his criminal operation in the reality[269].

The criminal act is the material aspect of the crime represented by the activity of the perpetrator, the result achieved through this activity, and the causal relationship between them.

In the crime committed on the website, the technical activity is the axis of the electronic crime. This is the most important feature that distinguishes its criminal act from the traditional crime. When the various legislations dealt with the legal regulation of the crime on websites, they dealt with this element, as it requires that such crimes be committed using a computer through automated data processing. The legal texts stress the necessity of carrying out a technical activity, as ignorance of the techniques does not enable the user to enter the Internet, and therefore the user must possess a special skill with the technology, which entails an important result, which is that conviction in this type of crime requires knowledge of the computer and its use, as it is considered part of the material activity in technical crimes committed on the website[270].

The crime on the website shows criminal behavior when accessing personal and financial data and information and the preparatory work for technical criminal conduct has

---

266 Hosni, Mahmoud Naguib, 1989, pg. 217

267 Al-Sarraj, Abboud, , 2018, p. 137

268 Muhammad Al-Waseet in the Criminal Code, General Section, 2012, p. 51.

269 Al Jarallah, Abdul Aziz Ghuram Allah 2017, 2017, p. 85.

270 Jaafar, Rabie Mahmoud Mohamed, 2017, p. 96-97

been considered as one of the elements of the crime. Among the actions that considered preparatory work is the purchase of breach sites and programs through the network, or the purchase of passwords and equipment to decrypt electronic codes, which means the availability of criminal behavior[271].

As for the criminal result, it is the change that results from the occurrence of criminal behavior on the ground, and cancels a right or interest guaranteed to a person with a legal bail[272].

When talking about the criminal result of the crime on the website, it is represented by the breach of information or data of a person or an institution[273], and the crime on the website may be limited to criminal behavior without a result of this behavior, as it is in the case of unauthorized access without making any change to the website[274].

This result is distinguished in the crimes of assaulting electronic security in two basic aspects, one of which represents harm to the interest and the other represents danger. Among the crimes of electronic harm is the crime of cancellation, deletion, destruction, harm or alteration of a website. As for dangerous crimes, such as the crime of entering without authorized into the network or electronic information system[275].

5.2.2 The Criminal Intent of the Crime

The legal liability resulting from the crime was limited to the criminal act only, without looking at the criminal intent, which is the reason for the criminal act. After that this responsibility developed through the adoption of the criminal intent of the crime. Which made the presence of the criminal act not the only reason for the punishment against the criminal, but rather the perpetrator of the crime should have done it consciously and willfully[276].

So the criminal intent of the crime represents the mens rea, and legal knowledge, that the person intends to bring about the criminal result that results from the criminal behavior of the criminal act ,knowledge is embodied in a person knowing that what he does or refrain from doing is a crime punishable by law. In addition, under this element, a criminal will is required that results in criminal intent under the concept of what is called sinful will[277].

---

[271] Al-Hayazi, Ahmed Muhammad, 2010, p. 103

[272] Mostafa, Hosni, 1988, p. 28

[273] Al-Faridi, Adam Suleiman Diab, Part 1, 2017, p. 28

[274] Journalist, Rawan Atiyatallah, Issue 24, Month 5, 2020, p. 23

[275] Al-Jamal, Criminal Protection of Electronic Security, p. 30

[276] Ananza, Muhammad Abd al-Rahman, 2017, p. 55

[277] Hosni, Mahmoud Naguib, Explanation of the Criminal Code, previous reference, p. 502

The criminal intentis the psychological and mental state of the perpetrator, and the thoughts and mental matters that link this state with its material component, and it is an essential element for committing the crime and punishing because of it. And the criminal intentis embodied in two things, the criminal is aware that the behavior that he will perform is legally criminal behavior[278], and the other matter is represented by the sinful will, which is the motive that comes into the intentions of the perpetrator and pushes him to bring about criminal intent by showing it through criminal behavior that results in a criminal result[279].

The criminal intent of electronic crimes is represented in the perpetrator's will to bring about the punishable criminal result called intentional criminal intent, the perpetrator of the crime planned and managed to commit it, by obtaining electronic information by any means, or by penetrating a computer network, so, electronic crimes is only achieved in its intentional form [280].

Some electronic crimes require the existence of criminal intent explicitly, such as the crime of accessing an information program or information system, or any intentional act intended to flood e-mail, while some crimes stipulate that criminal intent is indirectly provided for in bad faith or by way of fraud or requiring the knowledge of the perpetrator[281], Among the special intent is what is stated in Article 4/A of the Jordanian Electronic crimes Law No. 17 of 2023, if its goal is to access data or information not available to the public that affects national security, the Kingdom’s foreign relations, public safety, or the national economy.

5.2.2.1 Cases of Criminal Intent.

The First Case: The Event That the Perpetrator Wants to Achieve a Result of His Criminal Behavior That Is Expected from His Criminal Behavior.

If the perpetrator wants to achieve the criminal result of his criminal behavior emanating from his criminal intent, whether the image of this behavior is negative or positive, and the result of his behavior causes harm to a right that the legislator has valued for legal protection, or represent a threat to the interest of the legislator’s ability to be worthy of legal protection and guarantee, provided that the perpetrator knows that the criminal behavior emanating from his criminal intent is legally criminal and punishable behavior.

---

[278] Al-Sarraj, Abboud, previous reference, p. 221

[279] Al-Marsafawi, Hassan Sadiq, , 1972, p. 66

[280] Al-Maraghi, Ahmed Abdallah, , 2017, p. 36

[281] Al jany, Criminal Protection of Electronic Security, p. 38

as the criminal result is expected for this criminal behavior emanating from the criminal intent, so here the criminal bears the criminalty imposed by the law for this act, and an example of it is the crime of illegal access to the website with the knowledge of the perpetrator that this matter is prohibited by law, however, his will was directed to the practice of this legally criminal act, so he must bear the legally stipulated result by punishing this act[282].

The Second Case: The Case of Permissibility of Intent.

This case happens if the criminal act and behavior, in any form, negatively or positively, results in a danger or harm that is more than the danger or harm that can be imagined to occur from this criminal behavior. The criminal intended a result that was less harmful and dangerous than the result that occurred on the reality.

such as one person sending a virus to another through the computer, the intention of the first person to send this virus is to reduction the speed of the other person's device, if the virus works to permanently destroy the device of the other person then here the law and the judiciary adopt the principle of permissibility of intent, because the criminal here did not intend to destroy the device of the other person, but rather intended to reduction its speed only[283].

The Third Case: The Case of the Enorm of the Criminal Result.

In this case, the criminal behavior and the act of the crime are related to the criminal because of his action or his abstention from a certain behavior, and it is supposedly that the criminal intent of the perpetrator existed without achieve it. The reason for this is the enorm of the criminal result that was achieved through the criminal behavior of the perpetrator, here, the perpetrator has to bear the results resulting from his criminal act and behavior, whether he expected them or not [284].

Examples of such cases in the crime committed on the website include a person breach another person’s computer in order to get a file containing personal photos of this person, and the file that he obtained include the financial information of this man, so this criminal person publishes that file believing that it contains pictures of the man only, so if the person’s financial information is spread on the websites, Here, the criminal is fully responsible for his

[282] Al-Jabbour, Muhammad, 2010, p. 238-239

[283] Al-Jabour, Muhammad, The Mediator in the Law of Contracts, previous reference, p. 238-239

[284] Al-Ajmi, Abdullah Daghash, , 2014, - p. 30

crime and its results, and it may exceed the limit of the punishment that he was expected to get for him doing this act [285].

5.2.3 Causal Relationship

5.2.3.1 Definition of Causal Relationship:

It's the relationship between criminal behavior and criminal results[286] .In criminal law, there is the criminal act, criminal intent, and the causal relationship, which links these two elements, that is, it represents the relationship between the act and the result. It is one of the most important issues in attributing the action to the actor

5.2.3.2 There are Three Theories to Determine the Criterion of Causal Relationship, and These Theories are:

The Theory of Equivalent Causes:

It is a theory that establishes the principle of equality between all factors contributing to the creation of the criminal results, as soon as there is a relationship between the act and the harmful result, and the fact that criminal behavior is one of the factors contributing to its occurrence, even if its share is small, so the availability of a causal relationship in this case. It justifies considering the behavior of the perpetrator as a reason for the result, especially since it is the behavior of the perpetrator that made matters end to what they ended up with the occurrence of the result, and then he is held accountable regardless of the various factors that interfered between his behavior and the result that this behavior led to. Whether these factors are due to the victim's act, the act of another person, or the act of nature[287]. An example of this theory in traditional crimes is what happens in a murdering case by shooting by the perpetrator, and the time when the life of the victim ends. The causal link here is represented by the severity of the criminal behavior and its impact on the emergence of the criminal results represented in the end of a person's life[288], and this theory cannot be applied to crimes on the website.

---

[285] Al-Jabour, Muhammad, The Mediator in the Law of Contracts, previous reference, p. 238-239

[286] Hosni, Mahmoud Naguib, , previous reference, p. 293

[287] Obaid, Raouf, Criminal Captivity between Jurisprudence and Judiciary, p. 28

[288] Ebeid, Raouf 1974, p. 184

The Direct Cause Theory:

It means that the perpetrator is not held accountable for the result that occurred as a result of his criminal behavior unless it is directly related to his behavior, and that he is the main or strongest cause of the occurrence of this result. It can be said that it occurred from the behavior of the perpetrator alone. The causation of this situation requires some kind of material connection between the criminal behavior and the criminal result because it only recognizes the direct link achieved between them[289].

An example of it in light of electronic crimes is the crime of seizing a person's electronic money by stealing the personal financial data of a person if the password for this data is not strong, here, the weakness of the password is not considered a reason for the occurrence and appearance of the result of the act of appropriation, but theft is considered the strongest reason for the occurrence of the appropriation, and not the weakness of the password for this data and information[290].

The Theory of Appropriate Cause:

The causal relationship between criminal behavior and the criminal results is available when the importance of the contribution of criminal behavior in causing the criminal results is proven in relation to other factors contributing to events with the same results, however, this relationship between the behavior of the perpetrator and the result is severed if foreign factors interfere between them, then the responsibility of the perpetrator stops at the limit at which the foreign factor is involved, he is not asked about the result that followed that intervention, as the responsibility rests in this case on the foreign factors that led to the creation of this result [291].

This theory is the closest of the three theories to the theories of the causal link to the criminal actin electronic crimes, and as an example is when the perpetrator sends from his device a virus directed to the victim's device to work on disturbing the internal system of the device without this virus having effects in destroying the information in this device, and when the virus is transmitted to the victim's device, something may happen that is not in the perpetrator's thoughts, and the victim's device is completely destroyed. Here, the judiciary, when applying its adjudication and implementing it on the perpetrator, relies on the theory of the appropriate cause, as the virus does not completely disable the device, so the punishment

[289] Fouda, Abdul Hakim, the provisions of the causal link in intentional and unintentional crimes, p. 39

[290] Al-Mashhadani, Muhammad Ahmad, 2003, p. 145

[291] Wahhabiyyah, Abdullah, , 2003, p. 185

of the perpetrator is limited to the supposed work of the virus when it entered the computer, and he is not punished for the impact that the virus had on the ground[292].

In the context of talking about the causal relationship in crimes of assault on electronic security and the causal relationship in crimes of harm, the causal relationship in crimes of harm is clearer than in crimes of danger, since in crimes of danger it depends on the estimated probability and before the outcome occurs when it was. It is possible to evaluate the activity that contains the elements of occurrence of the potential outcome.[293].

After this introduction on the elements of crime in general and electronic crimes in particular, it is appropriate for us

5.3 DIVIDE ELECTRONIC CRIMESS:

According to The Scene of the Crime and The Type of Data electronic crimes can be divided into the following sections:

- Crimes whose subject matter is the value of computer data, such as electronic forgery crimes, information and data destruction crimes, electronic theft crimes, and electronic espionage crimes.
- Crimes involving money, such as fraud and electronic fraud.
- Crimes the subject of which is personal data, which are crimes of assaulting privacy
- Crimes whose subject matter is intellectual property rights, such as software piracy crimes[294].

We talk about electronic crimes in the event that the information system is the subject of the crime, and what is meant by the information system, such as data and programs, such as assaulting data stored in computer memory or transmitted through communication networks by theft, forgery, or assaulting the program itself by claiming ownership, theft, imitation, destruction, erasure, or disabling it[295].

Since we are talking in this part about the website, we must define it, as it is the electronic space that a user of the Internet occupies and gives a simple overview of it to all the

---

[292] Al Jarallah, , previous reference, p. 93

[293] Abdel Salam, Mazhar Moataz, 1999, p.113

[294] Al-Helou, Hassan Aziz, Al-Zubaidi, Jalal Khudair, 2015, p. 149.

[295] Al-Khaili, Shamsan Naji Saleh, 2009, p. 37.

people on the World Wide Web. An example is the electronic page on websites belonging to a company or even ordinary people [296]

5.3.1 Among the Images of Crimes That Occur On the Website.

The forms of electronic crimes do not come in the same method, as they differ according to the result that the criminal seeks to achieve

- Interfering and manipulating system inputs.
- Planting virus programs.
- Manipulating computer data.
- Program manipulating[297] .

Dr. Ali Al-Husseinawi considers that the crimes that occur on the website, such as forgery, destruction, and theft, are fraud crimes, and he decides that whoever practices fraudulent means in confronting the data processing system and is able to hack it with the aim of achieving material benefit or obtaining a service is not responsible for the crime of fraud in the sense of the Jordanian criminal code, and he indicated the correctness of what he went to, that the computer data subject to the crime of fraud lacks the material characteristic, which is the basis of the fraud process, and therefore lacks the requirement of the Jordanian legislator in requiring that the subject of the crime of fraud be movable money of a tangible material nature [298].

However, in my opinion I objects to this interpretation, because one of the forms of money at the present time is digital or electronic money, which is money that is transmitted through devices and electronic wallets without any material space for it. And what Dr. Al-Husseinawi went to regarding the crimes of forgery, theft, and destruction as fraud crimes[299] went to some contemporary researchers, but the researcher believes that the crimes of forgery, destruction, and electronic theft are among the crimes that occur on the website, while the crime of electronic fraud is one of the crimes whose subject is money and is done by means electronic.

---

[296] Mustafa, Ahmed Mahmoud, 2010, pp. 78-79

[297] Al-Husseinawi, Ali Sabara, 2018, p. 59

[298] Al-Husseinawi, Computer Crimes, p. 61

[299] Dr. Ali Al-Husseinawi explains the crimes that occur on the website, such as forgery, damage, and theft, are fraud crimes. He also states that anyone who practices fraudulent means in the face of the data processing system and is able to penetrate it with the aim of achieving a financial benefit or obtaining a service is not responsible for the crime of fraud within the meaning of the Jordanian Penal Code.

This opinion was in agreement with what the Court of Cassation decided in its General Assembly's decision in its penal capacity, Resolution No. 1008 of 2020, dated 7/28/2020, which stated: "In this we find that with the development of technology, means of communication, information, and the Internet, cybercrimes fall under two descriptions:

The first of them:

The first of them are crimes that occur on the Internet. These are crimes that have arisen with the appearance of new technologies and require their existence for their commission. For example, unauthorized access to automated data processing systems, virus crimes, crimes of theft of information and computer services and crimes of communication of false or falsified data, as well as other crimes that occur on the network.

The second is:

The crimes committed via the Internet, which the Criminal Code criminalizes and defines their nature and material and criminal intents.

What is new here is the means of committing them, where the criminal uses the network as a means to achieve the criminal result he envisioned, such as theft, fraud, drug trafficking, defamation, slander, contempt, and moral crimes, since these crimes may occur through material action and may occur via the Internet[300].

There is a part of jurists who said that the scene of the crime of electronic fraud could be the information system or the website. This is done by manipulate with the inputs that the information system or website is intended to process and manage. This can be done in several ways, including:

- Changing the data and information to be entered into the computerized system or deleting any part of it, whether this change and increase is during the entry process or during the preparation stage necessary for the entry, and the process of changing and manipulating all or only part of the information[301].

- The second method is based on deleting all or part of the data during the preparation stage for entry or during the entry process, changing the validity of this information and data, and entering data that is appropriate to the purpose of the fraudster.

---

[300] Decision of the Jordanian Court of Cassation - a public authority - in its criminal capacity - Decision No. 1008 of 2020 dated 7-28-2020.

[301] Al-Maaita, Hamza Atef Ali, , 2012, p. 49

- The third method which is used to manipulate data during the input stage, is called , which is represented in entering information other than the matter assigned to it and hiding it so that it is not seen by those who want to use it , which means disabling the effectiveness [302].

It is necessary to explain, next, how crimes are committed over the Website

5.4 ILLEGAL ACCESS OR BYPASSING AUTHORIZED ACCESS:

Simply accessing the website illegally is considered a crime punishable by Jordanian legislation, as merely viewing the information or data without any change to it, whether by deletion, modification or addition, is in itself considered a crime.[303].

The crime of illegal access to the website consists of two elements: the criminal actand the criminal intent.The crime of illegal access to the Internet is considered an intentional crime in which criminal intent is required.

The Jordanian legislator has considered that intentional entry, with a permit or bypassing that permit, into an information system or information network, regardless of the means, is an act that requires punishment[304].

Iraqi legislation lacks a text regarding this case, and the Iraqi Penal Code also did not address the issue of access to the information network or information system, and the draft Iraqi electronic crimes law has been stagnating for years without its approval[305].

It is noted that Jordanian legislation criminalizes mere access to the website, and this is evident through the financial penalty represented by a fine, or the deprivation of liberty penalty represented by imprisonment. Jordanian legislation does not specify the method of accessing the website, as it can be done by any mean[306].

---

[302] Al-Maaita, the crime of electronic fraud, pg. 50

[303] Skiker, Muhammad Ali, Information crime and how to confront it, 1st edition, p. 36.

[304] Article 3 of the Electronic crimes Law No. 17 of 2023 A - Anyone who intentionally accesses the information network, information system, information technology facility or any part thereof by any means without authorization or in a manner that violates or exceeds the authorization shall be punished by imprisonment for a period of not less than one week and not more than Three months or a fine of no less than (300) one hundred dinars and no more than (600) two hundred dinars, or both of these penalties.

[305] Article Five of the draft of the Iraqi Electronic crimes Project stated: First: Anyone who eavesdrops on any messages via Information network, computer devices, or the like, or captured or intercepted without permission from the competent authority or the owner.

[306] Muhammad, Lina Jamal, 2016, p. 10.

The Jordanian legislator restricted the criminal entry in the law with intent, that is, the entry was intentional and intended for this entry, and accordingly, the unintentional entry is not considered a legal entry[307].

5.4.1 Severity of punishment: Jordanian and Iraqi legislation

The Jordanian legislator stated that the penalty is severe if the target is accessing data or information not available to the public that affects national security, the Kingdom's foreign relations, public safety, or the national economy.

The Jordanian legislator indicated that access, whether authorized or exceeding what is authorized, to information system affects institution or governmental, security or sovereign department, and even banking, and accesses information or data that a natural person cannot access and is not available to the general public and threatens national security or We affect in any way the state's relationship with other countries as an severe circumstance[308]

The draft Iraqi Electronic crimes law is still at a standstill without being approved, but in the draft, if implemented, the Iraqi legislator did not stray far from the Jordanian legislator We note that access with the aim of obtaining information that affects national security or affects the safety of the state and affects its economy is punished more severely.[309].

The Jordanian legislator indicated that access an information system or information network intentionally while knowing that he does not have the right to do so, and if this entry was intended, then his action is legally criminal[310].

in my opinion that the Jordanian legislator did well, as allowing access to information that is not available to the public is inconceivable, as it could lead to undesirable results.

---

[307] Khaled Mamdouh Ibrahim, 2009, p. 242.

[308] Article 4 of the Jordanian Electronic crimes Law of 2023

[309] As stated in Article Five of the draft Iraqi law, what it states: Third: Anyone who intentionally enters a site or A system, computer hardware, or the like, with the intention of obtaining data or information that affects the national security or national economy of the country, or he deletes, destroys, or changes data or information that affects the national security of the country or the national economy.

[310] Paragraph A of Article Three of the Electronic crimes Law No. 17 of 2023 stipulates: Anyone who intentionally enters or accesses the information network, information system, information technology facility or any part thereof by any means without authorization or in a manner that violates or exceeds the authorization shall be punished with imprisonment for a period not exceeding Less than a week and not more than three months, or a fine of not less than (300) three hundred dinars and not more than (600) six hundred dinars, or both of these penalties.

5.4.2 Elements of The Crime of Illegal access

5.4.2.1 The Criminal Act

It is the act of use that must be done without right in a way that would harm the victim. Here, the crime of unauthorized access or bypassing the permit is represented by the perpetrator's attempt to access an information system or website that he is not authorized to enter or view.

5.4.2.2 The Criminal Intent

The criminal intentis the general criminal intent consisting of elemental cause and the will, and knowledge in the sense that the perpetrator knows that he uses objects owned by others without their consent and without the right to do so, as well as the intention of his will[311].

The special criminal intent for this crime, which the legislator made a reason for sever the punishment, as he indicated in the article3/B of the Electronic Crimes Law that if the goal of entry is to destroy, add, disclose, or publish any change, and not just entry, then this is considered a reason for the presence of the specific criminal intent and is considered an aggravating circumstance. The Jordanian legislator indicated that entering an information system or information network intentionally while knowing that he does not have the right to do so, and if this entry was intended, then his action is legally criminal[312]

[311] Paragraph A of Article Three of the Electronic crimes Law No. 17 of 2023 stipulates: Anyone who intentionally enters or accesses the information network, information system, information technology facility or any part thereof by any means without authorization or in a manner that violates or exceeds the authorization shall be punished with imprisonment for a period not exceeding Less than a week and not more than three months, or a fine of not less than (300) three hundred dinars and not more than (600) six hundred dinars, or both of these penalties.

[312] Paragraph B of Article Three of the Electronic crimes Law No. 17 of 2023

5.5 THE CRIME OF FORGERY INFORMATION:

5.5.1 Definition of the Crime

The crime of forgery is defined as a crime against the integrity of a protected electronic editor, any act of alteration of the content of information documents by means of intentional deletion, modification or addition in a valid electronic editor, with the intention of harming others[313].

5.5.2 The Reason Why the Crime of Forgery Information Is Considered the Most Serious Crime:

The crime of forgery information is considered one of the most serious and harmful forms of cheat in the field of automated data processing, and the reason why the crime of electronic forgery is considered the most serious crime, as it results in undermining the trust that must be provided and maintained in information documents regardless of their nature[314].

5.5.3 Images of Information Forgery Crime

The crime of information forgery is achieved by the insert, deletion or alteration of data and machine-processed software so as to affect the natural flow of such data. Electronic forgery images include the forgery of electronic signatures and the forgery of electronic documents and replacing them with false and misleading data, the distortion of facts, the withholding of accurate information and the incorporation of unrelated information[315].

5.5.4 Reason for Criminalizing the Information Forgery

Forgery in documents has been criminalized because it threatens the general confidence of individuals in them, since the written document is considered an essential means of civil and commercial evidence in all matters that require proof in writing, and since the computer replaced papers in many fields, it was necessary for legislation to provide protection for electronic documents[316].

---

[313] Salama, Mohamed Abdullah, 2006, p. 71.

[314] Al-Qahwaji, Ali Abdel-Qader, 2007, p. 307.

[315] Article entitled NATO Anti-Counterfeiting Technology, https://www.aljazeera.net/

[316] Tamam, Ahmed Hussam, , 2000, p. 387

The Jordanian legislator explicitly indicated that if access is aimed at deleting, destroying, destroying data, or reducing its confidentiality, it is a penalty requiring imprisonment[317].

In this regard, the Jordanian Court of Cassation, in its criminal capacity, upheld the decision of the Court of Appeal to amend the criminal description of the crime of forgery, in contravention of the provisions of the Penal Code, the Economic Crimes Law, and the Integrity and Anti-Corruption Law, by criminalizing access to the information network or information system in excess of authorizing the deletion of data and information, otherwise. According to the provisions of Article (3/B) of the Electronic crimes Law[318] .

It appears from this adjudication that the court adopted the minimum criminalty, in both parts, a fine, as it decided two hundred dinars and imprisonment, as it sentenced the accused to three months imprisonment.

As for Iraqi legislation, it lacks a legal text with regard to the crime of forgery information, but can the general penal text be taken into account with regard to the crime of forgery, and can this text be applied to the crime of forgery information?

We notice here that the Iraqi judge is trying to use traditional texts to address this clear deficiency, as in this crime he returns to the texts of the Penal Code.

Anyone who commits forgery in an ordinary instrument that creates or confirms a debt or disposes of money, a release or settlement, or an ordinary instrument that can be used to prove ownership rights, shall be punished by imprisonment for a period not exceeding seven

---

[317] Jordanian Electronic crimes Law No. 17 of 2023, Paragraph (B) of Article Three thereof stipulates: If the entry or access stipulated in Paragraph (A) of this Article is to cancel, delete, add, destroy, disclose, publish, re-publish, or destroy Or blocking, modifying, altering, transferring or copying data or information, or losing its confidentiality, or encrypting, stopping, or disrupting the operation of the information network, information system, or information technology, or any part thereof. The perpetrator shall be punished by imprisonment for a period not less than three months and not exceeding one year, and a fine not exceeding one year. less than (600) six hundred dinars and not more than (3000) three thousand dinars. The penalty shall be imprisonment for a period of not less than one year and not more than three years and a fine of not less than (3000) three thousand dinars and not more than (15,000) fifteen thousand dinars. If he can achieve the result

[318] Decision of the Court of Cassation in its criminal capacity No. 3087 of 2022 dated 9/19/2022 , , has upheld the Court of Appeal's decision to amend the criminal description of the crime of forgery, contrary to the provisions of articles 260 and 263/1 of the Criminal Code, articles 2, 3, 4 and 5 of the Economic Crimes Act, article 16/a of the Integrity and Anti-Corruption Act, to criminalize access to the information network or information system in excess of the authorization to delete and place data and information, contrary to the provisions of article 3/b of the Electronic crimes Act, and to sentence him to three months' imprisonment, and (200 dinars) fees and fines

years or by detention.The penalty shall be imprisonment if forgery is committed in any other ordinary document[319]

In the absence of a conclusive text in Iraqi legislation on the crime of Forgery of electronic information, jurisprudence expands the meaning of the traditional text that criminalizes falsification. This is justified by indicating that the electronic document has legal value of proof and that there is a relationship between the crime of falsification and the electronic document that has this value, so the falsification of electronic documents can be included through the general criminal text[320].

Or that the judge does not impose a penalty for the crime of electronic forgery, based on the absence of a specific legal text that criminalizes the penalty for electronic forgery, and based on what a group of jurists have stated, it is not possible to expand the traditional texts contained in the general criminal law to include electronic forgery. . This trend was justified by not including the crime of electronic forgery. Under the general criminal text for the crime of forgery, the data stored in the computer's memory is not considered readable in itself because it is recorded electronically on a support that can be read through the computer, which negates the quality of the document.[321].

The crime of information forgery may be through deleting [322] or adding [323] or modifying data or information.

In my opinion I believes that the traditional legislative text cannot be extended to include electronic transactions, as forgery in the traditional text, as we see in Iraqi legislation, is unable to address forgery in the electronic document. It is not logical to remain in the circle of jurisprudential opinions and court rulings. There must be a clear text. Accordingly, the researcher believes that the legislator is committing a major mistake in not filling the clear

---

[319] Article 295 of the Iraqi Penal Code No. 111 of 1969 and its amendments. The draft of the Iraqi Electronic crimess Project criminalized the crime of electronic forgery, as Article Five/Second of the draft draft stipulated: He shall be punished by imprisonment for a period of not less than two years and not more than five years and a fine of not less than (3,000,000) three million Iraqi dinars and not exceeding (5,000,000) five million Iraqi dinars. Anyone who intentionally, without authorization, enters an electronic website, information system, computer device, or the like, and views or copies its content, or deletes, deletes, destroys, discloses, or changes data or information owned by others.

[320] Brahmi, Hanan 2014 , p. 175

[321] Farid, Rustom Hisham 1995, p. 328.

[322] What is meant by deletion here is the deletion of data or information, regardless of whether it is a text, image, video clip, or audio recording, from the electronic space occupied by a legal or ordinary person on the Internet, and which has harmful effects on the victim, third parties, or both. Al-Sayed, Atef, Education and Information Technology and the Use of Computer and Video in Learning and Teaching, Ramadan Press for Publishing and Distribution, Alexandria, 2000, p. 91).

[323] What is meant by addition here is adding data or information, regardless of whether it is a text, image, video clip, or audio recording, to the electronic space occupied by a legal or ordinary person on the Internet, and which has harmful effects on the victim, others, or both. (Al-Sayed, Education and Information Technology, pg. 91).

legislative deficiency. Since there is no text that includes this type of crime, there is no solution other than expanding the traditional text and trying to apply it to this type of crime.

5.5.5 Elements of the Crime of Electronic Forgery

5.5.5.1 The Criminal Act

Which is changing the truth in an electronic document in one of the ways specified by the law.

It consists of many elements, namely:

- Changing the truth, which is the basis on which the crime of forgery is based, by changing the truth on electronic documents using a computer.
- The presence of the editor, which is the scene of the crime, and is composed of letters or signs indicating a specific meaning or idea.
- Harm, and by the harm we mean the harm that is caused by the breach of trust in electronic documents, its impact on legal security, and its serious impact on the public interest of individuals. Therefore, it is necessary to refer to the general rules of the provisions of the harm in achieving or possibly achieving it, and to indicate its type and how to compensate for it[324].

5.5.5.2 The Criminal Intent

Which is the perpetrator's intention to change the truth in an electronic document, knowing that this act is criminalized and punishable by law[325]. The specific criminal intent in the crime of electronic forgery is that the perpetrator has the criminal's intention to use the document that has been forged and the intention of his will to commit the act of forgery, with his knowledge of that[326].

The offender must also know that he is changing the truth in a document in one of the legally stipulated ways. If he did not know that, then there is no criminal intent, even if his ignorance was due to his negligence in verifying that. This knowledge is assumed, so he does not lose responsibility for that due to his ignorance, as he should know. His action may cause actual or potential harm to others. If this is not the case, then intent is also absent. The offender's intention must also be to use the document for what it was forged, even if it is not

[324] Al-Obeidi, Saddam and Awwad Hussein, 2020, p. 232

[325] Al-Obeidi, Saddam and Awwad Hussein, 2020, p. 232.

[326] Abdullah, Fahd bin Saad 1996 , p. 293.

used. There is no point in denying the perpetrator of this accusation by saying that he did not receive his benefit[327]

5.6 THE CRIME OF DESTROYING INFORMATION:

5.6.1 Defining the crime of destroying information:

destroying is the destruction of the object of the crime scene by damaging or devaluing it by rendering it unusable or ineffective [328] , or it is the effect upon the substance of an object in such a way as to detract or reduction its economic value by diminishing its efficiency for the intended use [329].

The destruction of information has become a major target for perpetrators who are attempting to target information data by destroying it in various ways, whether it is completely destroyed or by corrupting it so as not to become usable[330].

5.6.2 Ways to Destroy Information

The crime of destruction of information is carried out by many means, the most important of which is viruses, which are a set of coded instructions that allow themselves to replicate and automatically join application programs and system components to control the performance of the system they are infected with at a certain stage[331].

A computer virus is a small harmful program that copies itself and multiplies like a real virus, and it harms and sabotages programs and files in the computer or causes harm to the computer[332].

There are many types of viruses, such as the ransomware virus [333] and the worm virus [334] and the Trojan horse virus [335] and the ticking time bomb virus [336] and it causes harm to the

---

[327] Rostom, Hisham, Mohamed Farid, , 1995, , Assiut.

[328] Al-Khaili, Crimes illegally used on the Internet, p. 218

[329] Huda, , 1993, p. 564

[330] Qashqoush, Hoda Hamed, Computer Crimes and Other Crimes in the Field of Information Technology, p. 558.

[331] Tolba, , 1992, p. 29.

[332] The art of computer virus research deferns

[333] The malicious ransom virus struck, within one day, the data and systems of thousands of institutions, companies, hospitals, financial institutions, and major factories in one hundred and fifty countries through electronic assaultss, and then this software encrypts the data stored on it, and that encryption is only

moral components of the computer or disable computer networks from performing their tasks [337].

Viruses are spread through removable media such as optical disks, flashes, corporate file servers, e-mail, inbox documents, pixels and other types, websites, newsgroups or pirated software[338].

One of the images of information destruction is the informational flooding of email, where this file starts sending hundreds of emails to the injured targeted machine using all the names of e-mail accounts stored on it, which results in badly affecting a huge number of personal computers of individuals and companies, and the filling of e-mail servers with that message. Such an assault took place on America Online, and the losses due to these assaults amounted to about $50 million[339].

Among these is the crime of disrupting Internet services through the crime of dumping directed at servers, and this crime is available in its material corners once the perpetrator causes a disruption that prevents users from communicating with the Internet[340] .

The Jordanian legislator has criminalized the crime of destroying information. The Jordanian legislator has indicated that if access is aimed at deleting, destroying, destroying, or

---

decrypted by paying three hundred US dollars for each computer that is encrypted or is Destruction of data and information within a period of time specified by the hacker These assaultss were described as the largest in history, and this was followed by another cyber assaults that affected more than a hundred countries around the world, targeting information, data and their systems in companies operating in the pharmaceutical, shipping and advertising industries. It was called the malicious beta program. (Al-Zindani, Ibrahim Muhammad, Electronic crimes from the perspective of Islamic law and its provisions in Qatari law and Yemeni law, Pattani University, 2018, p. 59).

334 A worm virus, which is a software that moves from one computer to another, especially by self-activation. This virus causes the keyboard and screen to freeze and the computer to slow down. (Ibrahim, Khaled Mamdouh, Electronic crimes Security, University Publishing House, Alexandria, 2008, pg. 73).

335 Trojan horse virus This virus appeared in England in 1989 by a person called Bob from America and this virus was sent via discs and affected by this program about twenty thousand from England This program hides inside the program in memory, then it activates at the specified time and executes the order given to it by destroying or distorting the information. (Mattar, Essam, Electronic government between theory and practice, p. 140).

336 The time bomb virus, which is a virus that remains dormant until a specific event occurs, a specific word that the user may write, or a specific date that starts its work through its memory location, then activates and destroys the program. (Ibrahim, Electronic crimes Security, p. 74).

337 Shawa, Mohamed Sami, 2002, p. 132.

338 Al-Munaifi, Ahmed Muhammad Abdel-Raouf, Computer Viruses and Their Rule in Islam and Contemporary Laws, p. 16.

339 Al-Zindani, Electronic Crimes, p. 63.

340 Al-Khaili, Crimes illegally used on the Internet, p. 236

adding and providing many similar images, then here we are faced with the crime of destroying information[341].

The decision of the Court of Cassation of Jordan in its criminal capacity stated that: "Since the reason for the appeal relates to the failure of the Court of Appeal to apply the legal text, the Public Prosecutor has assigned the defendants (M. (f) and (m) The crime of destroying and disrupting an information system jointly contrary to the provisions of Article 3 (b) of the Information Systems Crimes Act and the significance of Article (76) of the Criminal Code , the Court of Appeal, before dropping the public right action pursuant to the provisions of Article (3.2.a) of the Code of Criminal Procedure, had to verify, starting with the existence of a law called the Code of Information Systems Crimes, and then, after that, whether the crime committed was one of the crimes mentioned in Article (3.1.a) of the Code of Criminal Procedure, and then consider whether the requirements of Article (3.2.a) of the Code of Criminal Procedure had been met . And since the Court of Appeal went to the opposite, it thus violated the law, which makes the reason for the appeal included in its decision and it must be overturned[342].

As for Iraqi legislation, it lacks a legal text regarding the crime of destroying informationThe legal problems that result from the lack of approval of the draft Electronic crimes law become clear here, as the draft law criminalizes in Article Five entry into an information system with the aim of destroying or modifying data.[343]

---

[341] Paragraph (b) of Article Three of the Electronic crimes Law No. 17 of 2023 stipulates: If the entry or access stipulated in Paragraph (a) of this article is to cancel, delete, add, destroy, disclose, publish, re-publish, destroy or block Or modify, alter, transfer, or copy data or information, or lose their confidentiality, or encrypt, stop, or disrupt the operation of the information network, information system, or information technology, or any part thereof. The perpetrator shall be punished by imprisonment for a period of not less than three months and not exceeding one year, and a fine of not less than (600) six hundred dinars and not more than (3000) three thousand dinars. The penalty shall be imprisonment for a period of not less than one year and not more than three years and a fine.

[342] Decision of the Court of Cassation in its criminal capacity No. 570 of 2018 dated 21-2-2018

[343] The draft of the Iraqi electronic crimes project criminalized the destruction of information, as Article Five/Second of the draft draft stipulated: He shall be punished by imprisonment for a period of not less than two years and not more than five years and a fine of not less than (3,000,000) three million Iraqi dinars and not exceeding (5,000,000) five million Iraqi dinars each. Whoever intentionally, without authorization, enters a website, information system, computer device, or the like, and views or copies its content, or deletes, deletes, destroys, discloses, or changes data or information owned by others.

5.6.3 Elements of the crime of destruction

5.6.3.1 The criminal actin in the crime of destruction:

First:

The criminal activity may be through destruction, which is the loss of usability, destruction, making the thing unfit for use, or disabling the thing, i.e. hindering it from working in whole or in part[344].

Second:

The crime scene the scene of the crime is the non-material components, which means providing the information system by destroying it or erasing the program instructions or the data itself. The destruction is not intended to be done here simply to obtain the benefit of the computer in whatever form, but to cause harm to the information system and to impede its functioning[345].

5.6.3.2 The Criminal intentin inThe Crime of Destruction

The criminal intentis criminal intent and the crime does not require special intent. The general intent is sufficient with respect to the racial nature of knowledge and will. Knowledge is available in the event that the perpetrator is aware that his behavior would harm the situation of others in a manner which would be wholly or partly without legitimate proof, knowing that the money belongs to others. The availability of criminal intent also requires that the result of the perpetrator's will is to cause harm, sabotage, disruption or unusability of the information system[346] .

On the other hand, a side of jurisprudence had a different opinion and said that the special criminal intent in this crime is represented by the intention to achieve profit or harm othersSome have criticized the requirement of special criminal intent in the crime of destroying information because it leads to excluding many acts of destruction and not criminalizing them when the perpetrator’s intention is not to achieve financial gain or harm others despite the value of the destroyed information. Also, estimating losses should not be limited to material damage only. that befalls the victim[347].

---

[344] Al-Khaili, Crimes illegally used on the Internet, p. 220

[345] Al-Khaili, Crimes illegally used on the Internet, p. 221

[346] Kamel, Computer Crimes, p. 209

[347] Aoun, Asmahan 2021, , 2021, p. 365

The Jordanian legislator referred to special criminal intent in Article (3/C) of the Electronic Crimes Law No. 17 of 2023 we note that the Jordanian legislator limited the cases that represent the special intent in this article[348]

In my opinion, the legislator made a mistake here, so it would have been better not to mention the cases and only mention the act of destruction so that this text would be able to accommodate all the actions that represent destruction. Or to add a phrase, but not limited to it

5.7 The Crime of Stealing Information

Assaults on information system software may be through manipulation in various forms, such as by implanting a subprogram in the original software that allows it to illegally access the necessary elements of the information system, where it is difficult to detect such a program for its accuracy and small size[349].

Driver programs, which are the programs responsible for the functioning of an information system in terms of organizing and adjusting the order of instructions for the system The crime provides the program with an additional set of instructions to facilitate access by code that allows access to all the data contained in the information system, taking two forms: the catch, which is the preparation of a program with corridors, gaps in the program and additional branches. The programmer can use the program at any time and becomes its controller and owner. Or design a program specifically for this purpose, which is to commit the crime, so that this program is difficult to detect[350].

5.7.1 Definition of the crime of stealing information

They include unauthorized access or unauthorized access to a system or group organized through security procedure violations, as well as unauthorized interception through certain means of communication directed to a computer system, several systems or a communication network[351].

The theft of information and data processed automatically is intended to be seized without the knowledge and will of its rightful owner and may be carried out by the capture of

---

[348] Article (3/C) of the Electronic Crimes Law No. 17 of 2023: Anyone who intentionally accesses or accesses a website to change, cancel, destroy, modify its contents, occupy, encrypt, stop, disable, impersonate its capacity, or impersonate its owner shall be punished. Imprisonment for a period of not less than three months and a fine of not less than (600) six hundred dinars and not exceeding (3000) three thousand dinars.

[349] Report of the Council of Europe 15-18- November 1975

[350] Al-Malt, Ahmed Khalifa, 2006, p. 175.

[351] Yunus, Arabs, 2002, p. 320

electromagnetic waves transmitted by the computer, which are then processed and have visible information on the screen[352].

So-called breach is the illegal copying of software or the improper acquisition of information stored directly or indirectly in computer memory[353].

5.7.2form of Information theft

Information theft has many form, including ([354]):

- Stripping a digital work of its value by taking possession of it while the original remains in the possession of its owner.
- Depriving the right holder of the desired benefit from his right.
- Intellectual piracy through copying the digital work scene to legal protection.
- Emulating a specific program by producing copies so that when they are marketed they look like original.

The researcher, Dr. Nahla Al-Momeni, goes on to say that theft of information stored in a computer or exchanged via the global information network (the Internet) still needs Jordanian legislation to ensure its protection from the dangers of theft[355]. .

in my opinion, as a comment Dr. Al-Moumni's statement that the Jordanian legislator has protected information from the dangers of its theft by criminalizing theft of information in the Electronic crimes Law, which stipulates, Paragraph (b) of Article Three of the Electronic crimes Law No. 17 of 2023 stipulates: If the entry or access stipulated in Paragraph (a) of this article is to cancel, delete, add, destroy, disclose, publish, re-publish, or destroy Or blocking, modifying, altering, transferring or copying data or information, or losing its confidentiality, or encrypting, stopping, or disrupting the operation of the information network, information system, or information technology, or any part thereof. The perpetrator shall be punished by imprisonment for a period not less than three months and not exceeding one year, and a fine not exceeding one year. Less than (600) six hundred dinars and not more than (3000) three thousand dinars. The penalty shall be imprisonment for a period of not less than one year and not more than three years and a fine of not less than (3000) three thousand dinars and not more than (15,000) fifteen thousand dinars. If he can achieve the result

---

[352] Saleh, Nael Abdel-Rahman, Volume 1, 2004, p. 50

[353] Sheta, Muhammad, , 2001, p. 91.

[354] Al Khalayleh, Ayed Raja, 2011, p. 100.

[355] Al-Moamini, Nahla Abdel-Qader, 2010, p. 100

The Iraqi legislator was also very close to the Jordanian legislator, and in his draft project, the Iraqi text, if applied, was close to the Jordanian text.[356]

The definition of the crime of theft in the Jordanian Penal Code is taking the property of others without their consent, meaning that possession of the thing scene to the theft is transferred from the owner to the thief. In my opinion, some of the expression mentioned in this article, such as copying, republishing, modifying, transferring, etc., are consistent with the concept of possession contained in the traditional text means the transfer of possession and ownership of data or information from its owner to the thief

5.7.3 Elements of the Crime of Electronic Theft

5.7.3.1 The Criminal Act.

Which is the disclosure, transmission or copying of data or information in an electronic document in one of the ways specified by the law.

It consists of many elements, namely:

- Stealing information or data is the basis of a crime by stealing such information or data that pertains to the perpetrator.
- The presence of the editor is the object of the crime scene and is made up of letters or signs indicating a certain meaning or idea.
- Harm is harm that is caused to the victim by the theft of the victim's information or data and the loss of profits that would have been caused by the retention of such data or information[357].

5.7.3.2 The Criminal intent.

Which is the will of the perpetrator represented in stealing this information and data, knowing that this act is criminal and punishable by law[358]. The specific criminal intent is

---

[356] The draft of the Iraqi electronic crimes project also criminalized the destruction of information, as Article Five/Second of the draft draft stipulates: Each person shall be punished by imprisonment for a period of not less than two years and not more than five years and a fine of not less than (3,000,000) three million Iraqi dinars and not exceeding (5,000,000) five million Iraqi dinars. Whoever intentionally, without authorization, enters a website, information system, computer device, or the like, and views or copies its content, or deletes data or information owned by others.

[357] Al-Obeidi, Saddam and Awwad Hussein, , 2020, p. 232.

[358] Al-Obeidi, Saddam and Awwad Hussein, 2020, p. 232.

achieved by the perpetrator's intention to possess the stolen item using the canonical method[359]

It was said that criminal intent is achieved by simply violating the programmer's information system, which has a password or technical system that indicates the presence of intent and bad faith on the part of the perpetrator[360].

5.8 Criminal Liability of the Electronic Service Provider:

5.8.1 Definition of Criminal Liability and Service Providers:

In order to enable the users of electronic services to access the Internet, it is necessary to join forces with many people to provide this service. The roles of electronic service providers are divided between storage, broadcasting and presenting information. Hence, it is necessary to get to know each of them before talking about the provisions of the criminal liability of electronic service providers.

In the field of legal relations for electronic transactions, third party liability was raised. Specifically, are Internet service providers, web hosts, or those charged with site registration asked about website activities that deceive the existence of an electronic business, whether it exists or not? And legislation tends to exempt the third party from these responsibilities, as it is foreign to the contractual relationship. This is due to the presence of reliable companies that can give the necessary guarantees to the parties to the relationship without the need for companies that provide Internet service, who are the third party in the relationship.[361].

5.8.1.1 Definition of Criminal Liability and Its Forms:

There is no specific definition of criminal responsibility in criminal codes and criminal legislation, but rather the jurisprudential definitions of this term.

Responsibility in general has been defined as: the situation in which a person is held responsible for an act, which presupposes a violating of a legal rule, the violating of which follows a legal responsibility to be met by a criminalty established by law or its terms. The concept of liability extends to a personal commitment to bear the results of the act of a person under his control, administration, mandate or tutelage. The concept of liability also includes

[359] Al-Amayra, Munther Abdel-Razzaq Musleh 2012, doctoral thesis, p. 135.

[360] Ibrahim, Khaled Mamdouh, Information Crimes, p. 87.

[361] Marra Shebl, Al-Shammari, Khaled, 2012, p. 193

the commitment of a person to respect the commitments and conduct imposed on him by law and to bear the results of a violating of that commitment[362].

As for criminal liability, some jurisprudence has defined it as: the commitment of a person to what he pledged to do, or to abstain from it, even if he violates his commitment to be held accountable, then he is obliged to bear the results[363].

While another aspect of jurisprudence proceeded in defining criminal responsibility as: a question directed to the person who committed the legally criminal act, why did he commit the crime? What is the purpose of this act? And why did he breach the adjudications and rules prevailing in society?[364].

Some said that it is the criminal accountability of the person for the crime he committed by applying the rules of the criminal law to him[365].

Criminal liability is personal responsibility, meaning that a person is not held criminally accountable unless he commits the crime or contributes to its commission, whether by instigation, agreement, or contribution.[366].

5.8.1.2 Forms of Criminal Responsibility

There are multiple forms of criminal responsibility. And its impact falls directly on the person's him self, even if its effects are gradual, and its impact is called a felony[367]. Criminal responsibility has occupied great importance in studies and criminal cases, in an attempt to establish a rule that criminalizes and punishes those who violate it[368],

The concept of criminal responsibility was linked, during its development, to the history of its philosophy of law and general philosophy and became a clear legal idea in the late 18th and early 19th centuries. Thus, the intellectual and scientific renaissance of criminal law was born of different philosophical tendencies on the subject of criminal responsibility, and the development of criminal law was always associated with the development of criminal responsibility and its philosophical foundation. The violator of criminal responsibility is, in the definition of the law, a "criminal"; The crime is doing an act that the legislator has

---

362 Marks, Suleiman, Al-Wafi , 1998 p.1

363 Al-Awji, Mustafa, 1982, p. 11

364 Rabei, Hassan Muhammad, 1996, p. 242.

365 Mansour, Mohamed Hussein, 2006, p. 7.

366 Bilal, Ahmed Awad, 1993, p.5.

367 Issa, Mohamed Gamal Attia, 2009 p.5

368 Swailem, Muhammad Ali, 2007 p.10

forbidden and set a criminalty for the perpetrator, or abandoning an act that must be done, and imposing a specific criminalty for those who do not comply with that[369].

Criminal responsibility was not an unknown idea in the old laws, although it differs from its current concept. Criminal responsibility in the old societies was based on spontaneity and materialism, and the idea of revenge was the most prominent, even the only, criminal responsibility , And the idea of revenge also developed, as revenge began as an individual, as the individual was himself responding to the assault that falls on him, but the matter developed later, as the matter shifted from individual revenge to collective revenge, as the aggressor began to take revenge on the aggressor with the help of his family members [370].

The term "criminal responsibility" refers to a violation of a criminal provision of the Criminal Code, according to the legal rule, of which there is no crime and no punishment except by a legal provision and the term "responsibility" in general, which refers to the responsibility of the individual for the commission of an order prohibited by law, such as murder and other crimes punishable by law, or, more clearly, to indicate the meaning of the commitment of a person to bear the results of his or her act or conduct, which he or she has undertaken in violation of certain principles and rules[371].

In the field of electronic transactions, the criminal liability is on the electronic service provider in two cases:

First:

In the event that he is an accomplice to the electronic crimes carried out by a person on the Internet.

Second:

As for the second case in which the criminal liability is based on the electronic service provider, it is when he is aware of the illegal electronic content, and allows it to spread on the electronic network, and we will talk about it later.

[369] Al-Alfi, Ahmed Abdel Aziz, 1969, p. 316-317

[370] Al-Haythami, Muhammad Hammad, 2005 p.10

[371] Odeh, Abdel Qader, 1987, p. 25

5.8.2 Definition of Electronic Service Providers and Their Commitments

5.8.2.1Service providers

Presenter and providers of electronic services do not fall under one type. Rather, there are contractors for electronic services, contractors for storage services, and presenter of informational content.

Service providers provide services of a technical nature, which is to allow the public to connect to the Internet and connect the user to the sites he wants to access[372].

The European approach to electronic commerce has defined the service provider as any natural or legal person who provides Internet service in the information services community[373]. As for the Spanish legislator, it did not address the definition of the service provider in its own legislation, but the European approach, which is adopted by the Spanish legislator, defined it.

As for the French legislation, it was defined as the person whose activity secures the connection service to an electronic communications network[374].

While some have defined it as a company that provides an Internet connection service and is the mandatory passage for users to access it, this commitment is to connect users to the network through modems[375].

The Arab Agreement to Combat Information Technology Crimes defines a service provider as any natural or legal person, public or private, who provides subscribers with services for communication through information technology or processes or stores information on behalf of a telecommunications service or its users[376].

The Jordanian legislator, in Electronic crime Law No. 17 of 2023, defined the service provider as: any natural or legal person, public or private, who provides subscribers with electronic services by means of information technology, or processes or stores information on behalf of the telecommunications service or its users[377].

---

372 Ramadan, Medhat Abdel Halim, 2000, p. 59.

373 European Directive No. 3000/29.

374 Article No. (1) of Law No. 50 of 2003 on trust in the digital economy.

375 Valérie Sédallian, Internet Law: Regulations, Liability, Contras, Collection Association of Internet Users, Net press. ,p 123

376 Article 2 of the Arab Agreement to Combat Information Technology Crimes

377 Article (2) of the Jordanian Electronic crimes Law No. 17 of 2023

As for the Iraqi legislator, he did not define the electronic provider in the Electronic Signature and Transactions Law No. 87 of 2012. Rather, he defined the electronic medium in Article 1/8 of the same law, so he defined it as an electronic computer program or system used to implement a procedure or respond to a procedure for the purpose of creating, sending, or receiving a message. Information. While the draft Iraqi Communications and Information Technology Law, in Article 10, defines the provider as the person who owns and manages a public or private communications network, while the service can be defined as stated in Article 1/3 of the Iraqi Consumer Protection Law No. (1) Of 2010, as Work or activity provided by any party, for or without compensation, with the intention of benefiting from it[378].

As for the first article of the Iraqi draft anti-electronic crimes law in the seventeenth section of the aforementioned article, it defined - the service provider as: Every natural or legal person, public or private, who provides subscribers with services to communicate using information technologies, or who processes or stores electronic data and information on behalf of the communication service and its users.

5.8.2.2 Storage Service contractor

The storage service contractor has been defined in European orientation as an activity of a natural or moral person that aims to store online and web pages on server computers directly and permanently, for a fee or free fee, and through which its clients have at their disposal the technical and information means that enable them at any time to transmit their own texts, pictures and sounds, organize conferences and panels and establish information links with other websites[379].

Also, when we look at the Spanish legislator, we find that it did not address the definition in its legislation the storage service contractor, as it was content with the definition found in the European approach, which the Spanish legislator adopts.

The French legislator defined him as any natural or moral person who, through public Internet communications services, allows the public to store signals, writings, images, sounds or messages of any nature for the benefit of users of such services[380].

While the Jordanian legislator in the Electronic Transactions Law No. 15 of 2015 did not address the concept of the storage service contractor. Similarly, in the Electronic Signature and Electronic Transactions Law No. 87 of 2012, Iraqi legislators have not defined the storage service contractor.

---

[378] Article 1/3 of the Iraqi Consumer Protection Law No. 1 of 2010.

[379] Article (92) of the European Directive on Electronic Commerce No. 3000/29.

[380] Article (2) of Law No. 50 of 2003.

In my opinion i hopes that both Jordanian and Iraqi legislators will define the electronic storage service contractor.

5.8.2.3information content provider

As for the information content provider, he is: as any natural or legal person who transmits information and messages on a particular subject on the Internet, so that the network user can access them for free or for a fee[381].

It has also been defined by some as the author of the message, the person who adds it on the site using various communication services, especially the Internet, or the person who is involved in the creation of the content or one of its elements[382].

5.8.3 The Commitments of Electronic Service Providers, They Are Represented in the Following Matters

After the tasks and duties carried out by electronic service providers have been clarified, and that the electronic service provider is of more than one type, therefore it is not logical that there is no legal organization for them and what are the obligations imposed on them, and this will be explained as follows:

- Material connection of remote communication networks in order to facilitate the process of transferring information.
- Enabling network users to access the information content circulating on the Internet, and this is done by linking computers and smart phones to websites, Often the responsibility of this role rests with the telecommunications authorities in the countries[383].
- As for the mission of the information carrier, it is represented in securing the material transfer of information between the different parties. He performs the process of materially transferring information from one unit to another, and therefore he is not assigned either to monitor the information or to know its content[384].

---

[381] Schuhl christian, 2002, p129.

[382] Stowel (A) and Ide (N), Liability of intermediaries: Legislative and case law news, Law and New Technologies, October 10, 2000, p 1

[383] Al-Nuaimi, Alaa Yaqoub, 2009, p. 3.

[384] Farah, Ahmed Qassem, , 2005, p. 231.

- As for the commitment of the service provider, which is through a subscription contract between him and the person receiving the service, whether natural or legal, he must provide the delivery service in return for the subscription or the price paid by the recipient of the service, The role of the service provider is not limited to civil commitment, it has another role, which is to monitor what is broadcast, so that it does not constitute any legal violation. If service users and recipients are enabled to broadcast content that violates the law, or provide them with content that violates the law, which results in a criminal liability here[385].

5.8.3.1 The Most Important Commitments with Regard to Criminal Liability Are

After clarifying the obligations imposed on service providers in general, we must talk about the obligations related to criminal liability in particular.

- It is obligatory for electronic service providers, in the event of publishing any data or information that threatens the national or economic security of the state, or publishing pornographic materials, to inform the authorities of the addresses of these persons, e-mails, and the personal page of users, which requires obliging electronic service providers to obtain personal information for users in advance[386].

- The commitment of electronic service providers to respect the right to privacy and confidentiality of correspondence[387].

- The electronic service providers must monitor the information that constitutes a crime that threatens the safety and security of the state and inform the competent authorities of that[388].

- Commitment to block websites, links or informational content at the request of the investigation and trial authorities[389].

---

[385] Bayoumi, Abdel-Fattah, New Crimes in the Scope of Modern Communications Technology, National Center for Legal Issues, , p. 10.

[386] United Nations Office on Drugs and Crime, Using the Internet for Terrorist Purposes, United Nations, New York, 2013, p. 132

[387] Al-Ahwani, Hossam El-Din Kamel, 1990, p. 4.

[388] Al-Maraghi, Ahmed Abdel-Ilah, 2020, p. 128.

[389] Mustafa, Khaled Hamed, 2013, p. 22.

5.8.3.2 Trends in Determining the Criminal Liability of Electronic Service Providers and Their Cases

The criminal liability of electronic service providers for the publish of illegal information or data through the Internet service arose from two distinct trends:

- The first approach says that there is no criminal liability on the service providers, and this trend justifies what he went to in this regard that the job of the service providers is a technical job, it is also impossible for service providers to monitor all information via the World Wide Web[390].

- The other trend went to say that it rests on a criminal liability on the providers of electronic services, as imposing criminal liability leads to limiting the spread of illegal information through the World Wide Web, As for not arranging a criminal liability on electronic service providers, it leads to a greater contribution to the spread of illegal electronic information [391].

And those who said that the criminal liability is rests on the providers of electronic services, some of them went to say that the sequential liability serves as a basis for the establishment of criminal liability, and they justified that by analogy with the responsibility resulting from the press publishing in the traditional ways , In the case of press publication, the director or editor-in-chief is held accountable, and if the editor-in-chief is not responsible, the writer is held accountable, and if the writer is not responsible, the typist is held accountable , And if the responsibility does not fall on the character, the seller or the advertisement poster may be held accountable [392].

However, some of those who claim criminal liability have rejected the idea of sequential liability as a basis for criminal liability of electronic service providers. This direction has justified the approach that sequential liability is contrary to the original notion of innocence. The basis of liability is based on the fact that illegal information is disseminated. The task of the editor-in-chief is to find out what is legitimate to publish and what is illegal to prevent the publication of information. If unlawful information is allowed to be made public, then criminal liability follows[393].

As for the French legislator, he took an intermediate approach in determining criminal liability, as he did not exempt electronic service providers at all, Despite this, it did not establish the criminal liability for electronic service providers as a rule, Article 1/22 of Law

---

[390] Pierre TRUDEL, Responsibility on the Internet, text prepared for the Law and Web seminar, Bamako, organized by , May 27, 2002, p17.

[391] Olivier cachard, e-commerce law, RDAI, N 3, 2004, P 394

[392] Atallah, Shaima Abdel-Ghani Mohamed, , 2007, p. 219.

[393] Olivier Cachard, Op. Cit, p 399

No. 719-2000 related to freedom of communications decided that the electronic service provider shall be exempted from criminal liability, except that two cases are excluded, in which the criminal liability is determined, and these two cases are:

The first case:

Non-implementation of the judicial order issued obliging the provider to prevent the recipient of the service from accessing the content of the electronic content.

The second case:

the case of third parties estimating the existence of illegal content that would harm the electronic customer, And alert the service provider of this matter, however, the service provider did not take any action to prevent the publication of this content [394].

As for the French judiciary, the Court of First Instance in Paris confirmed in the EDV case that the service provider is not responsible for the nature of the legality of the information provided to users on the pretext that its work was limited to transferring information from the site to the user[395].

As for the European approach, it went for not holding the electronic service provider accountable unless it is proven that it is the source of the content of illegal information or data , Or in the event that he makes changes to the content during the transfer and storage process in a way that makes it appear in an illegal capacity, or in the event of failure to stop the transmission of illegal content despite his knowledge of that, or in the event of his refusal to cooperate with the judicial authorities if he was asked to do so [396].

The American legislator did not deviate much in this regard from the European and French legislation. The responsibility of the service provider in the American legislation is limited to two cases:

The first case:

The appearance of the illegality of the informational content to an extent that it cannot be ignored.

---

[394] For more, see Al-Ghafri, Saeed bin Muhammad, Compensation in Electronic Dealing, PhD thesis, Naif Arab University for Security Sciences, Riyadh, p. 309.

[395] https://www.google.com/ =W.W.W-France.html.action.jugement

[396] Article 29 of the European Orientation.

The second case:

The affected person or the government authorities informed the service provider of the illegality of the content, yet the electronic service provider did not take any action in this regard.

The US Judiciary has determined criminal liability for crimes committed online, in Cube v. Cambio surf, criminal liability is established The facts of the case are that CambioSurf is an electronic library service on the Internet that includes daily press releases for people working in another enterprise, The court ruled that the constitutional guarantees of freedom of expression stand in the way of the criminal liability of the distributor for what the read material contains of phrases that contain defamation or insult [397].

The Jordanian legislator resolved the situation and did not leave the issue unclear, unlike the Iraqi legislator, in which we still see very clear legislative lack. The Jordanian legislator determined criminal liability on the service provider, forcing him to provide the authorities, through a judicial order, with all the data they need to reveal the truth and stop broadcasting and displaying any content, in accordance with He also issued a judicial order and specified punishment for anyone who does not comply with a judicial order[398]

---

[397] Awad, Mohamed Mohieldin, 1998, p. 26.

[398] Article (33) of the Jordanian Electronic crimes Law stipulates:

A- To the competent public prosecutor or to the competent court, and when the information system, website, service provider inside or outside the Kingdom, social media platforms, or the person responsible for any account, public page, public group, channel, or anything similar publishes any materials that violate the provisions of this law. Or the legislation in force in the Kingdom, issuing an order to those in charge of it to take the following:

1- Remove, block, stop, disable, record, intercept the flow of data or any publication or content, prevent access to it, or block the user or publisher temporarily during the period specified in the decision.

2- Providing them with all the necessary data or information that helps reveal the truth, including the data of the owner or user of the website or information system that helps determine his identity and conduct legal prosecution.

3- Urgent preservation of data and information necessary to reveal the truth, store them and maintain their integrity.

4- Maintaining confidentiality.

B- In the event that those in charge of the information system, social media platform, website, or service provider do not respond or refuse to the order stipulated in Clause (1) of Paragraph (A) of this Article, or if urgency requires it, the competent public prosecutor or the competent court may By a reasoned decision, an order is issued to the competent authorities to block the information system, website, social media platform, or service on the national network, or prohibit access to violating content.

C- Anyone who refrains from implementing or violates the orders of the public prosecutor or the competent court and does not exceed (30,000) thirty thousand dinars shall be punished with a fine of no less than (15,000) fifteen thousand dinars and no more than (30,000) thirty thousand dinars.

While the draft Iraqi project did not address the responsibility of the service provider. This necessitates further review of the draft of this project and its approval

5.9 Criminal Protection for Service Recipients

Criminal protection is considered one of the most important types of legal protection in general, and it is achieved through rules and legislative texts that criminalize and punish the legislator for prejudice to important interests, the latter include in the scope of electronic security the protection of many elements[399].

5.9.1 Elements to Be Protected In the Field of Electronic Security

Protection includes the following elements[400]:

First the Information System

A set of programs, applications, social media platforms, devices, or tools designed to create data or information electronically, or send, receive, process, store, manage, or display it by electronic means[401].or a set of programs and tools that are used in the processing and management of electronic data [402].

Secondly Information

It is data that has been processed and has meaning[403] or it is the content of the electronic material, whatever the form of the content in it is text, image, audio, video, and the like[404].

Third Data

It is everything that can be processed, stored, supplied, or transmitted using information technology, including writing, images, numbers, videos, letters, symbols, signs, etc[405]. . Or they

---

399 Al-Saifi, Abdel-Fattah Mustafa, The criminal rule, , p. 3.

400 El-Gamal, Hazem Hassan, 2015, p. 17

401 Article 2 of the Electronic crimes Law No. (17) of 2023

402 Item 9 of Article 1 of the Iraqi draft electronic crimes draft.

403 Article 2 of the Electronic crimes Law No. (17) of 2023.

404 The thirteenth item of the first article of the draft Iraqi electronic crimes.

405 Article 2 of the Electronic crimes Law No. (17) of 2023.

are numbers, letters, symbols, shapes, sounds, images, and everything that is stored, processed, generated, produced, and transmitted by computer or any other electronic media[406].

Fourthly the Information Network

It is a link between more than one information systems or any information technology means to make and obtain data and information available[407] or it is a link between more than one information system to obtain or exchange information. [408] .

Fifth the website

It is a space for making information available on the information network through a specific address[409] or is the place where electronic information is made available on the information network through a specific address[410].

5.9.2 Criminal Protection for Service Recipients through Criminal penalties for Electronic crimess

5.9.2.1 A Voluntary Punishment, Which Is Imprisonment or a Fine

It is a penalty stipulated by the Jordanian legislator in the event of illegal access to the information network or information system, whether this access is without a permit or in a manner that violates or exceeds the permit. The penalty for depriving freedom of imprisonment must not be less than a week and not exceed three months, and the fine should not be less than less than 300 dinars and not more than 600 dinars. The legal text has empowered the judiciary to choose one of the two punishments or to combine them[411].. The draft of the Iraqi electronic crime Project makes no mention of a criminalty of voluntary.

---

[406] The third item of the first article of the draft Iraqi electronic crimes.

134 Article 2 of the Electronic crimes Law No. (17) of 2023.

[408] The twelfth item of the first article of the draft Iraqi electronic crimes.

[409] Article 2 of the Electronic crimes Law No. (177) of 2023.

[410] The fifteenth item of the first article of the Iraqi draft electronic crimes project).

[411] Paragraph (A) of Article (3) of the Jordanian Electronic crimes Law No. (17) of 2023 stipulates: Anyone who intentionally enters or accesses the information network, information system, information technology facility, or any part thereof, by any means without permission or without permission shall be punished. Whoever violates or exceeds the authorization shall be imprisoned for a period of not less than one week and not more than three months or a fine of not less than (300) three hundred dinars and not more than (600) six hundred dinars, or with both of these two penalties.

5.9.2.2 A double Punishment, which is both imprisonment and a fine

It is a penalty stipulated by the Jordanian legislator in the event of access to the information network, an information system, or a website and any change occurs, regardless of the type of this change. Here, the penalty of imprisonment and the penalty of a fine are combined. Despite the provision for combining the two penalties, the judiciary still has a discretionary role between the two limits of the penalty. The lowest and the highest[412].

> While we see that the draft of the Iraqi electronic crimes project stipulates the penalty of combining a fine and a prison sentence for illegal entry without causing a change. It also decides to combine the penalty of imprisonment with a fine and more severely in the event of a change, whatever its nature. It also leaves the judiciary to estimate both penalties at their minimum. And the highest. The first clause of Article Five of the draft of the Iraqi Electronic Crimes Project stipulates: Anyone who eavesdrops on any messages via Information network, computer devices, or the like, or captured or intercepted without permission from the competent authority or the owner. While the first clause of Article Five of the draft of the Iraqi Electronic crimess Project stipulates: Anyone who intentionally enters without He is authorized to have an electronic website, information system, computer device, or the like, and he has accessed or copied its content, or deleted, deleted, destroyed, disclosed, or changed data or information owned by others.

5.9.2.3 Confiscation

Confiscation: adjudication to expropriate certain things and add them to the ownership of the state forcibly on behalf of their owner without charge[413].

The Jordanian legislator has granted the court competent to consider electronic crimes cases to confiscate the devices, tools, means and materials used in committing electronic crimess, and has also granted it the right to confiscate the funds obtained from these crimes[414].

---

412 Paragraph (b) of Article Three of the Jordanian Electronic crimes Law No. 17 of 2023 stipulates: If the entry or access stipulated in Paragraph (a) of this article is to cancel, delete, add, destroy, disclose, publish, re-publish, or destroy Or blocking, modifying, altering, transferring or copying data or information, or losing its confidentiality, or encrypting, stopping, or disrupting the operation of the information network, information system, or information technology, or any part thereof. The perpetrator shall be punished by imprisonment for a period not less than three months and not exceeding one year, and a fine not exceeding one year. less than (600) six hundred dinars and not more than (3000) three thousand dinars. The penalty shall be imprisonment for a period of not less than one year and not more than three years and a fine of not less than (3000) three thousand dinars and not more than (15,000) fifteen thousand dinars. If he can achieve the result.

Paragraph C of the same article stipulates: Anyone who intentionally accesses or accesses a website to change, cancel, destroy, modify its contents, occupy, encrypt, stop, disable, impersonate or impersonate its owner, shall be punished by imprisonment for a period of not less than three months and a fine. Not less than (600) six hundred dinars and not more than (3000) three thousand dinars.

413 Al-Darini, Muhammad Fathi, 1994, p. 105.

As for the draft of Iraqi electronic crimes, it required the competent court to rule to confiscate devices, programs and media used in electronic crimes[415].

Here we notice the clear similarity between the Jordanian legislator and the Iraqi legislator regarding the obligation of confiscation.

In my opinion, the Jordanian legislator did well when he made the last amendment to this law, as previously he had given the judge the power to confiscate or not to confiscate, and this is a legislative flaw, but in the last amendment to this law he followed the approach of the Iraqi draft, where confiscation became obligatory, and he did well.

5.9.3 Criminal Protection for Service Recipients by Severre the Punishment

Jordanian legislation Severre the punishment for the electronic crimes perpetrator in two cases, namely, when the perpetrator was an employee, and the other case when the crime was repeated. While the draft of the Iraqi electronic crimes bill toughened the punishment for the employee, but neglected the issue of repetition of the crime. We present both of these cases:

5.9.3.1 Severre the Punishment If the Perpetrator Is an Employee:

An employee may not make his work a starting point for committing a crime or exploit his job to facilitate others to commit a electronic crimes. Therefore, Jordanian

---

[414] Paragraph (a) of Article (31) of the Electronic crimes Law No. 17 of 2023 stipulates: Without prejudice to the rights of bona fide third parties, in the event of conviction, the court shall rule on its own initiative as follows:

1- Confiscation of devices, programs, tools, means or materials used in committing any of the crimes stipulated in this law or the funds obtained from them.

[415] Article 19 of the draft Iraqi electronic crimes stipulates: Without prejudice to the rights of bona fide third parties, the competent court must rule in all cases as follows:

Confiscation of all devices, programs, or media used in committing any of the crimes stipulated in this law, or the funds obtained from them.

Closing down the shop or project in which any of the crimes stipulated in this law were committed if they were committed with the knowledge of its owner , The closure may be permanent or temporary, for a period determined by the court in light of the circumstances and circumstances of the crime.

legislation has doubled the penalty[416] while the draft of the Iraqi legislator went to say the most severe punishment[417].

5.9.3.2 Severre the Punishment in Case of Recurrence

The Jordanian legislator stipulates that the penalty will be doubled if it is repeated[418] which is a good thing that the Jordanian legislator did so that the perpetrators of these crimes would be deterred when thinking of re-committing them, This is something that was overlooked by the draft of the Iraqi electronic crimes project and did not refer to it in any of its texts.

5.9.4 Criminal Protection for Service Recipients through Mitigation or Exemption from Punishment:

The Jordanian legislator Mitigation the criminal penalty for those who committed a cybercriminal crime in some cases, but it did not exempt this penalty absolutely, as the draft Iraqi electronic crime law did.

5.9.4.1 Mitigation the Punishment

The legislator gave the court the authority to Mitigation the penalties stipulated in this law by half if the perpetrator provided information about any of the crimes stipulated in this law before referring it to the public prosecutor and this would reveal or arrest the crime or its perpetrators[419].

While the draft Iraqi electronic crime law punishes anyone who initiates a electronic crime and does not commit it, with half the maximum penalty prescribed.

---

[416] Article (28) of the Electronic crimes Law No. 17 of 2023 stipulates:

The penalties stipulated in this law will be doubled in the following cases:

A- If the perpetrator committed his crime by taking advantage of his position, work, or powers granted to him.

[417] The fourth branch of Article Five of the Iraqi draft electronic crimes law stipulates: The severest criminalty shall be applied if the perpetrator of the crime is an employee or assigned to a public service.

[418] Article (28) of the Electronic crimes Law No. 17 of 2023 stipulates:

The penalties stipulated in this law will be doubled in the following cases:

C - If any of the crimes stipulated in this law is committed repeatedly

[419] Article (29) of the Jordanian Electronic crimes Law No. 17 of 2023:

5.9.4.2 Exemption from Punishment

The draft Iraqi electronic crime law exempted those accused who cooperate with the authorities and report to them about an electronic crime in violation of the provisions of the law before it is revealed. However, if this reporting of the crime occurred after the relevant authorities revealed it, then in this case the order was given to the competent court to exempt him from punishment. However, in order for this exemption to be achieved, it is required that the accused's report to the authorities result in the arrest of the rest of the accused. [420].

The Jordanian legislator did not refer to anything related to exemption from punishment, and the researcher believes that it would be better if the Jordanian legislator did so to encourage people who intend to commit a crime to refrain from it.

Here, the researcher raises a question in this case, which is what is the situation if some of the accused were arrested as a result of this report, while others escaped, and the hand of justice did not reach them, so is this accused exempted?

5.10 CONCLUSION: -

- That electronic crimes are crimes of a special nature, but for the criminal liability of these crimes to be obtained, the criminal act must be available, and the technical activity is the focus of it Likewise, the criminal intent, which is represented in planning and managing the perpetrator, must be existent, and his intent to bring about his crime in the electronic environment must be available, with his knowledge that the law criminalizes it In addition, there must be a causal relationship linking his technical activity and his intent to cause crime in the electronic environment.

- Criminal intent in the electronic environment is based on three cases:

a) The case of the perpetrator's will to achieve a result of his criminal behavior, such as the perpetrator's illegal entry to the website, knowing that this entry is illegal.

b) In the case of permissibility of intent, and that is if one person sends another virus through computers, the intention is to reduction the speed of the device of the person to whom the virus is sent, and this virus works to destroy the device.

---

[420] Article 20 of the Iraqi draft electronic crimes law stipulates: Exemption from the criminalty prescribed under the provisions of this law shall be granted to any of the suspects, whether the principal perpetrator or an accomplice, who hastens to inform the competent authorities of information about a crime that occurred in violation of the provisions of this law before its disclosure , If such information was notified after its disclosure, the competent court may exempt him from punishment, provided that his disclosure results in the arrest of the rest of the accused.

c) The case of the enormity of the criminal result, when a person hacks another person's device in order to obtain a file that contains personal photos of that person, then he publishes it, and along with the personal photos of that person, his financial data

- **Many theories have been found to determine the criterion for achieving the causal relationship. These theories are:**

  a) Equivalent theory of causes and this theory cannot be applied in cyberspace.

  b) The theory of the direct cause, and an example of it in cyberspace, is the seizure of a person's electronic money. The weakness of the password is not considered the reason for the seizure of electronic money. Rather, the act of theft is considered the direct reason for the seizure.

  c) The theory of the appropriate cause, as if a person sends a virus that is known to disrupt the system of the device without destroying it but, after sending this virus, the device of this person is destroyed. Here, the criminal liability is limited to disturbing the system without destroying it.

- Among the crimes committed on the website is the crime of illegal entry or exceeding the authorized entry without making any order As well as the crime of unlawful entry or exceeding the authorized entry in order to delete, add, modify or hack the data or information of the information system.

- The Jordanian legislator and the Iraqi draft criminalized illegal entry or exceeding the authorized entry and imposed financial fines and custodial criminalties for this crime.

- An aggravating circumstance is the crime of unlawful entry or exceeding authorized entry if it affects national security, foreign relations, public safety or the national economy.

- The Jordanian legislator and the Iraqi draft criminalized illegal entry or exceeding the authorized entry in order to delete, add, hack or modify the data or information of the information system.

- The aggravating circumstance is the illegal entry in order to delete, add, modify or hack data if it is intended to transfer funds or related to electronic payment services or any of the financial services provided by banks and financial companies.

- Criminal responsibility is the criminal accountability of a person for the crime he has committed by applying the rules of criminal law to him.

- Criminal liability in the field of electronic transactions rests with the service provider in two cases:

a) The case of being an accomplice to an electronic crime that is carried out by a person on the Internet.

b) The state of being aware of the electronic content and allowing it to spread.

- The European approach defines a service provider as any natural or legal person who provides Internet service in the information services community.

- The most important commitments of the service provider with regard to the criminalty liability are as follows:

a) The commitment to inform the authorities in the event of publishing information related to a threat to the national or economic security of the state or publishing pornographic material.

b) Commitment of electronic service providers to respect the right to privacy and confidentiality of correspondence.

c) Electronic service providers must monitor information that constitutes a crime that threatens the security and safety of the state.

d) The commitment to block websites, links or informational content at the request of the investigation and trial authorities

- There are three trends in determining the criminal liability of the electronic service provider, as follows:

a) **The first trend:** - They acknowledge that criminal liability does not fall on electronic service providers, as it is impossible for electronic service providers to monitor all information via the web, in addition to their job being a technical one.

b) **The second trend:** - says the determination of the criminal responsibility on the providers of electronic services, considering that failure to determine responsibility leads to the spread of illegal electronic information more.

c) **The third trend:** - He said that the criminal liability is rests on the electronic service provider in three cases: -

The first case:

A case where it is proven that he is a source of illegal information and data.

The second case:

The case of his failure to stop broadcasting illegal content despite his knowledge of that.

The third case:

The case of his refusal to cooperate with the authorities if he was asked to do so.

However, the general texts in the criminal code in both countries and the special texts related to consumer protection laws can be dropped in relation to electronic transactions regarding electronic crimes in order to avoid legislative lack in both countries.

The Jordanian legislator did not address the issue of exemption from punishment in the event that one of the accused reported the crime, and it would have been better for him to do so.

6

Procedural Criminal Protection for Electronic Transactions

6. PROCEDURAL CRIMINAL PROTECTION FOR ELECTRONIC TRANSACTIONS

6.1 INTRODUCTION

Criminal protection does not only pertain to the substantive aspect of electronic transactions, but it also extends to encompass the procedural aspect. However, there are numerous procedural challenges in electronic transactions, particularly concerning electronic processing data and non-material entities. These challenges make detection difficult on one hand, and collecting evidence about them on the other hand. The speed and accuracy of executing these crimes, along with the possibility of erasing their effects and concealing the obtained evidence immediately after committing such crimes, further enhance the complexity of these procedures. [421]

6.2 PROCEDURAL CRIMINAL PROTECTION IN THE INVESTIGATION STAGE

Procedural provisions related to electronic transaction crimes do not significantly differ from procedural provisions regarding other crimes. They go through the same stages, with the investigation stage preceding the trial stage. Public proseccution [422]perform tasks through which they are able to reveal the crime, arrest the perpetrator, and preserve the evidence of the accusation thereafter. This is achieved by referring the matter to the public prosecution for investigation and assessment of evidence. However, the procedures of investigation, which

---

[421] Abdulilah, Ahmed Hilali 2013, p. 146.

[422] The term "investigation" refers to the procedures taken by the judicial control authority to apprehend criminals, gather necessary evidence for initiating legal proceedings against the accused, and impose penalties on those proven guilty (Al-Basyuni, Abdulghani (2003), General Theory of Administrative Law, Manṣhūrat al-Ma'ārif, Alexandria, p. 391). The stage of investigation aims to collect information related to the crime, discover its location, pursue offenders, and identify them. This stage is carried out by judicial control agents under the supervision and oversight of the public prosecution, and it can be either secretive or public (Al-Halabi, Mohammad Ali Al-Salim (2009), Concise Guide to the Principles of Criminal Trials, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, p. 13).

are conducted in an electronic environment and digital space, face several challenges. This distinguishes them from the criminal procedures followed in detecting traditional crimes.[423]

There are numerous procedures in the search and investigation stage carried out by Public proseccution. In the investigation stage, actions are taken before start the criminal lawsuit. The purpose in this stage is to determine the reasons behind the occurrence of the crime under investigation. This is done by collecting evidence related to individuals suspected of involvement. Additionally, various scientific methods and legitimate techniques are employed in this stage to uncover the mystery of the crime and reveal the truth.[424]

In this stage, criminal protection involves safeguarding the rights of the perpetrator or the person under suspicion during the investigation process until their condemned is proven. This is done to maintain the confidentiality of the investigation and the privacy of individuals. It is possible that the individual under investigation is not actually the perpetrator[425]. Without the confidentiality of the investigation, this individual might be wrongly perceived as a criminal by society. This could lead to negative consequences, such as social alienation and an inability to interact with the community in which they live. The society might form a negative opinion about them, leading to material harm resulting from this perception[426]. Considering the future vision of internet crimes, the legislator found it necessary to surround the process of investigating electronic crimes with a degree of privacy to protect the individuals under suspicion. The investigation must also respect the privacy of individuals, and it is not permissible to invade their homes day or night under the pretext of searching for evidence. Instead, such actions must be carried out in accordance with the law. In Jordanian legislation, the Jordanian legislator has outlined the procedures of this stage according to the provisions of the Jordanian Code of Criminal Procedure No. 9 of 1961 and its amendments and the Electronic crimes Law No. 17 of 2023. In Iraqi legislation, the provisions of the Iraqi Code of Criminal Procedure No. 23 of 1971 and its amendments govern these procedures in this stage. The investigation should be limited to the person under suspicion and should not extend to others who are not directly related to the suspect. [427]

[423] Rustom, Hisham Farid 2010, , p. 79.

[424] Musa, Mustafa Mohamed 2015, p. 297.

[425] Abdul-Baqi, Mustafa 2018, p. 293.

[426] Bouamara, Mohamed, Benibala, Sidi Ali 2019, p. 66.

[427] Saghir, Yusuf 2013,p. 72.

6.2.1 Specialized Authorities in Combating Electronic Transactions Crimes

Calls have risen for the establishment of a dedicated judicial authority for the investigation and detection of electronic crimes. This policy finds its justification in the complex nature of these crimes, which require specialized technical expertise for detection.[428]The idea of establishing a specialized unit to deal with electronic transaction issues was introduced during a conference held at the Sorbonne in 2005, titled 'Internet Police.[429]

Many countries have taken steps to establish specialized units to address electronic transaction issues due to the complexity of electronic crimes in general, and electronic transaction crimes in particular.[430] This has led to the development of control mechanisms to keep pace with the continuous developments in electronic crimes. Simultaneously, efforts have been directed towards training and equipping specialized human resources capable of dealing with these types of crimes.[431]

In Jordan, an Electronic Crimes Combat Unit was established under the General Security Directorate in 2008. This unit is specialized in pursuing electronic crimes and consists of experts skilled in tracking electronic crimes. The unit employs advanced tools and collaborates with internet service providers. It is responsible for investigating and conducting research on crimes committed through the internet, including electronic fraud, electronic payment crimes, illegal e-commerce, and unlawful marketing.[432] In Iraq, there is a department known as the Electronic Crime Combat Department under the Iraqi police. [433]

Regarding international entities specialized in combating electronic transaction crimes, the International Criminal Police Organization (INTERPOL) is one of the most prominent units focused on addressing information crimes. It consists of five entities: the General Assembly, the Executive Committee, the General Secretariat, the Advisory Board, and the Situation-Centered Regional Offices. Its headquarters are located in Paris. Its primary functions involve collecting all data and information related to crimes and criminals. Its secondary role is to arrested fugitive criminals and deliver them to their respective countries.[434]

---

[428] Al-Jamal, Hazem Hassan 2015, p. 62.

[429] Haroal, Nabeela Hiba 2007, p. 97.

[430] Haroal, Nabeela Hiba 2007, p. 97.

[431] Al Khreisah, Ahmed Mohammed Abdullah 2023, p. 1805.

[432] Hamaat Al Haq website, Published on 11/11/2021, titled "How to Detect Electronic Crimes in Jordan

[433] https://www.mohamah.net/law/ -

[434] Jamil Abdul Baqi 2002, p. 76.

Several conditions should be met by specialized units responsible for investigating and detecting electronic transaction crimes, including but not limited to:

- Having an understanding of how judicial investigation works, being prepared to deal continuously with this type of crime, through qualification and training in the field of technology, computers, and virtual world interaction.

- Defining the scope of the tasks assigned to the Judicial Police, due to their role in addressing acts occurring through the Internet, such as concealing identities through communications and the potential creation of fake identities and others.

- The Judicial Police are commitment by all legal duties according to the conditions and procedures stipulated by law. This includes documenting the procedures undertaken during the investigation of the crime and commitment to obtaining authorization from the competent authorities for actions that are restricted by individuals' freedom.[435]

6.2.2 Jurisdiction of Judicial Police in the Investigation Stage

The scope of jurisdiction of the judicial police during the investigation and inquiry stage is limited to two main aspects: receiving reports and complaints and conducting preview.

6.2.2.1 Receiving Reports and Complaints

This refers to the information submitted to the judicial police officer, with the purpose of reporting a crime that has occurred or is about to occur, relating to electronic transactions. Typically, this report is submitted in writing or orally, and it can be provided by the reporting party themselves or by an authorized representative using various means of communication.[436]

Any person has the right to report to the competent authorities about any crime that has occurred or is known to be about to occur. Regarding reporting electronic crimes in Jordan, individuals can head to the nearest police station, which will refer the complainant to the Electronic Crimes Unit through an official letter. Alternatively, the complainant can directly head to to the Electronic Crimes Unit through an official letter or contact the local prosecutor's office near their residence, requesting to initiate legal proceedings and transfer the case to the Electronic Crimes Unit within the Criminal Investigation Department.

[435] Al-Hassan, Mohammed Tariq Abdul Rauf 2011, p. 231.

[436] Al-Akayleh, Abdullah Majid 2010, p. 110.

In my opinion i recommends the establishment of an electronic platform in Jordan for reporting electronic crimes, as many other countries have done.

In Iraq, individuals can access the Iraqi Electronic Crime Department's website and enter the complainant's phone number, the content of the complaint, and the complainant's name. The complaint is received, and all important events and developments are immediately recorded. The specialized team later contacts the complainant to provide immediate and preliminary advice that should be followed. Verification of the crime is conducted, and the perpetrator is arrested in flagrante delicto and referred to the public prosecutor's office[437].

The significance of reporting electronic crimes lies in informing the community about the occurrence of such crimes that need to be addressed. Therefore, precautions must be taken to protect and preserve software.[438]

As for the affected individual, the one who suffered harm as a result of an electronic transaction, they have the right to file a complaint. A complaint is an action taken by the victim, their legal guardian, or their representative, to the competent authority, seeking the initiation of a criminal case in those crimes where the initiation of the case relies on this procedure.[439]

It is noticeable that there is a refrain to report crimes related to electronic transactions, which constitutes a significant hindrance to combating electronic crimes in the context of electronic transactions. For example, commercial companies fear for their reputation in the market and are reluctant to shake their customers' trust by disclosing electronic attacks they may be facing. Consequently, they avoid discussing the electronic assaults they are subjected to. Therefore, it has been proposed to include provisions in the laws that oblige employees of these institutions to report crimes under the penalty of criminal liability.[440]

Individuals may also refrain from reporting for various reasons, including complete unawareness of being targeted by an attack. They might not notice the situation until a certain period of time has passed, leading them to believe that reporting is futile. Additionally, some individuals fear damage to their reputation, skills, and apprehension of being perceived as naive and lacking awareness.[441]

---

[437] https://www.mohamah.net/law/

[438] Al-Halabi, Khaled Al-Sayyad 2011 , p. 192

[439] Al-Husseini, Ammar Abbas 2015, p. 134

[440] Beltagy, Samah Ahmed 2010, , Ph.D. thesis, , p. 20-21.

[441] Hegazy, Abdel Fattah Bayoumi 2006, p. 116.

6.2.2.2 Conducting Preview

The process of preview is considered one of the key challenges facing the investigation of crimes committed in the electronic scop. Preview is defined as direct and material proof of the state of a specific thing or person, achieved through direct visual observation by the individual conducting the procedure.[442]

Preview is a purposeful procedure aimed at uncovering the CRIMINAL ACT related to the ongoing investigation. Its significance lies in revealing the material evidence in traditional crimes. However, its role in the scop of investigating electronic crimes proves valuable in establishing their occurrence, attributing them to their perpetrators, and understanding their impact. [443]

The importance of preview is underscored by the following considerations:

- Electronic crimes rarely lack material effects or resulting evidence that takes the form of non-visible data, making their difficult to preview challenging.
- The potential for destruction, alteration, or tampering with material evidence weakens the reliability of preview.
- Perpetrators can remotely manipulate or erase data, necessitating legislation to impose penalties on those altering or modifying information stored in computer memory.[444]

The mechanism for conducting preview in the investigation of electronic crimes involves navigating the virtual world. This includes examining computers, mobile phones, or the premises of Internet service providers. Various forms of preview include capturing images of the computer using a traditional camera or utilizing specialized computer software to capture the on-screen display. Alternatively, the examination can involve saving a webpage using the available "save" feature in the operating system.[445]

---

[442] Sorour, Ahmed Fathi 1985, p. 288.

[443] Rostom, Hisham Mohamed Fareed 1992, p. 57.

[444] Harwal, Nabeela Hiba 2007, p. 217.

[445] Al-Dhahabi, Khawduja 2019, Doctoral Thesis, p. 215

6.3 ESPECIALLY OF INSPECTION IN ELECTRONIC TRANSACTIONS CRIMES AND SPECIAL METHODS FOR COMBATING THEM

The importance of inspection has increased in modern electronic systems, as it is considered one of the most powerful criminal methods used to combat the escalation and modern developments of crime.[446]

Inspection is a procedure among investigative methods that aims to search for material evidence of a crime or crime that occurred in a specific location with privacy, in accordance with established legal guarantees and restrictions[447].

It is also a procedure aimed at searching for material evidence of a crime or crime that occurred in a location with the privacy of a residence or person, with the purpose of proving its commission or attributing it to the accused in accordance with specified legal procedures[448].

The role of inspection in electronic crimes is limited to the scope of the information crimes unit within the country, whose task is to investigate electronic crimes that occur within the country's borders via the Internet. The scope of inspection is not limited but rather broad, in order to identify all individuals involved in the crime, even if their involvement is minor[449]. Examples of inspection in electronic crimes include monitoring all devices near the victim's device to identify all devices that played an auxiliary or primary role in the commission of the crime. Adding security features to the Internet network that enhance security within the digital space can help reduce electronic transaction crimes [450]

Inspection takes various forms, including:[451]

- Real inspection, where the legislator allows it due to a committed crime, prioritizing the public interest over individuals' private interests.
- Administrative inspection, which is a precautionary procedure aimed at ensuring the smooth functioning of work and achieving administrative purposes.

---

446 Ben Younes, Omar Mohamed Abu Bakr 2004, p. 825.

447 Hussein, Sami Hassani 1972, p. 37.

448 Sorour, Ahmed Sabahi 1993, p. 544.

449 Qazoura, Naela Adel Mohammed Fareed 2005, p. 98.

450 Al-Halabi, Khaled Abbad 2011, p. 86

451 Al-Habbara, Abdel Fattah Abdel Latif 2015, p. 376.

- Preventive inspection, procedure targeting the Combat of crime in its various forms and the arrest of individuals attempting to commit it while they are in the preparation and planning stage.

- Executive inspection, procedure where the legislator authorizes it to confirm the public interest of obtaining material evidence that aids in uncovering the truth and aims to arrest the perpetrator of the crime.

6.3.1 Characteristics of Inspection in Electronic Transactions Crimes

In general, inspection has several characteristics, including[452]:

- It is a judicial investigation procedure and is among the most important powers exercised by the investigating authority against individuals and their residences.

- It is a process of evidence collection in criminal investigations, aiming to search for and secure the necessary evidence for the investigation.

- It is related to privacy and violates the right to privacy, as it targets accessing a location that has sanctity and enjoys confidentiality.

- It represents a form of restricting human freedoms, which most legislations sought to preserve, subject to guarantees and restrictions provided for in their implementation[453].

Inspection in electronic transactions crimes requires specific skills and techniques, differing from general inspection cases. The targeted data in electronic transactions is often swiftly and easily disposed of, making the inspection process challenging and difficult[454].

6.3.2 Feasibility of Inspection for Information System Components

Computers consist of physical components, such as the external units of the device, and intangible components, such as data and information stored inside it.When electronic crimes involve material components, inspection does not pose difficulty. Traditional rules for inspection apply to such components, contingent on the nature of the location. Inspection is

[452] Ash-Shawi, Tawfiq Muhammad, (2006), , p.27.

[453] As-Saffir, Jamil Abdul Baqi 2002, p.113.

[454] Al-Halabi, Khalid Ayyad, 2011, p.150.

easier if the location is public, compared to a private location like the suspect's residence or its annexes. Private locations are subject to specific legal cases and guarantees.[455]

In our field of study, for inspection to occur, there must be a committed electronic transaction crime. A legal provision criminalizing the act, considering the nature of the crime location (public or private), is required for an inspection warrant. The specific details hold special importance in the scope of inspection[456].

Although some legislations allow judicial officers to enter public location without prior permission from the public prosecutor, opening closed items in a public location requires a judicial warrant. Public scenes encompass government buildings, public parks, roads, buses, cafes, stores, hospitals, clinics, offices, and hotels. While inspections in public location are more accessible, they are subject to legal guarantees and restrictions[457].

In the case where the crime location is in a private location such as the suspect's residence or its annexes, inspection is only allowed under conditions that permit inspecting the residence. The same legal guarantees apply as in different legislations[458].

Regarding the inspection of the Internet, those conducting inspections on this network face no obstacles. The Internet is a global network accessible to the public, allowing access without a judicial warrant[459].

Inspecting computer networks faces difficulties in obtaining data that links these networks to locations beyond the jurisdiction or even in another country. This increases complexity, as information networks span the globe. In cases where the suspect's computer is connected to a system in another location within the state, the Budapest Convention of 2001 permits extending inspection to devices connected to the suspect's device if information accessed through the inspected device is stored therein[460].

If the suspect's computer is connected to a system or terminal located outside the country, inspection must occur within the framework of bilateral or international cooperation agreements, allowing such extension or obtaining prior permission from the other country[461].

The Arab Convention also allowed for remote inspection through the second paragraph of Article 26 if there is a belief that the required information is stored in another information

---

455 Al-Halabi, Investigation and Inquiry Procedures, p.159.

456 Ahmad, Hileli Abdullah, , 2008, p.73.

457 Awad, Mohamed Awad 2006, p.90.

458 Bouker, Rachida 2017, p.276.

459 Abdelghani, Shimaa 2007, p.351.

460 See Article 19 of the Budapest Convention of 2001.

461 Ibrahim, Khaled Mamdouh 2009, p.205.

technology and this information is legally accessible or available in the first technology. In the event that the accused system is connected to a system in another country, it is subject to bilateral agreements between the countries.

Recommendation No. 13 of 1995 issued by the European Council extended the computer inspection process to the connected network even if that network is located outside the state's territory. Some legislative systems, such as the U.S. legislation, have gone so far as to allow inspection to extend to other devices even if they are in other countries.[462]

When we look at the Spanish legislator, we find that it includes the issue of inspecting information systems in an article588 in the Code of Criminal Procedure. Looking at this article in general, we find that the Spanish legislator was keen to have a judicial warrant to search information systems, and even that there must be a judicial warrant to obtain the information contained in devices. The computer was confiscated, and the Spanish legislator did well. These things are not emphasized in our legislation, and this preserves the rights and privacy of individuals.

As for inspecting electronic information systems located outside Spain, it was also referred to in Article588 Article 588 e. ii. Access to the information on electronic devices confiscated outside the domicile of the party under investigation. The requirement provided for in paragraph 1 of the previous article will also be applicable to cases where computers, communications instruments or mass data storage devices, or access to online data warehouses, are seized independently of a house search. In these cases, the agents will make the confiscation of such effects known to the judge. If the judge considers access to the information housed in their content is essential, they will grant the relevant authorization

We also find that the Spanish legislator specified some crimes for which information systems are searched remotely in the article588[463] The Spanish legislator was excellent in his

---

[462] Ahmed, Ayman Ramadan 2010, PhD thesis, p.299.

[463] Article 588 f. i. Premises. 1. The competent judge may authorise the use of identification data and codes, and software to be installed, which allow remote, online examination, without the knowledge of their owner or content user, of a computer, electronic device, computer system, mass computer data storage device or data base, provided that one of the following crimes is being investigated: a) Crimes committed by criminal organisations. b) Crimes of terrorism. c) Crimes committed against minors or persons who are legally incapacitated. d) Crimes against the Constitution, treason and those related to national defence. e) Crimes committed using computer devices or any other information or telecommunications or communications service technology. Criminal Procedure Act ▒ 165 . 2. The judicial decision authorising the search must specify: a) The computers, electronic devices, information systems, or part of them, computer media for data storage or databases, data or other digital content subject to the measure. b) The scope of the measure, the manner in which access and seizure of the computer data or files relevant to the case will be made and the software to be used to control the information. c) The agents authorised to carry out the measure. d) The authorisation, as appropriate, to make and keep copies of the computer data. e) The measures needed to preserve the integrity of the data stored, and to deny access to or suppress such data from the computer system that was accessed. 3. Where the agents carrying out the remote search have reasons to believe that the data sought are stored on a different computer system, or on a part of it, they will make this fact known to the judge, who may authorise an extension to the terms of the search.

treatment of these matters, but in my opinion, if he used the phrase outside the borders of Spain, it would be better than using the term “remotely” or “outside the homeland of the person under investigation,” because these terms can carry more than one meaning, that is, they are broad or broad terms.

Jurisprudence have not reached a consensus on whether the general rules for inspection apply to the moral components of computers, or if the matter requires specific legislation to regulate the inspection process of the moral components of computers.

6.3.2.1The Supporting Direction for the Inspection Process:

This direction has gone on to state that legal texts related to inspection in some legislations allow the inspection of non-material components of the computer. This is due to the general formulation of these texts falling under the sezure 'regulating anything,' encompassing both material and non-material components of the computer. This means that it includes stored or electronically processed data[464]. Moreover, this direction adds another justification that even though information and programs might lack tangible material existence, they still occupy a material space in the computer's memory or storage media, which can be measured by a specific unit, the byte. Consequently, information can fall within the scope of material entities.[465]

However, a critique of this direction is that the legal texts that specified the controls governing the inspection process were enacted before the law recognized non-material entities. The nature of electronic data and information requires specific rules to govern them, rather than adapting traditional rules and expanding their scope. The specific texts pertaining to inspection in their traditional sense cannot be directly applied to computer systems since measuring them against non-material entities contradicts procedural legitimacy.[466]

6.3.2.2 The Second Opposing Direction for the Inspection Process:

They argue against the possibility of applying general inspection provisions along with what might be required to uncover the truth in electronic crimes: searching and probing evidence in computer programs and data. They state that when legislations defined the purpose of inspection as searching for seizure things, it was limited in its concept to tangible material possessions. Hence, it does not cover moral entities, and there must be specific

[464] Bioumi, Abdel Fattah 2009, p. 652.

[465] Tawalbeh, Criminal Inspection, p. 30.

[466] Jafali, Hussein 2020, Ph.D. Thesis, p. 293.

provisions regulating the inspection process on information systems, as general texts do not apply to these moral entities.[467]

Therefore, there's a need to confront the technomoral evolution of computers and communication by enacting specific legal texts that target the inspection and control of processed data through computers and information systems. The purpose of inspection in traditional crimes is to control material evidence that aids in revealing the truth.[468] Thus, the Budapest Convention urges member states to enact special laws that enable competent authorities to inspect, enter computer systems, or parts thereof, or stored data, or media storing computer information.[469]

Regarding international law on this matter, the first paragraph of Article 19 of the Budapest Convention emphasizes the direction that supports excluding non-material computer data from general rules. It states that each party state must adopt additional procedures it deems necessary to empower its competent authorities with the authority to inspect or access stored information systems.

The Jordanian legislator and the draft Iraqi law, if implemented, as it permitted examination of the moral components of the computer, as the Jordanian legislator permitted entry into any place where evidence indicates its use in committing the crimes stipulated in this law. It also authorized the examination of tools, programs, and devices that evidence indicates were used to commit crimes[470]

6.3.3 General Inspection Provisions

6.3.3.1 Inspection Controls in the Electronic Environment:

Inspection is a procedure initiated by the public prosecutor, the investigating judge, or authorized officers of the judicial police based on the existence of useful evidence, and that the person to be inspected contributed to committing the crime as a primary perpetrator or accomplice.[471]

[467] Erhuma, Musa Masoud 2009, p. 8.

[468] Tawalbeh, Ali Hassan 2004, p. 31

[469] Article 19/1/2001 of the Budapest Convention.

[470] Article (32/A) of the Jordanian Electronic crimes Law No. 17 of 2023

[471] Tawalbeh, Ali Hassan Mohammed, 2004, p. 212.

There must be sufficient evidence of the existence of items, equipment or information that could lead to the discovery of the truth the purpose of inspection is to seizing these components found in the possession or residence of the individual.[472]

Most procedural legislations include specific controls that must be commitment to during procedures involving personal freedom, such as inspection. The purpose of this is to achieve a balance between society's interest in punishing criminals and individuals' rights and freedoms.[473]

6.3.3.1.1 Objective Controls for Inspecting Information Systems:

It does not make sense to inspect an information system or any type of inspection without a set of factors that necessitate conducting such an inspection, such as the occurrence of a crime punishable by law and the presence of evidence proving the place to be searched that contains things that help discover the perpetrator of the crime. This is what we might call controls Objectivity. Which will be studied as follows:

- The occurrence of a crime related to electronic transactions. For the inspection to be valid, there must be the occurrence of a crime related to electronic transactions, and this crime must be classified as a felony or misdemeanor. Violations do not warrant inspection due to their minor significance.[474]

- Accusing a specific person or individuals of committing a crime related to electronic transactions. In this case, there must be sufficient evidence in favor of the person being inspected to believe that they contributed to the commission of a crime related to electronic transactions, either as a primary perpetrator or accomplice. This implies that sufficient evidence, consisting of various indicators and specific signs, which are part of the mental and moral content of the incident, as well as the experience of the inspecting authority, must support attributing this crime to that person as a perpetrator and accomplice.[475]

- The presence of indicators or signs of the existence of items, devices, or information equipment that can help reveal the truth. Inspection is only carried out if the investigator has sufficient reasons to believe that there are tools used in a crime related to electronic

[472] Al-Halabi, Investigation and Interrogation Procedures, p. 154.

[473] Hasani, Mahmoud Naguib, 2021, p. 594.

[474] Bouker, Rachida, Criminal Protection, p. 28.

[475] Ahmed, Helali Abdelilah, Computer System Inspection, p. 115.

transactions, or items derived from it, or any electronic documents that may be useful in clarifying the truth to the accused or others.[476]

Article 87/3 of the Jordanian Code of Criminal Procedure states: "In all cases, the inspection order must be justified and may not be executed after seven days from the date of its issuance, under penalty of nullity.

The Jordanian legislator has permitted entry into any place where evidence indicates that any crimes stipulated in the Electronic crime Law have been committed. It has also authorized the inspection of programs and equipment that evidence indicates that they have been used in committing crimes stipulated in the Electronic crime Law[477].

.63.3.1.2. Formal Controls for the Inspection of Information Systems

When the objective controls explained above are available, there must be controls during the inspection process, which can be called formal controls.

.63.3.1.2.1. Rule of Presence

When conducting inspections related to residences and their attachments, it is necessary for the suspected person to be present during the inspection by the judicial police. In case the suspected person is unable to attend, the judicial police officer should appoint a representative. If the suspected person refuses to attend the inspection or flees, the inspection is conducted in the presence of two witnesses who are not subordinate to the authority of the conducting judicial police officer.[478]

The Jordanian legislator indicated that Inspection are conducted in the presence of the accused, even if he is in prison. If he does not attend, whether due to his unwillingness to attend or his inability, the Inspection are conducted in the presence of his representative, or the public prosecutor brings two witnesses[479].

The Iraqi legislator was not far from the Jordanian legislator

The inspection shall take place in the presence of the accused and, if present, the owner of the house or premises, with two witnesses accompanying the inspector or his deputy. The person conducting the inspection must write a report that includes the procedures he followed, the time and location of the inspection, the items seized and their descriptions, the names of

---

476 Al-Ghafrri, Hussein bin Saad, , PhD Thesis, 2007, p. 381.

477 Article32 of the Jordanian Electronic crimes Law

478 Khalifa, Ilham, 2016, p. 272.

479 Article36 of the Jordanian Code of Criminal Procedure

those present, any remarks made by the accused or others involved in the case, and the names of the witnesses. The accused, the owner of the premises, and the person being inspected, as well as any present witnesses, must all sign the report. The failure of any of them to sign will be noted in the report. On demand, a copy of[480]

.63.3.1.2.2. Inspection Scene

The term refers to the storage where a person keeps items containing his secrets. In crimes related to electronic transactions, the scene of inspection is the computer system and the mobile phone with all its material and virtual components, as well as the connected communication networks.[481]

Inspection in electronic crimes differs from traditional crimes in that it includes not only material component like computers but also virtual component like information systems, software, and electronic data that lack material appearance.[482]

The focus of inspection in electronic crimes is on the information system to collect evidence for electronic transaction crimes. The scene of inspection must fulfill two conditions: it should be specific and permissible for inspection. However, determining the scene of inspection is challenging due to the complex interconnection of files. Inspectors often have to conduct a general search to find evidence, risking privacy violations by accessing files not covered by the inspection warrant. Regarding the second condition, legislation typically exempts certain scenes from inspection due to their association with public or individual interests that override the investigative purpose, like diplomatic missions' headquarters.[483]

The Jordanian legislator has stated in the electronic crime law that devices, tools, programs, operating systems, the information network, and the means that evidence indicates are used to commit any of these crimes are the subject of inspection in electronic crime[484].

While the draft of the Iraqi legislator did not address this matter.

---

[480] Article 82 of the Iraqi Code of Criminal Procedure

[481] Jafali, Hussein 2020, p. 300.

[482] Al-Fil, Ali Adnan 2012, p. 39.

[483] Jalal, Sami 2011, p. 130.

[484] Article 32/A/2 of the Jordanian Electronic crimes Law No. 17 of 2023

.633.1.2.3.Authority Responsible for Inspecting Information Systems

Since inspection impacts individual rights and freedoms, procedural laws grant the authority to conduct inspections to investigating authorities. To expedite investigations, the judicial police are authorized to perform inspections, provided that written authorization from the competent judicial authority is obtained.[485]

Hence, conducting inspections in the electronic environment necessitates a judicial warrant explicitly granting the authority to inspect computer systems.[486]

The public prosecutor has the authority to inspect under Jordanian law. "The public prosecutor shall bring his clerk and record all the items he deems necessary to reveal the truth, draft a report on them, and be responsible for their preservation".[487]."

In the new Jordanian Electronic crimes law, the Jordanian legislator did not neglect to mention the authority responsible for inspection when what is to be searched includes information and electronic websites, as he touched on this in the article32 of this law as follows:

Taking into account the terms and conditions stipulated in the applicable legislation and the personal rights of the defendant, to the judicial police officer, after obtaining permission from the competent public prosecutor or from the competent court.Entering any place that evidence indicates that it will be used to commit any of the crimes stipulated in this law and searching it.Inspecting and examining devices, tools, programs, operating systems, the information network, and the means that evidence indicates that they were used to commit any of these crimes[488].

As for the Iraqi legislator, despite not ratifying the Iraqi electronic crimes law, he relies on traditional texts. The investigating magistrate may travel to any location within his jurisdiction to conduct any necessary investigations. He may also be required to transfer to locations outside of his jurisdiction if the investigation requires it. In such cases, he has the authority to arrest, detain, inspect, question witnesses, interrogate suspects and related parties, and release individuals on bail or without bail, provided that he informs the investigating magistrate of the actions taken[489].

In Spanish legislation, the competent authority to inspect information systems is a judicial authority represented by the investigating judge. If the Public Prosecution or the

---

[485] Mustafa, Aisha bin Qada 2010, , p. 106.

[486] Jafali, Hussein 2020, , p. 301.

[487] Article 87 of the Jordanian Code of Criminal Procedure

[488] Article (32) of the Jordanian Electronic crimes Law No. 17 of 2023

[489] Article (56) of the Iraqi Code of Criminal Procedure

judicial police want to directly inspect information systems, there must be a judicial authorization for the inspection process. The inspection process may take place by direct order from the investigating judge, and it may It is carried out at the request of the Public Prosecution or the Judicial Police, and when a request from the Public Prosecution or the Judicial Police is submitted to the competent judge requesting an inspection, it must be accompanied by several data stipulated in the Spanish Code of Procedure[490].

In my opinion i believes that the Iraqi legislator is trying to apply the traditional text to electronic transactions and that the legislative strength of the text is not at the required level. The difference is clear between the article32 in the electronic crimes law and that we continue to use the traditional text as is the case in Iraqi legislation.

6.3.3.1.2.4 The Timelines for Conducting an Inspection

Failure to respect this guarantee by conducting an inspection outside the legally specified timeframe can lead to violations of individual freedom and the sanctity of homes.[491] Both the Jordanian and Iraqi legislations have remained silent on the specific timing of inspections, making inspections available at any time.

In my opinion i believes that leaving the inspection date open and not stipulating a specific date for the start and end of the inspection is unjustified and opens the way for invading individuals' privacy and violating their rights under the pretext of inspection and searching for evidence.

6.3.3.1.2.5 Inspection Report

Since inspection is considered part of the investigative process, it is necessary to prepare a report documenting the procedures conducted, the evidence obtained, and the general conditions required for the validity of such reports. Among the essential requirements for a valid inspection report are the inclusion of key information such as the name of the report's author and their signature, the location and time of report preparation, and details related to the subject of the inspection report[492].

We will discuss how the Jordanian and Iraqi legislation dealt with this part, and we will see how the Jordanian legislator dealt with this topic in detail in the electronic crimes law, and Iraq is still suffering from the lack of ratification of this law.

---

[490] Article 588 A. secondly. From the Spanish Code of Criminal Procedure

[491] Khalifa, 2016. p. 277.

[492] Husseini, Sami 1972. p. 377.

The public prosecutor shall bring his clerk and record all items considered necessary to reveal the truth, as well as draft a report on them and be responsible for their preservation Inspection shall only be allowed for the items for which the inspection is carried out. If during the inspection something appears that constitutes in itself a crime or aids in the discovery of another crime, it should also be seized.[493].

In addition to the Jordanian Electronic crime Law, the legislator did well when he indicated how to conduct the report the employee who carried out the inspection or examination must prepare a report thereof and submit it to the public prosecutor or the competent court[494].

The inspection must be conducted in the presence of the accused and, if present, the owner of the house or premises, as well as two witnesses. The person conducting the inspection is required to write a report detailing the procedures he followed, the time and location of the inspection, the items seized and their descriptions, the names of those present, any remarks made by the accused or others involved in the case, and the names of the witnesses. The report must be signed by the accused, the owner of the premises, the person being inspected, and any present witnesses. Failure to sign by any of them will be noted in the report. On request, a copy of[495]

6.3.3.1.3 The Consequences of Correct Inspection of Information Systems

Obtaining material evidence that leads to the discovery of the truth is the ultimate purpose of inspection, as it is the direct result of this procedure. Therefore, it is an investigative procedure subject to the same rules that apply to the inspection itself, and its invalidation results in the invalidation of the seizure[496].

The truth is that the seizure is a direct result of the inspection, and in this regard we reach the following conclusions from both Jordanian and Iraqi legislation:

- Seizures are not permitted unless they are described as evidence related to the crimes under investigation. The material evidence discovered during the inspection is considered material evidence in the seizure, and inspection is only permitted for the items for which the inspection is performed. If something appears during the

[493] Article 87 of the Jordanian Code of Criminal Procedure

[494] Article32/b of the Electronic crimes Law

[495] Article 82 of the Iraqi Code of Criminal Procedure

[496] Hussaini, 1972.. p. 302.

inspection that constitutes a crime in and of itself or aids in the discovery of another crime, it should also be seized[497].

- • Iraqi legislation is completely similar to Jordanian legislation and is not far from it, as it does not allow inspection except for the purpose of determining the locations of the items being inspected. If something is discovered during the search that is a crime in itself or helps in the discovery of another crime, it can also be confiscated[498].

- Seizure is not limited to items that could lead to the defendant's conviction but must focus on items that help uncover the truth, even if they lead to the defendant's exonerate This applies to both Jordanian and Iraqi legislation [499].

- If the accused is found with documents or items that support the accusation, establish exonerate, or are illegal, the public prosecutor must seize them and file a report[500].

6.3.4 Special Methods for Combating Electronic Crimes

6.3.4.1 Intercepting Correspondence and Recording Voices and Capturing Images

Intercepting correspondence involves the use of techniques that infringe upon the personal lives of targeted individuals. This procedure is essential in combating electronic transaction crimes. Intercepting electronic correspondence includes monitoring email communication. There are specialized programs designed for this purpose, such as the (Carnivore Decisys) program, which is used for email interception. Another program is BronzeViber, which scans and monitors all images attached to email messages. As for regular correspondence, it refers to messages sent from one person to another, containing private information. An example of this is a message from a suspect to their lawyer.[501]

---

[497] Article87 of the jordanian Code of Criminal Procedure

[498] Article78 of the Iraqi Code of Criminal Procedure

[499] Hussaini, Sami, 1972.. p. 304.

[500] Article 34/1 of the Jordanian Code of Criminal Procedure

[501] Al-Daoudi, Marhab 2016, Ph.D. Thesis, p. 203.

Recording voices and capturing images are highly effective methods for proving crimes. Voice recording refers to recording oral conversations that individuals hold privately or in public place.[502]

Regarding image capturing, due to the efficiency of cameras in documenting crimes, various legislations employ this method for combating crime.[503]

We will study what the Jordanian and Iraqi legislators stipulated as follows:

The Jordanian Constitution, which is the highest law in Jordanian legislation, was explicit in stipulating the necessity of a judicial order to intercept correspondence, as stated in Article18 All postal, telegraphic, telephonic, and other forms of communication shall be kept confidential and shall not be subject to inspection, eavesdropping, detention, or seizure unless authorized by judicial order[504]

In addition to the Jordanian Code of Criminal Procedure, which was more detailed than what was stated in the constitution .The public prosecutor has the authority to seize all postal letters, messages, newspapers, publications, and parcels, as well as all telegrams. When necessary to reveal the truth, the public prosecutor may also monitor telephone conversations[505]

Iraqi legislation is not far from Jordanian legislation, as it is quite similar to it in this regard

Communication freedom, including postal, telegraphic, telephonic, and electronic correspondence, is guaranteed. It may not be monitored, wiretapped, or disclosed unless there is a legal and security requirement as well as a judicial decision[506].

In my opinion i believes that both legislators did well when they stipulated the presence of a judicial order in all procedures in order to protect individuals and ensure the greatest amount of privacy for them and not to be encroached upon by the security services, but we hope that this will be implemented on the ground.

---

[502] Khalifa, Ilham 2016, p. 311.

[503] Amara, Fawzi 2010, Ph.D. Thesis, p. 197.

[504] Article 18 of the Jordanian Constitution

[505] Article 88 of the Jordanian Code of Criminal Procedure

[506] Article 40 of the Iraqi Constitution

6.4 PROCEDURAL CRIMINAL PROTECTION IN THE TRIAL STAGE

Procedural protection in the trial stage for electronic crimes involves narrowing the scope of attendance in the trial sessions resulting from an electronic crime. The sessions are not open, providing a form of protection for the accused person. The presence of the victim's relatives might disrupt the judicial body when the accused person gives their testimony defending themselves against the lawsuit brought against them[507].

6.4.1 Competent Criminal Court

It is important to determine the competent court to adjudicate the dispute. This determination leads to identifying the applicable law in cases of conflicting laws. Consequently, the competent court is the one that determin the applicable law. Therefore, determining the court competent to hear the case holds clear importance. This significance goes beyond the procedural aspect and extends to substantive rules that the judge will apply to the subject of the lawsuit. It is also in the interest of the plaintiff to file their case before an international court where they know the language and can follow the proceedings[508].

If an international element is present in a case, the rule suggests that multiple states might have jurisdiction over the case. In line with this, the European Court of Justice ruled in a case where Dutch farmers were harmed in their farms due to water pollution caused by a mining project in France. The principle of dual jurisdiction was applied, with the Dutch court having jurisdiction over the harm occurring in the Netherlands, while the French court having jurisdiction over the harmful act in France[509].

The application of criminal law rules in terms of jurisdiction is governed by the principle of territoriality. This means that crimes committed within a certain state's territory are subject to its effective criminal law, making its courts the competent ones to handle cases arising from them.

Regarding crimes related to electronic transactions, and with respect to the competent criminal court, this issue raises complexities due to the international nature of electronic transaction contracts. These contracts are often characterized by their international nature, as they are concluded through various digital means, particularly the global information network, involving offers for sale and purchase by individuals located in one state or multiple states[510].

---

[507] Al-Halabi, Khaled Abbad 2011, p. 102.

[508] Ibrahim, Khaled Mamdouh 2009, p. 413.

[509] Shaimaa, Abdelghani, Criminal Protection of Electronic Transactions, p. 370.

[510] Matar, Essam Abdel Fattah 2015, p. 342.

6.4.1.1 Jurisprudence's Stance on Jurisdictional Conflict

Jurisdiction is determined by the place of the crime's occurrence, the defendant's residence, or the arrest. It fundamentally does not subject to any foreign law. Conversely, the application of a state's criminal law does not extend beyond the state itself. Concerning electronic crimes, jurisprudence has witnessed a dispute over jurisdictional criminal conflict, which can be categorized into three stances: the criminal activity approach, the place where the result is completed approach, and the mixed approach.

6.4.1.1.1. Approach of Criminal Activity

It is the trend that goes to determine the competent authority to look into the criminal behavior or activity, and according to this trend, Jurisdiction is assigned to the court in whose jurisdiction the criminal activity occurs based on the principle of territoriality. This trend has been argued by saying that in the location where the behavior is committed, the perpetrators can be very easily prosecuted, and that the investigation procedures necessary to reveal The crime and determining its details and what this may require in terms of inspecting the scene of the crime can only be done through the judicial authorities within whose jurisdiction the location where the behavior was committed falls, and therefore priority in jurisdiction shall be given to the court within whose jurisdiction the criminal electronic act occurred. [511], Not the location of the crime or its effects, given that taking the effects of the act as a basis for determining the location of the crime is beset by some difficulties that can be summarized as a flexible location and a loose standard.in addition to the fact that the criterion for the occurrence of the activity called for facilitating the process of proof and collecting evidence of the crime, and that the court that has jurisdiction The case shall be heard close to the crime location, and the ruling issued in the incident will be more effective and facilitate the prosecution of the perpetrators. [512]

However, there are several criticisms of this trend, the most important of which is that some actions may not be criminalized by the state in which the criminal activity occurred, which may constitute a means that helps the perpetrators evade punishment.[513]

6.4.1.1.2 The place where the Result is Completed

It goes in determining the competent authority to look into the place where the result is completed, as some jurists have said that jurisdiction to look into electronic crimes rests with the courts in whose jurisdiction the criminal result was investigated or where it was supposed to be achieved, or from the court in which the criminal conduct occurred on

[511] Afifi, Moataz Sayed 2013, , p. 45.

[512] Musa Masoud Arhuma, p. 16.

[513] Saleh Shafik, Previous Reference, p. 263.

the territory of the country to which it belongs. This trend was argued by saying that the statute of limitations for a crime is calculated from the time the criminal result was achieved, and the enorm of the damage is taken into account as a basis for estimating compensation. This trend has been criticized because it does not take into account the interest of the accused by transferring him to distant location for trial, which increases and prolongs the duration of the dispute.[514]

6.4.1.1.3 Mixed Approach

The mixed approach is a trend that equals jurisdiction between courts located within their territory, where the criminal activity occurs, and the court that investigates the criminal result within its territory. The majority of jurists have inclined towards adopting this view, and this approach has advantages that can be outlined as follows:

- Maintaining the unity of the crime and not separating the act from its consequences.
- The court within whose jurisdiction the criminal result is realized is more capable of evaluating the results and confirming the severity of the damages.
- The court where the incident occurred is less concerned with criminal results that occur in foreign states. Adequate effort might not be exerted to arrest the criminals due to a lack of awareness of the impact of the resulting consequences.
- The judiciary in the state where the criminal activity occurred might have less awareness and thus less concern about the potential results in the territory of another state.[515]

- Where the crime occurred, evidence can be obtained more than where the result was achieved

6.4.1.2 The Legislative Stance on Jurisdictional Conflict

6.4.1.2.1 The Jordanian Legislator's Stance on Jurisdictional Conflict

The provisions of this law apply to anyone who commits one of the crimes listed below within the kingdom.If any of the elements constituting the crime, or any act of

[514] Moataz Afifi, Previous Reference, p. 46.

[515] Moataz Afifi, p. 46.

indivisible, primary, or secondary participation, occurred on the territory of this kingdom, the crime is considered committed within the kingdom[516].

Public rights lawsuit permissible brought in the Jordanian judiciary against the defendant if the crime was committed using electronic means outside the kingdom and the consequences resulted, wholly or partially, in the kingdom, or against any of its citizens[517].

Thus, the Jordanian Court of Cassation ruled in its penal capacity: "Article (5/4) of the Code of Criminal Procedure and the article17 of the Electronic Crimes Law Accordingly, the Jordanian courts have jurisdiction to consider this case, because according to the aforementioned legal articles, the Jordanian courts have jurisdiction if one of the parties to the case is Jordanian or residing in Jordan, or if the effects of the crime extend to inside Jordan and where Al Jazeera Channel, specifically the Opposite Direction Program, is located. It included expressions of slander and contempt for the people complaining, who were Jordanians, and that the program hosted a Jordanian person. Therefore, jurisdiction falls to the Jordanian courts, and accordingly, the appeal submitted is rejected."[518]

If any of the crimes specified in this law were committed using information systems within the kingdom, or if they caused damage to any of its interests or residents, or if the consequences of the crime resulted therein, wholly or partially, or if they were committed by any person residing within the kingdom, public rights and personal rights cases may be brought before Jordanian courts against the defendant[519].

Accordingly, we conclude that the legislative jurisdiction of the Jordanian judiciary falls within the following cases, as stated in all Jordanian legislation:

- If the electronic crime was committed using information systems within the kingdom.
- In the event of causing harm to the interests of the Jordanian state.
- In the event of causing harm to the interests of any resident of the kingdom, whether a citizen or not.
- If any impact resulted from this crime, either wholly or partially, within the kingdom's borders.
- If this crime was committed by any person residing within the kingdom, whether a citizen or not.

---

[516] Article 7 of the Jordanian Penal Code

[517] Article 5/4 of the Jordanian Code of Criminal Procedure

[518] Criminal Cassation Decision No. 1549 of the Year 2014, dated 8-9-2014. https://qarark.com/

[519] Article 17 of the Jordanian Electronic Crimes Law

It was stated in this decision that the appealed decision is correct, as the judicial jurisdiction is in accordance with the article5 of the Code of Criminal Procedure and the article17 of the Electronic Crimes Law that the place where the effects of the crime arise is a criterion for international jurisdiction, not local jurisdiction. Therefore, considering the place of residence of the complainant, which is the place of receiving messages, as the place where jurisdiction is held is not correct. From the legal perspective, therefore, the place of residence of the complainant, which is the city of Tafila, does not have jurisdiction, and the Aqaba Court has jurisdiction because the act was committed there..[520]

6.4.1.2.2 The Iraqi Legislator's Stance on Jurisdiction Conflict

The Iraqi legislator followed the same approach that the Jordanian legislator followed in his traditional texts, and we will explain this as follows

The Iraqi citizen is tried by the Iraqi courts for any obligations he may have, even if they are outside Iraq[521].

If they are present in Iraq, the foreigner will be tried by Iraqi courts.and If the lawsuit is about immovable property in Iraq or movable property in Iraq at the time the claim is filed.and If the lawsuit is based on a contract signed in Iraq, an obligation to execute, or an incident that occurred in Iraq[522].

Electronic documents are considered sent from the location of the website's headquarters and received from the location of the recipient's headquarters. Unless the sender and recipient agree otherwise, the scene of residence is considered the transaction's headquarters if neither has one. If the website or the recipient has multiple headquarters, the one closest to the transaction is considered the scene of sending or receiving. If determination is not possible, the primary business scene is regarded as the scene of sending or receiving[523].

From the above text, it can be concluded that jurisdiction in crimes related to electronic transactions is held by Iraqi courts if the defendant is an Iraqi or a foreign resident in Iraq, or if the foreign individual's location of business is in Iraq.[524]

In my opinion i believes that Jordanian, Iraqi and Iraqi legislators did well when they explicitly stipulated judicial jurisdiction so as not to leave room for personal rulings, as this is

---

[520] Judgment No. 12 of the Year 2021 - Court of First Instance in Al-Tafilah in its appellate capacity, dated 17-1-2021.

[521] Article 14 of the Iraqi Civil Law

[522] Article 15 of the Iraqi Civil Law

[523] Article 21 of the Iraqi Electronic Signature and Transactions Law No. (87) of 2012

[524] Ibrahim, Mohammed Majid Karim 2017, , p. 686.

an important issue and entails great obligations, especially in Iraq as an exporting country. Oil in large quantities.

6.4.2 Discretionary Authority of the Criminal Judge in Evidence Evaluation

To study the issue of the judge's authority to evaluate evidence, this falls under two frameworks: the formal framework for electronic evidence and the legal framework for electronic evidence, as follows:

6.4.2.1 The Formal Framework for Electronic Evidence

6.4.2.1.1 Electronic Evidence: Conceptual Delimitation:

Electronic evidence is defined as information of value that is stored, transmitted, or conveyed in digital form.[525]

Alternatively, it is what experts deduce from results built upon applications and principles, following several observations and notes. Through these, hidden results can be accessed through moral deduction, scientific judgment, and theories.[526]

In short, it is evidence derived from computer systems, presented in the form of electromagnetic or electrical pulses, which can be assembled and analysed using specific software, applications, and technology. They can be used in court[527]

6.4.2.1.2 Forms of Electronic Evidence

Forms of electronic evidence include tapes, magnetic discs, video cylinders, and other non-traditional electronic forms. It also encompasses displaying computer-processed outputs on its screen or on the internet through screens or visual disc units.[528]

6.4.2.1.3 Types of Electronic Evidence

Electronic evidence falls into two types: evidence prepared to be a means of proof, and evidence that no longer serves as proof. The latter type of electronic evidence arises unintentionally from an individual and leaves an impact without the perpetrator's intention. This type of evidence is known as electronic footprint, manifested in the effects left

---

[525] Zmanaki, Abdul Rahim 2021, p. 40.

[526] Fouda, Abdul Hakim 2014, p. 7.

[527] Mustafa, Aisha Ben Qara 2009, , Master's Thesis, p. 8.

[528] Digital Evidence and Computer Crime by Eoghan Casey, 1st edition, Academic Press, 2000.

by internet users. It includes recorded sent messages and received messages, along with all communications made via computers and the internet.[529]

This type of evidence is not essentially preserved by its originator. However, specialized means can preserve this evidence even after some time has passed. Communications over the internet and messages sent or received can all be printed using special technology.[530]

Additionally, electronic evidence is classified into fixed evidence and variable evidence. The basis for this classification is the type of memory used in computer devices for data storage, namely read-only memory and read-write memory. Fixed electronic evidence includes documents, documents, images, chat logs, browser history, audio or video recordings, and email messages. On the other hand, variable evidence consists of data stored in the random access memory of the device, such as time information, services, and operations of internet-based platforms.[531]

6.4.2.1.4 Nature of Electronic Evidence

Jurisprudence differed regarding the nature of electronic evidence and headed in three directions

- The first direction asserts that electronic evidence is material evidence, representing an advanced stage of tangible material evidence perceived by the senses This trend is justified by what they said is that electronic outputs can be extracted in the form of supports such as magnetic tapes or magnetic disks..[532]

- The second direction views electronic evidence as moral evidence, as it is not tangible. Material evidence requires material contact, whereas electronic evidence might not be tangible and might be perceived through a device's screen.[533]

- The third direction suggests that electronic evidence is a distinct and unique type of evidence. It doesn't fall under either material or moral evidence categories. It possesses independent characteristics that differentiate it from both types.[534]

In my opinion I agree with the second trend, as electronic evidence cannot be touched and is intangible, even if it is possible to extract it in a material form that does not change its

---

[529] Hajazi, Abdel Fattah B. 2007, p. 64.

[530] Abdel Muttalib, Abdul Hameed, Electronic Research and Investigation in Computer and Internet Crimes, p. 108.

[531] Al-Arabi, The Role of Electronic Evidence, p. 77.

[532] Hanafi, Hazem Mohammed, Electronic Evidence and Its Role in the Criminal Field, p. 15.

[533] At-Tahatawi, Ahmed Youssef 2015, p. 28.

[534] Al-Bushri, Mohammed Al-Amin 2004, , p. 235.

nature in any way. Therefore, there must be special legislation that includes it. However, I also believe that if there is no special legislation that includes it, then it is possible to use the traditional text and the analogy to it. In any case, a legal reform in this respect would be desirable.

6.4.2.1.5 Characteristics of Electronic Evidence

Electronic evidence does not differ from traditional evidence in terms of its effects, but this does not prevent it from being characterized by a set of characteristics that stem from its electronic nature.

- The techno moral nature of electronic criminal evidence necessitates the use of computer hardware, equipment, and software systems to realize it. [535]
- Electronic evidence is scientific evidence, serving the same purpose as scientific evidence by revealing the truth. The rules applicable to scientific evidence apply to electronic evidence, as they don't conflict with established scientific norms. [536]
- Electronic evidence is difficult to erase or delete, as it can be retrieved even after being deleted and repaired after being destroyed, subsequently revealed after being concealed. [537]
- Electronic evidence is subject to copying, allowing identical copies to be produced with equivalent probative value. [538]
- Electronic evidence is diverse, appearing in various forms. It can be unreadable, such as in non-network monitoring or technical network servers. Alternatively, it can be readable or comprehensible, as seen in stored images on a personal computer or in emails. [539]
- Electronic evidence is characterized by speed and low cost, enabling swift access to it anywhere in the world and facilitating its creation and distribution. [540]

---

[535] Farghali, Criminal Proof with Electronic Evidence, p. 15.

[536] Hamou, Nidal Yassin, The Role of Electronic Evidence in Criminal Proof, University of Tikrit Journal of Legal and Political Sciences, Volume 1, Year 5, Issue 19, p. 186.

[537] Mustafa, Aisha Ben Qara, the Validity of Electronic Evidence, p. 35.

[538] Mustafa, Aisha Ben Qara, the Validity of Electronic Evidence, p. 36.

[539] Hanafi, Hazem Mohammed, Electronic Evidence and Its Role in the Criminal Field, p. 19.

[540] Al-Aboudi, Abbas, Explanation of Provisions of the Evidence Law, p. 334.

- Electronic evidence crosses borders and isn't limited to a specific country or geographic region. [541]

- Electronic evidence excels in accuracy and clarity due to its origin from technology devices with minimal error rates. Furthermore, errors can be corrected without leaving a material trace. [542]

- Electronic evidence is also characterized by secrecy and legal security, being encrypted, and written in programming language. It can only be read by the concerned parties or through automated devices.[543]

6.4.2.2 The legal framework for electronic evidence

6.4.2.2.1 Challenges and Risks Facing Electronic Evidence

The technical nature of electronic evidence gives it a set of advantages and characteristics, but at the same time there are risks and problems resulting from this electronic nature of evidence, and this is what will be discussed.

- The electronic evidence contradicts the principle of that It is not permissible to fabricate evidencefor itself. One of the established principles in the field of evidence is that a fabricate cannot present evidence that it has created. Electronic evidence is extracted from a computer that is owned and controlled by the claimant, making it susceptible to modification by the claimant for their benefit.[544]

- Forgery and Electronic Hacking:

  Electronic hacking is conducted to damage electronic evidence. Electronic hacking is a result of technomoral advancement, leading to the creation of various methods that individuals can use to gain unauthorized access.[545]

- Errors that may affect the electronic evidence, and some of these errors are due to the human element, a technical error, or an environmental error. Regarding human errors, the French judiciary decided not to adopt the evidence because this evidence must be

---

[541] Al-Hawamdeh, Lawrence Said, The Validity of Electronic Evidence in Criminal Proof, Al-Buhuth Al-Fiqhiya Wa Al-Qanuniya Journal, Issue 6, 2021, p. 899.

[542] Al-Aboudi, Abbas, Explanation of Provisions of the Evidence Law, p. 335.

[543] Muhammad, Al-Maali, Faryan 2021, , Master's Thesis, , p. 14

[544] Adham, Mu'tasim Billah Fawzi, 2017, p. 178

[545] Al-Aboudi, Abbas, Explanation of Provisions of the Law of Evidence, p. 370.

submitted within a certain period and was sent by fax, and the fax did not contain paper and did not arrive on time[546].

As for the technical error, it is the error related to the technology and its misuse. As for the environmental error, it is what is in the environmental environment that affects the evidence or the electronic device, such as being affected by wind or rain.[547]

- Verification of Contracting Parties' Identities

In most cases, contracts are formed between two individuals who do not materially meet in one place. They are connected through the virtual world.[548]

6.4.2.2.2 Modern Brocedures for Seize Electronic Evidence

These procedures are carried out by seizing or intercepting electronic evidence and monitoring it. The Budapest Convention (2001) approved these procedures, and among the procedures it decided regarding stored data is the urgent reservation of data in Article (16/1) thereof, which stipulates:- " Each State Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or obtain expedited preservation of specified computer data, including traffic data stored by a computer system, particularly where there are grounds for believing that such data is particularly vulnerable to loss or modification." .

Taking into consideration the terms and conditions stipulated in the applicable legislation as well as the defendant's personal rights, to the judicial police officers, after obtaining permission from the competent public prosecutor or the competent court:- Entering and searching any place where evidence indicates that it will be used to commit any of the crimes specified in this law. Inspecting and examining devices, tools, programs, operating systems, the information network, and the means by which any of these crimes were committed. The employee who conducted the inspection or examination must write a report and submit it to the public prosecutor or the appropriate court[549].

This legal text shows the modern procedures used to seize electronic evidence, as these procedures are carried out by inspecting and examining devices, tools, programs, operating systems, the information network, and the means that evidence indicates that they were used to commit any of these crimes, and after carrying out this task by inspectors who have the status of judicial police and who They have a great deal of technical experience in these

---

[546] Al-Aboudi, Abbas, Explanation of Provisions of the Law of Evidence, p. 370

[547] Al-Aboudi, Abbas, Explanation of Provisions of the Law of Evidence, p. 370

[548] Mu'tasim Billah, Fawzi Adham, Electronic Contract Proof, p. 184

[549] Article (32) of the Jordanian Electronic crimes Law No. 17 of 2023

matters. A report is prepared in which the findings of the inspection are explained, and this report is submitted to the party that granted permission for the inspection, which is either the public prosecutor or the competent court.

6.4.2.2.3 The Importance of Electronic Evidence in Proof

Evidence, in general, is considered one of the most significant aspects that legislators and regulators worldwide need to pay attention to. This is due to the implications of such evidence in proving rights and obligations among members of society at various legal stances, particularly in cases of disputes. The high importance of electronic evidence can be summarized in the following points:

- Techno moral Advancements and Ease of Use: The evolution of technology and electronic means and their ease of use have led to their extended adoption.
- Economic Significance: Electronic evidence's economic significance is observed on an individual and corporate level. It reduces the financial costs associated with traditional documentation.
- Time and Effort Savings: It saves a significant amount of time and effort for parties involved in disputes.
- International Recognition: International recognition of electronic means as valid evidence in legal proceedings before the judiciary.
- Secure Preservation of Rights: Electronic evidence offers a secure method to preserve rights.[550]

6.4.2.2.4 Legitimacy of Electronic Evidence and Acceptance Conditions

To ensure the acceptance of electronic evidence as valid proof, it is essential that it is obtained through legal means; otherwise, the evidence could be invalidated.[551]

In criminal cases, whether the evidence is traditional or electronic, it must be obtained through lawful methods. This entails that the authorized entity responsible for collecting evidence adheres to the legally specified conditions.[552]

Regarding the legality of electronic evidence, a decision by the Jordanian Court of Cassation in its criminal capacity stated: “The reliable confession is the frank and clear

[550] Bur'ah, Bani Mahmoud, 2010, p. 28.

[551] Abdulilah, Ahmed Hilali 1997, p. 67

[552] Abdul Basir, Essam Afifi, 2003, p. 16

confession that is unambiguous and unambiguous and is not tainted by any kind of material or moral coercion, and which is also consistent with the facts of the case and the evidence presented therein. Accordingly, and since what was stated in the telephone recording between the complainant and her husband on the one hand, and what is discriminated against, On the other hand, it cannot be relied upon or relied upon in this way, especially since such recordings are considered to be in violation of Article (88) of the Code of Criminal Procedure, which makes it necessary to exclude such evidence due to illegality, lack of accuracy and clarity, and thus the lack of reassurance regarding what is contained in these recordings, which These two reasons must be rejected. Accordingly, since criminal rulings are based on crime and certainty, not doubt and conjecture, and if the evidence is clouded by doubt, then the reasoning for it becomes invalid, in this case, the person against whom the person discriminated against must be declared innocent of the crimes attributed to him due to the lack of convincing legal evidence against him, which must reject the appeal.discriminatory".[553]

As for the Iraqi legislator, he explicitly stated that it is not permissible to use any illegal means to obtain important evidence, including coercion or torture[554].

In my opinion, I think it would have been better if the Jordanian and Iraqi legislators had explicitly stipulated the legitimacy of electronic evidence, as well as its authority, and had not settled for the traditional texts and applied them.

6.4.2.2.5 Authentic of Electronic Evidence in Proof:

The authentic of electronic evidence means the extent to which rights can be proven through these means.[555]

During legal proceedings, electronic evidence is subject to the assessment of the court, allowing the judge the freedom to form their own judgment. This principle ensures the judge's He has the right in evaluating the presented evidence.[556]

The Jordanian Electronic Transactions Law No. 15 of 2015 considered electronic evidence admissible, much like conventional evidence. This stance is also supported by the Jordanian Data Law, as previously explained.

The Iraqi legislature has also aligned itself with the Jordanian one in this regard, as evidenced by the validity of electronic evidence stipulated in the Iraqi Electronic Signature and Transactions Law No. 87 of 2012.

---

[553] Cassation Ruling No. 4333 of the year 2019, dated 9-3-2020. https://qarark.com/

[554] The Iraqi Code of Criminal Procedure Article (127)

[555] For more information, refer to: Awwadah, Nasar Muhammad, The Extent of Legitimacy of Modern Technological Means in Proving Civil Matters, Doctoral Dissertation, Amman Arab University, 2006, p. 4.

[556] Rustom, Hisham 1999, p. 57

A decisions from the Babylon Misdemeanor Court convicted the defendant after reviewing Zain Company's response regarding the number in question and examining the contents of the messages.[557]

6.4.2.2.6 Discretionary Authority of the Criminal Judge Regarding Electronic Evidence:

The assessment of electronic evidence is subject to the jurisdiction of the competent court. In order to be convinced of the electronic evidence extracted from electronic media, the court examines and verifies it by presenting it in the trial session. This process allows for its discussion in the presence of the parties involved in the electronic crime dispute. The purpose is to arrive at a truth that satisfies the judge's conscience, ensuring that the innocent aren't wrongly convicted and criminals aren't allowed to escape punishment. Therefore, legislation grants the judge discretionary authority to weigh electronic evidence, much like traditional evidence presented in criminal cases. This discretionary authority is based on the judge's conviction and conscientious understanding derived from the case's facts, within the framework of logic and reason.

Countries have adopted various approaches in the field of criminal evidence, which include:

- Free Proof System: Many countries, such as France, Egypt, and Jordan, adopt this system. It grants the judge the freedom to assess the evidence.[558]

- Restricted Proof System: In this approach, the judge does not possess discretionary authority over the evidence. The law determines the judge's role in specifying the nature, type, legal value, and validity of the evidence in criminal proof. The United Kingdom is one of the countries that follow this system.[559]

- Mixed Proof System: This system combines elements of both the free and restricted proof systems. It allows the judge discretionary authority to accept evidence in some instances while denying such authority for other types of evidence.[560]

When we want to know the opinion of the Spanish legislator on this issue, the article588 answers that as it indicatedThe criminal judge has discretion in Spanish legislation regarding electronic evidence, but this discretion is subject to guidelines relating to specialization,

---

[557] Refer to the ruling of the Federal Babylon Court of Appeals, numbered 1887 /j/2017, dated 1/8/2017

[558] Al-Shadhli, Futoh Kamel, Mustafa, Computer Crimes, Copyright, and Law, Halabi Legal Publications, Beirut, p. 373.

[559] Arefa, Mohamed Abdel Hamid, 2018, p. 513.

[560] Hegazy, Abdel Fattah Beyoumi, Proof in Computer and Internet Crimes, Legal Books House, Cairo, p. 46.

sufficiency, exception, necessity and proportionality; The principle of proportionality is one of the principles that the court needs to weigh in determining the seriousness of the crime[561]

As soon as electronic evidence is presented, the court gains full jurisdiction to assess it. This falls within the jurisdiction of the judge overseeing the case. Regardless, the acceptance of electronic evidence rests on the judge's sole conviction, ensuring the evidence's integrity and the validity of the procedures used to obtain it. When the judge presents electronic evidence, their decision and explanation for not accepting it can lead to the exclusion of that evidence.[562]

Regarding the discretionary authority of the judge in Jordanian and Iraqi law concerning electronic evidence, both legislations stipulate the validity of electronic evidence and allow those who contest this evidence to prove otherwise. The judge has the authority to establish the facts through electronic evidence and also to reject such evidence while providing a rationale for the rejection. The purpose of providing rationale for rejection is that official electronic evidence can only be challenged through a claim of forgery. However, unofficial electronic evidence has various cases in which it cannot be rejected.[563]

[561] See Article 588.AA. From the Spanish Code of Criminal Procedure

[562] Hamou, Ahmed et al. 2015, p. 431.

[563] Al-Asaf, Faisal Sutoufi, 2023, p. 63.

6.5 CONCLUSION

- Criminal protection is not limited to the substantive aspect of electronic transactions, but rather this protection extends to include the procedural aspect as well.
- The Electronic crime Unit was established in Jordan, affiliated with the Public Security Service, in 2008. This unit is a unit specialized in Combat electronic crimes. It consists of a group of specialists in tracking electronic crimes. This unit uses advanced tools, in addition to seeking the help of telecommunications companies that provide Internet services. This unit works to investigate, research and investigate crimes occurring through the Internet. In Iraq, there is a department called the Electronic Crime Control Department, affiliated with the police. Iraqi.
- The jurisdiction of the judicial police during the research and investigation stage is limited to two matters: receiving reports, complaints, and conducting preview.
- The jurisdiction of the inspection mission in electronic crimes is limited to the information crimes unit located within the state, whose work is to investigate electronic crimes occurring within the borders of the state via the Internet, and the scope of the inspection is not limited, but rather broad, in order to find all persons contributing to the crime. Even if it is a small contribution.
- One of the special methods of combating electronic crimes is to intercept correspondence, record votes, and take pictures.
- Procedural protection at the trial stage consists of narrowing the scope of attendance at the trial resulting from a electronic crime, as its sessions are not open, which gives a kind of protection to the person of the perpetrator.
- A jurisprudential dispute arose over the conflict of jurisdiction with regard to the criminal information crime. Jurisprudence was divided into three directions: the approach. Of criminal activity, the approach. Of where the result is achieved, and the mixed approach.
- Electronic evidence is defined as evidence taken from computers and in the form of electromagnetic or electrical pulses that can be collected and analyzed using special programs, applications and technology and can be presented in the form of evidence that can be approved before the court.
- Modern procedures are implemented to control electronic evidence by seizing, intercepting, and monitoring electronic evidence.
- Means of proof, including electronic means of proof, are considered among the most important means that the legislator or regulator must pay attention to in various countries of the world because of the consequences of these means in proving the rights and obligations between members of society in their various legal positions.

7

Result and Conclusions

RESULT AND CONCLUSIONS

FIRST: THE RESULTS

The most comprehensive jurisprudential definition of electronic transactions is what has been defined in it as the completion of business and the conclusion of contracts through an electronic way. It also includes all activities and businesses related to the exchange of data and information, as well as goods and services via the Internet between consumers and companies, or between companies with each other, and it represents both parties to the contractual relationship in the electronic business environment. This definition is considered one of the most comprehensive definitions to explain what electronic transactions are, as it is a definition that includes contracts, the completion of work, and all private activities and works, whether it is an exchange of data and information, or an exchange of goods and services, as long as these activities are carried out through electronic means.

Among the positives of electronic transactions are that they cross geographical borders, achieve the principle of abundance, are subject to the provisions of international law, rely on electronic means of proof, achieve the health dimension, and achieve equality between ordinary individuals and people with special needs. Needs. . Dealing with electronic transactions is also one of the standards for countries' progress and development. One of the disadvantages of electronic transactions is that exposure to fraud is greater than fraud in regular transactions, and electronic fraud in electronic transactions is broader than fraud in regular transactions, in addition to the errors that occur in electronic transactions are greater than in regular transactions. This is because the contracting parties do not see each other. Some, and it is possible that they do not know each other either, and the perception of coercion is considered one of the defects surrounding electronic transactions, more than in regular transactions, because one party is the party that alone determines the conditions in some cases..

- The electronic transaction either has a local dimension or an international dimension.
- Whoever says that the international dimension in the electronic transaction is looking from the perspective of the cross-border nature of the electronic transaction, and that the electronic transaction may take place between states and sovereign states, then the rules of international law apply in this case, because the law of one state may not govern another state. It is also possible, through the law of will, to resort to the rules of international law and make it the governing law for electronic transactions

- As for those who say that electronic transactions are local, they look at the place of the contract,or the place of its implementation,or the nationality of the contracting parties, and even the authority of the will of the parties if they want to resort to the rules of local law in their electronic transactions.

- Financial data is considered personal data worthy of legal protection.

- The presence of criminal protection through legal legislation leads to preserving electronic transactions and keeping them from being exposed to danger.

- The threat to financial data is greater than threats to other personal data.

- There are many and varied forms of threat to financial data, from electronic piracy to phishing to penetrating vulnerabilities and decoding codes to blowing up websites and many others.

- An electronic contract is a contract characterized by a consensual nature, not an adhesion one, as the method used in contracting does not change the nature of the contract, and most contracts are consensual contracts, and adhesion contracts remain adhesion contracts, whether they are concluded by normal means or through electronic means, the means used In contracting do not change, the nature and reality of the contract.

- To prove electronic transactions, certain conditions must be met in order for the electronic signature of its owner to be proven. Also, certain conditions must be present in the record or electronic document so that it can be used as evidence in the event of disagreement between the two parties to the contract.

- Criminal intent in the electronic environment is based on three cases:

  A) The case of the perpetrator's will to achieve a result of his criminal behavior, such as the perpetrator's illegal entry to the website, knowing that this entry is illegal.

  B) In the case of permissibility of intent, and that is if one person sends another virus through computers, the intention is to reduction the speed of the device of the person to whom the virus is sent, and this virus works to destroy the device.

  C) The case of the enormity of the criminal result, when a person hacks another person’s device in order to obtain a file that contains personal photos of that person, then he publishes it, and along with the personal photos of that person, his financial data

- Among the crimes committed on the website is the crime of illegal entry or exceeding the authorized entry without making any order As well as the crime of unlawful entry

or exceeding the authorized entry in order to delete, add, modify or hack the data or information of the information system.

- The Jordanian legislator and the Iraqi draft criminalized illegal entry or exceeding the authorized entry and imposed financial fines and custodial criminalties for this crime.

- The aggravating circumstance is the crime of illegal entry or exceeding authorized entry if it affects national security, foreign relations, public safety, or the national economy.

- Criminal liability in the field of electronic transactions rests with the service provider in two cases:

  A) The case of being an accomplice to an electronic crime that is carried out by a person on the Internet.

  B) The state of being aware of the electronic content and allowing it to spread.

- The most important commitments of the service provider with regard to the criminalty liability are as follows:

  A) The commitment to inform the authorities in the event of publishing information related to a threat to the national or economic security of the state or publishing pornographic material.

  B) Commitment of electronic service providers to respect the right to privacy and confidentiality of correspondence.

  C) Electronic service providers must monitor information that constitutes a crime that threatens the security and safety of the state.

  D) The commitment to block websites, links or informational content at the request of the investigation and trial authorities

- Criminal protection is not limited to the substantive aspect of electronic transactions, but rather this protection extends to the procedural aspect as well
- There is a clear legislative deficiency in Iraqi legislation and the inability of traditional texts to keep pace with technological development due to the failure to ratify the draft electronic crime law.
- Political instability in Iraq may be the most prominent factor in the inability to ratify the Iraqi electronic crime law
- Failure to ratify the Iraqi electronic crime law will lead to negative consequences for the Iraqi state, as Iraq is an oil country and exports oil in large quantities. Now all

transactions and money transfers are done electronically, which necessitates the issuance of such a law.

- Among the rules that the judge resorts to in determining the applicable law in the event of a dispute is the language in which the contract was written, the currency in which the payment will be made, the nationality of the contracting parties, the place where the contract was concluded, or the place of its entry into force.

- Jordanian legislation has provided legal protection for individuals' personal data through legislation specific to electronic transactions, although the Jordanian electronic crimes law has been subjected to severe criticism because it restricts freedom of expression of opinion, but despite that, it achieves a kind of protection for individuals with regard to their electronic transactions and not harming them through any means. Social media also prevents criticism of the government more and more widely and imposes severe penalties for anyone who does so. This is due to the inability of traditional legislation to provide this protection. As for Iraq, the Iraqi electronic crimes law is still not in effect

- Both Jordanian and Iraqi legislation recognized the authentic of electronic transactions, and electronic contracts were given legal status as a contract that binds both parties to the content of the contract concluded between them by electronic means.

- Electronic crimes are crimes of a special nature that is, it occurs using electronic means, and the crime scene is often something intangible, but in order for criminal liability to arise from these crimes, the criminal act must be present, the essential of which is the technical activity. Likewise, the criminal intentmust be present, which is the planning and management of the offender and the presence of his intention to cause his crime in the electronic environment with his knowledge. The law criminalizes it, and there must be a causal relationship linking his technical activity and his intention to cause the crime in the electronic environment.

- Electronic evidence is considered intangible evidence, and extracting it in the form of CDs or hard disks does not change its nature in any way.

SECOND: RECOMMENDATIONS

The failure to stipulate the responsibility of the electronic service provider in Iraqi legislation, nor the cases in which criminal liability falls on the electronic service provider, will lead to a lack of control over the work of information systems and websites and will lead to the presence of many fraud operations due to the lack of control over electronic sites and

information systems. Therefore, the researcher recommends that this is stipulated in Iraqi legislation, as the Jordanian legislator did.

Ignoring the issue of severe the punishment for those who repeat crimes as if to encouraging individuals to commit crimes. The Iraqi legislator overlook this issue and did not severe the punishment for those who repeat crimes. This is a clear and disturbing lack as well. The researcher recommends that the Iraqi legislator enact in its legislation legal texts that tighten the punishment in the event of repetition.

Amending the article29 of the Jordanian Electronic crimess Law, which indicates that the penalty will not be mitigation if the investigative papers submitted to the Public Prosecutor and as if the Public Prosecutor is not a party concerned with the investigation. In fact, the Public Prosecutor is concerned with revealing the truth and investigating crimes, and if the accused provides any important information to revealing the truth and arrest the perpetrator, it must The penalty is mitigation to encourage the accused to provide information before the public prosecutor, and not just give this privilege to the police only. Accordingly, the researcher recommends amending and rephrasing this article.

The Jordanian legislator did not stipulate in any of its legislation an exemption from punishment, not in any case, unlike the Iraqi legislator, which stipulated cases in which one is exempted from punishment. Therefore, the researcher recommends that Jordanian legislation stipulate cases in which one is exempted from punishment, but on a narrow scale.

Failure to respect the dates for conducting inspections by conducting inspections outside the legally specified time frame may lead to a violation of individual freedom and the sanctity of homes, and Jordanian and Iraqi legislators ignored this issue. The researcher recommends determine a time limit for conducting the inspection after the inspection order is issued

- The researcher recommends working on launching an electronic platform in Jordan to report electronic crimes in Jordan, as many countries have done.

- The researcher recommends to the Jordanian legislator that electronic transactions include the personal scope in addition to the objective scope as the Iraqi legislator did, where he stipulated the personal and objective scope, where he stipulated that the electronic transaction is carried out by natural or legal persons..

- The researcher recommends Approval of the draft Iraqi electronic crime law
- The researcher recommends explicitly addressing the concept of possession contained in the definition of theft in traditional texts, and explicitly including this concept in the Jordanian legislation in the Electronic Crimes Law.

- The researcher recommends adopting a electronic crime law that takes into account the human right to expression.

- The researcher recommends controlling the broad terminology in the new electronic crime law, especially since it has been subjected to some criticism from international institutions, as it works to restrict freedom of expression in some of its texts.

- The researcher recommends that both Jordanian and Iraqi legislators define the storage service contractor

- Enacting unified global legislation related to issues of electronic transactions, taking into account that some actions are considered a crime in one country and are not considered a crime in another country.

- The researcher recommends that both Jordanian and Iraqi legislators define the electronic Evidence because of its great importance

- The researcher recommends that both legislators explicitly stipulate the legitimacy of electronic evidence and not just stipulate it's authentic.

- The researcher recommends setting a specific period for the start and end of the inspection to combine information and networks. The Jordanian legislator only specified the period in which the inspection must begin after the issuance of permission, and did not specify a date for its end. Leaving the door open in this way would constitute a violation of the privacy of individuals and companies, since this type of inspection can be carried out remotely without To feel the harmed person

- The researcher recommends that the legislator amend Article3\ C of the Electronic crimes Law by deleting the cases that he mentioned and that they represent special intent, and that he suffices with mentioning destruction so that it includes all acts, or that he adds a phrase as an example but not limited to it.

REFERENCES

• Abdullah, Fahd bin Saad (1996), Legal and regulatory provisions for crimes of forgery of official documents, Master's thesis, Higher Institute for Security Sciences, Riyadh, p. 293.

• Abdel Basir, Issam Afifi, The Principle of Criminal Legality, Dar Al-Nahda Al-Arabi, Cairo, 2003.

• Abdel Hamid, Tharwat (2001), The electronic signature, its risks, how to confront it, and its validity in proof, Dar Al-Nile for Printing, Publishing and Distribution, Cairo, Egypt.

• Abdel Rahman, Khaled Hamdi (2008), Expressing Will in the Electronic Contract, Dar Al Nahda Al Arabiya, Cairo.

• Abdel Salam, Mazhar Moataz, The Crime of Abstinence, 1st edition, Dar Al-Thaqafa for Publishing and Distribution, Amman, 1999.

• Abdel-Baqi, Mustafa (2018), Investigating and proving electronic crime in Palestine, a comparative study, research published in the University of Sharia and Law Sciences, Volume 45, Supplement 2

• Abdel-Ghani, Shaima (2007), Criminal Protection for Electronic Transactions, New University House, Alexandria, Egypt.

• Abdel-Hakim, Ibrahim, information crimes, research published in the Journal of Law and Human Sciences, Volume Two, Issue 23.

• Abdel-Ilah, Ahmed Hilali (1997), The Authenticity of Computer Outputs in Criminal Evidence, 1st edition, Dar Al-Nahda Al-Arabiya, Cairo.

• Abdel-Ilah, Ahmed Hilali (2013), Objective and Procedural Aspects of Information Crimes, Dar Al-Nahda Al-Arabiya, Cairo.

• Abdullah, Abdul Karim Abdullah (2007), Information and Internet crimes and electronic crimes, a comparative study in the legal system for combating information and Internet crimes with reference to the efforts to combat them internationally and locally, Al-Halabi Legal Publications - Beirut - Lebanon, 3rd edition.

- Abdullah, Ezz El-Din, Private International Law, 5th edition, Dar Al-Nahda Al-Arabiya, Cairo, 1965.
- Abu Al-Haija, Muhammad Ibrahim (2002), Arbitration via the Internet, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 1st edition.
- Abu Al-Haija, Muhammad Ibrahim (2017), Electronic Commerce Contracts, House of Culture, Amman, Jordan
- Abu Amer, Muhammad Zaki, Penal Code, General Section, Ma'arifat Establishment, Alexandria, Egypt, 1993.
- Abu Aqleen, Ahmed Fawzi (2012), Symptoms of eligibility, Master's thesis, comparative study between Palestinian and Egyptian law, Islamic University, Gaza, Palestine
- Abu Maria, Ali (2010), the electronic signature and the extent of its strength in proof, research published in the Hebron University Journal of Research, Volume 5, Issue 4
- Abu Salah, Wadah Mahmoud (2021), Legal adaptation of electronic banking transactions in light of Jordanian law, research published in the Journal of Scientific Development for Studies and Research, Volume 2, Issue 4
- Adham, Al-Muatasem Billah Fawzi, Proof of Electronic Contracting, Al-Halabi Legal Publications, Beirut, 1st edition, 2017.
- Afifi, Moataz Sayed (2013), Rules of Jurisdiction for Electronic Liability via the Internet, New University House, Egypt, 2013
- Agiza, Marwa Shibl, Al-Shammari, Khaled Butti, Electronic Marketing in the Arab World, Universities Publishing House, 2012
- Ahmed, Amanj Rahim, (2006), Mutual Agreement in Electronic Contracts via the Internet, 1st edition, Wael Publishing House, Amman, Jordan.
- Ahmed, Ayman Ramadan (2010), Criminal Protection of Electronic Signatures, PhD thesis, Ain Shams University, Egypt.
- Ahmed, Hilali Abdullah, Computer Systems Inspection, (2008), Dar Al-Nahda Al-Arabiya, Cairo, Egypt
- Al Jarallah, Abdul Aziz Ghurmallah (2017), Internet crimes punishable by stopping the Saudi electronic crime control system, a comparative study, University Book House, Riyadh, 2017

- Al Kharisa, Ahmed Muhammad Abdullah (2023), Procedural and Substantive Provisions for E-Commerce, research published in the Journal of Jurisprudential and Legal Research, Jeddah, Issue 41

- Al-Abadi, Muhammad Hamid (2015), New Crimes in the Light of Globalization, 1st edition, Dar Al-Masirah - Amman, Jordan

- Al-Ahwani, Hossam El-Din Kamel, Legal Protection of Private Life in the Face of the Electronic Computer, research published in the Journal of Legal and Economic Sciences, Ain Shams University, issues one and two, 1990.

- Al-Ajmi, Abdullah Daghash, Scientific and Legal Problems of Electronic crimes, Master's Thesis, Comparative Study, Middle East University - Amman - Jordan, 2014

- Al-Amayra, Munther Abdel-Razzaq Musleh (2012), The extent of criminal protection of information via computers and the Internet, doctoral thesis, Amman Arab University, p. 135.

- Al-Akaila, Abdullah Majed (2010), Al-Wajeez fi Judicial Police, Dar Al-Thaqafa for Publishing and Distribution, Jordan.

- Al-Alfi, Ahmed Abdel Aziz, Explanation of the Libyan Penal Code, Modern Egyptian Printing Office, Egypt, Alexandria, (1969)

- Al-Alfi, Muhammad (2008), Internet Addiction, Modern Egyptian Office for Publishing and Distribution - Cairo - Egypt

- Al-Assaf, Faisal Satoufi, What is electronic evidence in the Saudi system, a comparative study, research published in the International Journal of Law, April, 2023

- Al-Awji, Mustafa, General Criminal Law, Criminal Liability, Al-Halabi Legal Publications - Beirut - Lebanon, Part 2, (1982)

- Al-Ayeb, Samia (2020), The repercussions of the Corona pandemic and electronic commerce as a model, research published in the Journal of Labor and Employment Law, Issue 4, Volume 5

- Al-Basiouni, Abdel-Ghani (2003), General Theory in Administrative Law, Mansha'at Al-Ma'arif, Alexandria, Egypt.

- Al-Bishri, Muhammad Al-Amin (2004), Investigation of New Crimes, 1st edition, Naif University for Security Sciences, Riyadh.

- Al-Darini, Muhammad Fathi, Comparative Research in Islamic Jurisprudence and its Principles, 1st edition, Al-Resala Foundation, Beirut, 1994.

- Al-Desouki, Ibrahim, Legal Aspects of Electronic Transactions, Supreme Council for Scientific Publishing, Kuwait University, 2003.

- Al-Dhahabi, Khadouja (2019), Criminal Protection of Electronic Transactions, PhD thesis, Ahmed University, Algeria.

- Al-Fadl, Munther (1996), The General Theory of Obligations, Sources of Commitment, Dar Al-Nahda Publishing and Distribution Library, Amman - Jordan

- Al-Faridi, Adam Suleiman Dhiyab, Descriptions of Crimes, research published in Tikrit Law Journal, Issue 2, Year 2, Part 1, 2017

- Al-Feel, Ali Adnan (2012), Procedures for Investigation and Initial Investigation into Information Crime, Modern University Office, Alexandria.

- Al-Gamal, Hazem Hassan, Criminal Protection for Electronic Security, Dar Al-Fikr and Law, Egypt, 2015.

- Al-Gammal, Samir Hamid Abdel Aziz (2006), Contracting through Modern Communication Technologies, Dar Al-Nahda Al-Arabiya, Egypt.

- Al-Ghaferi, Hussein bin Saad (2007), Criminal Policy Confronting Internet Crimes, PhD thesis, Ain Shams University, Egypt

- Al-Ghafri, Saeed bin Muhammad, Compensation in Electronic Transactions, PhD thesis, Naif Arab University for Security Sciences, Riyadh.

- Al-Habara, Abdel Fattah Abdel Latif (2015), Criminal Procedures in Investigation, Dar Al-Hamid for Publishing and Distribution, Jordan

- Al-Haithami, Muhammad Hammad, The Presumed Error in Criminal Responsibility, Dar Al-Thaqafa for Publishing and Distribution - Amman - Jordan, 1st edition, (2005)

- Al-Halabi, Khaled Al-Sayyad (2011), Procedures for Investigation and Investigation of Computer and Internet Crimes, Dar Al-Thaqafa for Publishing and Distribution.

- Al-Halabi, Muhammad Ali Al-Salem (2009), Al-Wajeez in the Principles of Criminal Trials, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan

- Al-Hassan, Muhammad Tariq Abdel Raouf (2011), Online Fraud Crime, Al-Halabi Human Rights Publications, Beirut.

- Al-Hawamdeh, Lawrence Said, The Authenticity of Electronic Evidence in Criminal Proof, research published in the Journal of Jurisprudential and Legal Research, Issue Six, 2021.

- Al-Hawari, Ahmed Muhammad, Protection of the Vulnerable Bereavement in Private International Law, Dar Al-Nahda Al-Arabiyya, Cairo, 1995.

- Al-Hayazi, Ahmed Muhammad, The Criminal actof Crime, Al-Halabi Legal Publications - Beirut - Lebanon, 1st edition, 2010

- Al-Helou, Hassan Aziz, Al-Zubaidi, Jalal Khudair, Terrorism in International Law, Academic Book Center, 2015

- Al-Hindawi, Hassan (2005), Private International Law, Conflict of Laws, General Principles and Functional Solutions in Jordanian Law, A Comparative Study, Dar Al-Thaqafa for Publishing and Distribution, Amman - Jordan.

- Al-Husseinawy, Ali Jabbar (2009), Computer and Internet Crimes, Al-Yazouri Scientific Publishing and Distribution House, Amman, Jordan.

- Al-Husseini, Ammar Abbas (2015), Criminal Investigation and Modern Means of Detecting Crime, Al-Halabi Legal Publications, Beirut, Lebanon

- Al-Husseini, Ammar Abbas, Computer and Internet Crimes, 1st edition, Zein Law Library, Beirut, 2017.

- Al-Husseini, Sami Hosni (1972), The General Theory of Inspection in Comparative Egyptian Law, Dar Al-Nahda Al-Arabiya, Cairo, Egypt.

- Al-Ibrahimi, Muhammad Majeed Karim (2017), Obstacles to electronic commerce and the requirements of the legal system to confront them, research published in Al-Muhaqiq Al-Hilli Journal of Legal and Political Sciences, second issue, ninth year.

- Al-Issawi, Youssef Mazhar (2020), Impersonation to obtain economic benefit as a form of fraud, research published in the Tikrit University Journal of Law, Volume 4, Issue 3, Part 2

- Al-Jabour, Muhammad Al-Waseet in the Penal Code, General Section, 1st edition, Dar Wael, Amman, 2012.

- Al-Jubouri, Salim Abdullah, Legal Protection of Internet Information, Al-Halabi Legal Publications, Beirut, Lebanon.

- Al-Khaili, Shamsan Naji Saleh, Crimes Illegally Used on the Internet, Dar Al-Nahda Al-Arabiya, Cairo, 2009.

- Al-Khalayla, Ayed Raja, Electronic Tort Liability, Dar Al-Thaqafa for Publishing and Distribution, Amman, 2011.

- Al-Maaytah, Hamza Atef Ali, the crime of electronic fraud, Master's thesis, Mutah University, 2012

- Al-Malat, Ahmed Khalifa (2005), Information Crimes, A Comparative Study, Dar Al-Fikr Al-Arabi - Cairo - Egypt

- Al-Manasa, Osama Muhammad, Al-Zoubi, Jalal Muhammad (2017), Technical Crimes in Electronic Information Systems, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 3rd edition.

- Al-Maraghi, Ahmed Abdel-Ilah, Criminal Liability of Internet Service Providers, Helwan University, Egypt, 2020

- Al-Maraghi, Ahmed Abdullah, Electronic crime and the Role of Criminal Law in Reducing It, National Center for Legal Publications, Cairo, 2017

- Al-Marsafawi, Hassan Sadiq, Rules of Criminal Liability in Arab Legislation, Institute of Arab Research and Studies, Cairo, 1972.

- Al-Mashhadani, Muhammad Ahmad, Al-Waseet in Explanation of the Penal Code, Al-Warraq Publishing and Distribution Foundation - Amman - Jordan, 2003.

- Al-Masirfi, Muhammad (2008), Buying and Selling via the Internet, Modern University Office for Publishing and Distribution - Alexandria - Egypt

- Al-Masry, Hosni (2006), International Trade Complex, Dar Al-Kutub Al-Qanuniyya for Publishing and Distribution, Cairo - Egypt.

- Al-Masry, Muhammad Walid (2002), Al-Wajeez fi Explanation of Private International Law, a comparative study of Jordanian law with Arab legislation and French law, University Library for Publishing and Distribution, Amman - Jordan, 1st edition.

- Al-Momani, Bashar (2004), Problems of Contracting via the Internet, Dar Al-Kitab Al-Hadith for Publishing and Distribution, Irbid, Jordan.

- Al-Momani, Omar Hassan (2003), Electronic Signature and Electronic Commerce Law, Wael Publishing House, Amman.

- Al-Morsi, Abdul Aziz (2005), The extent of the validity of electronic documents in civil and commercial matters in light of the rules of ethics, without a publishing house.

- Al-Moumani, Bashar Talal (2003), Problems of Contracting via the Internet, doctoral thesis, Mansoura University, Egypt.

- Al-Moumani, Nahla Abdel Qader (2007), Information Crimes, 1st edition, Dar Al-Thaqafa Publishing House, Amman, Jordan.

- Al-Mousawi, Mona Turki, Fadlallah, Jean Cyril, information privacy, its importance and the dangers of modern technologies on it, research published in the Journal of the Baghdad College of Economic Sciences, University, special issue, 2013

- Al-Mubdi, Jihad Mahmoud, mutual consent in the formation of electronic commerce contracts, 1st edition, Library of Law and Economics, Riyadh, 2016.

- Al-Mutalaqa, Muhammad Fawaz, Al-Wajeez in Electronic Commerce Contracts, Amman, 2006.

- Al-Naimi, Alaa Yaqoub, The electronic agent, its concept and nature, research published in the University of Sharjah Journal of Sharia and Legal Sciences, Volume 5, Issue 3, 2009

- Al-Obaidi, Ali Hadi (2009), Named Contracts, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan.

- Al-Obaidi, Saddam and Awad Hussein, Provisions for Electronic Forgery Crimes in Islamic Jurisprudence and Positive Law, Arab Center for Publishing and Distribution, Cairo, 2020.

- Al-Otaibi, Muhammad Dhar (2013), The Legal System of the Electronic Contract, Master's Thesis, Comparative Study, Middle East University, Amman, Jordan

- Al-Qahwaji, Ali Abdel Qader, Explanation of the Penal Code, General Section, Al-Halabi Legal Publications, Beirut, 2007

- Al-Rashidi, Besman Fathi (2008), Electronic Commerce Contracts and the Rules for Concluding them, Master's Thesis, Institute of Arab Research and Studies, Cairo, Egypt.

- Al-Roumi, Muhammad Amin (2004), Electronic Contracting via the Internet, University Press House, Alexandria, Egypt.

- Al-Sadda, Abdel Moneim (1958), Lectures on Civil Law, Contract Theory in the Laws of Arab Countries, League of Arab States, Cairo - Egypt, Part 1

- Al-Saghir, Jamil Abdel-Baqi (2002), The Internet and Criminal Law, Dar Al-Nahda Al-Arabiya, Cairo, Egypt.

- Al-Saghir, Jamil Abdel-Baqi, Procedural Aspects of Internet-Related Crimes, Dar Al-Nahda Al-Arabi, Cairo, 2001.

- Al-Saifi, Abdel Fattah Mustafa, Al-Qaeda Al-Criminal, Dar Al-Nahda Al-Arabiya, Cairo

- Al-Sarraj, Abboud, Explanation of the Penal Code, First Section, Syrian Virtual University - Damascus - Syria, 2018

- Al-Shammari, Saad Ghaleb Ali, electronic arbitration and means of proving it in international trade contracts, Arab-African Council for Integration and Development, Cairo, 2018.

- Al-Shawa, Muhammad Sami, Criminal Policy Confronting Money Laundering, Dar Al-Nahda Al-Arabiya, Cairo, 2002.

- Al-Shawabkeh, Hazem Salem, The Legal System for Electronic Signature, research published in the Jordanian Journal of Law and Political Science, Jordan, Volume 11, 2019.

- Al-Shawi, Tawfiq Muhammad, The Sanctity of Private Life and the Theory of Inspection (2006), Manshaet Al-Maaref, Alexandria.

- Al-Shazly, Fattouh, Kamel, Mustafa, Computer Crimes, Copyright and the Law, Al-Halabi Legal Publications, Beirut.

- Al-Sheikh, Mahmoud Muhammad (2015), The Law Applicable to the Electronic Arbitration Agreement, Dar Al-Thaqifa for Publishing and Distribution, Amman - Jordan

- Al-Shibl, Abdul Aziz, electronic assault, doctoral thesis, Imam Muhammad bin Saud University, Riyadh, 2010.

- Al-Tahtawi, Ahmed Youssef (2015), Electronic Evidence and its Role in Proof, Dar Al-Nahda Al-Arabiya, Cairo, Egypt

- Al-Talawi, Ahmed Abis Neama (2016), Cyber attacks, their concept and the international responsibility arising from them in contemporary international regulation, research published in Al-Muhaqqiq Al-Halabi Journal of Legal and Political Sciences

- Al-Tawalba, Ali Hassan (2004), Criminal Inspection, Computer System Science and the Internet, Dar Al-Kutub Al-Hadith, Amman.

- Al-Zibari, Michael Rashid Ali, electronic contracts on the Internet between Sharia and law, research published in the Iraqi Journal, 2012.

- Al-Zindani, Ibrahim Muhammad, Electronic crime from the perspective of Islamic Sharia and its provisions in Qatari law and Yemeni law, Pattani University, 2018

- Amara, Fawzi (2010), Investigating Judge, PhD thesis, Mentouri University, Constantine

- Ananzeh, Muhammad Abd al-Rahman, Criminal Intent in Electronic crimes, Dar Al-Ayyam Publishing and Distribution, Amman, Jordan, 2017.

- Aoun, Asmahan (2021), Elements of the Crime of Information Destruction and Its Punishments, Nile African Studies Journal, No. 13, October, 2021, p. 365

- Arabic Language Academy in Cairo (1960), Intermediate Dictionary, Al-Shorouk International Library for Publishing and Distribution - Cairo - Egypt, 1st edition.

- Arafa, Muhammad Abdel Hamid, The extent of the validity of electronic evidence in criminal proof, research published in the Journal of the Faculty of Law for Legal and Economic Research, Alexandria University, Issue 1, 2018.

- Arbab, Youssef Zakaria Issa, Legal Implications of Electronic Contracts via the Internet, research published in Al Jazeera Journal of Economic and Social Sciences, Volume 10, Issue 1, 2019

- Arshour, Haitham Suleiman (2017), The Concept of Public Order in Administrative Law, Master's Thesis, Comparative Study, Al-Nilein University, Khartoum - Al-Wadan

- Atallah, Shaima Abdel-Ghani Muhammad, Criminal Protection for Electronic Transactions, New University House, Alexandria, 2007.
- Australian Competition and Consumer Commission (2018), Targeting scams. Report of the ACCC on scams activity 2017, Commonwealth of Australia.
- Awad, Ali Gamal El-Din (2000), Bank Operations from a Legal Point of View, Arab Renaissance Publishing and Distribution House, Cairo, Egypt, 3rd edition.
- Awad, Mohamed Awad (2006), Inspection in Light of the Court of Cassation, Manshaet Al Maaref, Alexandria, Egypt
- Awad, Muhammad Mohieddin, Problems of Contemporary Criminal Policy in Information Systems Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 1998.
- Ayoub, Julius Antios (2009), Legal Protection of Personal Life in the Field of Informatics, Al-Halabi Legal Publications - Beirut – Lebanon
- Badr, Osama Ahmed, (2005), Consumer Protection in Electronic Contracting, New University House, Alexandria, Egypt.
- Bahr, Mamdouh Khalil, Protection of Private Life in Criminal Law, Dar Al Nahda Al Arabiya, Cairo
- Bakr, Ismat Abdel Majeed, The Role of Scientific Technologies in the Development of Contracts, Dar Al-Kutub Al-Ilmiyyah for Publishing and Distribution, Beirut, 2015.
- Bakr, Othman, Responsibility for Attacking Personal Data via Social Media Networks, research published in the Journal of the Faculty of Law, Tanta University, Egypt.
- Baraa, Bani Mahmoud, Electronic Means of Evidence, Master's Thesis, King Saud University, Riyadh, 2010
- Barham, Nidal Ismail (2005), Provisions of International Trade, Dar Al-Thaqafa for Publishing and Distribution, Amman - Jordan, 1st edition.
- Basila, Ayman Alaa El-Din (2018), Procedural Criminal Protection for E-Commerce
- Beltaji, Sameh Ahmed (2010), Procedural Aspects of Criminal Protection of the Internet, PhD thesis, Alexandria University, Egypt

- Bilal, Ahmed Awad, Material Crimes, and Criminal Responsibility Without Fault, Dar Al-Nahda Al-Arabiya, Cairo, 1993.

- Bin Jadid, Fathi (2013), The extent of the validity of writing and electronic signature in proving a contract concluded via the Internet, research published in the Journal of Legal Studies, Al-Basira Center for Research and Consulting, Issue 16.

- Bin Younis, Omar Muhammad Abu Bakr (2004), Crimes Arising from the Use of the Internet, Master's Thesis, Mansoura University, Egypt

- Bouamra, Mohamed, Nepal, Sayed Ali (2019), Electronic crime Investigation Agency in Algerian Legislation, Master's Thesis, Khadra Oulhaj University, Bouira - Algeria

- Boudi, Hassan Muhammad (2009), Online Contracting, Dar Al-Kutub Al-Qanuniyya for Publishing and Distribution, Cairo, Egypt.

- Burhan, Samir, Iber Umm al-Aqd in E-Commerce, Arab Organization for Administrative Development, Cairo, 2007.

- Cachard, Olivier (2004), Droit du commerce electronique, RDAI, nº 3.

- Casey, Eoghan (2011), Digital evidence and computer crime, Academic Press Inc, Third Edition.

- Danoun, Samir, Electronic Contracts within the Framework of E-Commerce Regulation, Modern Book Foundation, Beirut, 2012.

- Daoudi, Mihrab (2016), Special Methods of Research and Investigation into Organized Crime, PhD thesis, University of Algiers

- Dodin, Bashar (2006), The Legal Framework for the Contract concluded via the Internet, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 1st edition.

- El-Sayed, Atef, Educational and Information Technology and the Use of Computers and Video in Learning and Teaching, Ramadan Publishing and Distribution Press, Alexandria, 2000.

- Farah, Ahmed Qasim, The Legal System for Internet Service Providers, research published in Al-Manara Magazine, Al-Bayt University, Mafraq, Jordan, Issue 1, Volume 92, 2005.

- Fathi, Ben Jadid (2012), Protecting the right to privacy during online contracts, research published in the Journal of Law, third issue.
- Féral-Schuhl, Christiane (2021), Cyberdroit: le droit à l'épreuve de l'Internet, Ed. Dalloz, Paris.
- Fikri, Ayman Abdullah, information crimes, a comparative study in Arab and foreign legislation, 1st edition, Library of Law and Economics, Riyadh, Saudi Arabia.
- Fouda, Abdel Hakim (2014), The Authority of Technical Evidence in Criminal and Civil Matters, Dar Al-Fikr Al-Jami'i, Egypt.
- Fouda, Abdel Hakim, Provisions of Causation in Intentional and Unintentional Crimes, Dar Al-Fikr Al-Arabi, Alexandria, Egypt.
- Gharib, Zainab Abdel Razzaq (2015) The validity of e-mail in evidence, Law Journal, 26.
- Guillemard, Sylvette (2003), Le droit international privé face au contrat de vente cyberspatial, Thèse de doctorat, Université Laval Québec.
- Gul, Halima, Mihoub, Ali (2020), the law applicable to e-commerce disputes, research published in the Legal Researcher Journal, Volume 1, Issue 1
- Habib, Adel Jabri Hamid (2003), The extent of civil liability for failure to adhere to professional or job confidentiality, Dar Al-Fikr Al-Jami'i for Publishing and Distribution, Cairo - Egypt.
- Hammad, Tariq Abdel-Al (2003), E-commerce, Concepts - Experiences - Challenges, University House for Publishing and Distribution, Alexandria - Egypt, p. 156
- Hamo, Ahmed et al (2015), Electronic Evidence from Legal and Technical Points, Institute of Law, Birzeit University
- Hamo, Nidal Yassin, the role of electronic evidence in criminal proof, research published in the Tikrit University Journal of Legal and Political Sciences, Volume 1, Year 5, Issue 19
- Harwal, Nabila Heba (2007), Procedural Aspects of E-Commerce in the Evidence-Collecting Stage, Dar Al-Fikr Al-Jami'i, Egypt.
- Hegazy, Abdel Fattah Bayoumi (2006), Principles of Criminal Procedure in Computer and Internet Crimes, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt.

- Hegazy, Abdel Fattah Bayoumi (2007), Criminal Proof in Computer and Internet Crimes, Dar Al-Kutub Al-Qanuni - Cairo - Egypt

- Hegazy, Abdel Fattah Bayoumi (2009), Criminal Protection of the E-Commerce System, Dar Al-Fikr University for Publishing and Distribution - Alexandria - Egypt

- Hegazy, Abdel Fattah Bayoumi (no year of publication), Introduction to Intellectual Property Rights and Consumer Protection in E-Commerce Contracts, Dar Al-Fikr Al-Jama'i for Publishing and Distribution, Cairo - Egypt

- Hegazy, Abdel Fattah Bayoumi, (2009), Procedural Aspects of Initial Investigation Work in Information Crimes, Dar Al Nahda Al Arabiya, Cairo, Egypt.

- Hegazy, Abdel Fattah Bayoumi, New Crimes in the Scope of Modern Communications Technology, National Center for Legal Issues, Cairo, Egypt.

- Hegazy, Abdel Fattah Bayoumi, the Legal System for the Protection of Electronic Commerce, Dar Al-Fikr Al-Jami'i, Egypt, 2002.

- Heshmat, Muhammad Ali Qasim (1993), Communications Technologies and Information Flow, Department of Culture Publishing, Imam Muhammad bin Saud Islamic University - Riyadh - Saudi Arabia

- Homsi, Hassan Abdel Basset, Proof of Legal Transactions That Have Been Concluded, Arab Nahda Library, Cairo, 2000.

- Hosni, Mahmoud Naguib (2021), Explanation of the Code of Criminal Procedure according to the latest legislative amendments, Dar Al-Nahda Al-Arabiya, Cairo.

- Hosni, Mahmoud Naguib, Explanation of the Penal Code, General Section, Arab Nahda Publishing and Distribution House - Cairo, 1989.

- Hussein, Sami Jalal (2011), Inspection of Information Crimes, Dar Al-Kutub Al-Qaniya – Egypt

- Ibn Manzur (1968), Lisan al-Arab, Sader Publishing and Distribution House - Beirut - Lebanon, 1st edition.

- Ibrahim, Ahmed Ibrahim, International Law on Conflict of Laws, Egyptian Nahda Library, 1997

- Ibrahim, Khaled Mamdouh (2006), Concluding the Electronic Contract, 1st edition, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt.

- Ibrahim, Khaled Mamdouh (2008), Electronic Arbitration in International Trade Contracts, New University Publishing and Distribution House, Alexandria - Egypt.
- Ibrahim, Khaled Mamdouh (2009), Criminal Investigation into Electronic Crimes, Dar Al-Fikr Al-Jami'i, Alexandria, Egypt.
- Ibrahim, Khaled Mamdouh, Electronic crime Security, University Publishing House, Alexandria, 2008.
- Ibrahim, Khaled Mamdouh, The authenticity of e-mail in proof, Dar Al-Fikr Al-Jami'i, Alexandria, 2010.
- Ibrahim, Khaled Mamdouh: Information Crimes, 1st edition, Dar Al-Fikr Al-Jami'i, Alexandria, 2009.
- Idrissi, Rashida Muhammad (2005), Concluding an Electronic Contract, Master's Thesis, Kuwait University, Kuwait
- Issa, Muhammad Gamal Attia, The Development of the Concept of Criminal Responsibility, A Comparative Study, Arab Renaissance House for Publishing and Distribution - Cairo - Egypt, (2009)
- Jaafar, Rabie Mahmoud Muhammad, Criminal Intent in Crimes Related to the Internet and Information Technology, Center for Arab Studies for Publishing and Distribution, Egypt, 2017
- Jalal, Sami (2011), Inspection of Information Crimes, Dar Al-Kutub Al-Qanuni, Cairo, Egypt
- Journalist, Rawan Atiyatallah, electronic crimes, research published in the comprehensive multidisciplinary electronic journal, issue 24, month 5, 2020
- Juffali, Hussein (2020), Criminal Protection of the Consumer in Electronic Transactions, PhD thesis, Al-Arabi Al-Nasibi University, Algeria.
- Khaled, Kawthar Saeed Adnan (2012), Electronic Consumer Protection, New University House, Alexandria, Egypt.
- Khalifa, Ilham (2016), Criminal Diet for Electronic Editors, PhD thesis, University of Batna, Algeria.
- Khalifa, Muhammad Ahmed Kasib, Evidence and Obligations in Electronic Contracts, Dar Al-Fikr Al-Jami'i, Alexandria, 1st edition, 2019.

- Khalifi, Samir (2010), Dispute Resolution in E-Commerce Contracts, Master's Thesis, Comparative Study, University of Tizi Ouzou, Algeria

- Mahat, Muhammad Thamer, Judicial Legal Protection of the Human Right to Privacy, Dhi Qar University, Algeria, 2015

- Mahmoud, Ban Saif Al-Din (2019), The electronic contract and means of proving it, research published in the Babylon University Journal of Human Sciences, Volume 27, Issue 7

- Makhloufi, Abdel Wahab, (2012), Electronic Commerce via the Internet, PhD thesis, Lahj Lakhdar University, Yatna, Algeria.

- Makki, Hassan, The Privacy of Contracting via the International Information Network, 1st edition, Zein Law Library, Beirut, 2019.

- Mansour, Muhammad Hussein, Electronic Responsibility, Ma'arif facility, Alexandria, 2006

- Manzolay, Saleh, The Law Applicable to Electronic Commerce Contracts, New University House, Alexandria, 2008.

- Markus, Suleiman, Al-Wafi in Explanation of Civil Law, Dar Al-Kutub Al-Qanuniyya for Publishing and Distribution - Egypt, 5th edition, Part 1, (1998)

- Matar, Essam Abdel Fattah (2015), E-commerce in Arab and Foreign Legislation, New University House, Egypt.

- Mehdaoui, Kamel (2010), La formation du contrat électronique international: le formalisme au regard de la convention CNUDCI 2005, Thèse de doctorat, Université du Québec.

- Michel, Tony Issa (2010), Legal Regulation of the Electronic Contract, Al-Halabi Publications for Publishing and Distribution, Beirut, Lebanon, 1st edition.

- Moazib, Abdul Khaleq Saleh Abdullah (2019), The Legal Framework for Electronic Transactions in International Trade, a legal study in accordance with international agreements related to international trade law, Arab Democratic Center, 1st ed.

- Moghabgab, Naeem (1998), The Dangers of Information and the Internet, Zain Legal Publications, Beirut, Lebanon.

- Mohamed, Nermin (2003), The Principle of Contracting Contractors and the Restrictions Relevant to it in International Protection Law, PhD thesis, Ain Shams University, Cairo - Egypt

- Moussa, Mustafa Muhammad (2015), Investigating the Crimes of the Information Society and the Virtual Society, Dar Al-Nahda Al-Arabiya, Cairo, Egypt

- Muhammad, Al-Maali, Faryan (2021), Authenticity of Electronic Means of Evidence, Master's Thesis, Mouloud Mammeri University

- Muhammad, Diaa El-Din Nasser Ismail (2018), The Law Applicable to E-Commerce Contracts, Master's Thesis, Larbi Ben M'hidi University, Oum El Bouaghi - Algeria

- Muhammad, Lina Jamal, Electronic crimes, 1st edition, Dar Khaled for Publishing and Distribution, Amman, 2016.

- Muqrash, Ahmed Samer (2018), The effects of using the Internet on the sanctity of private life, Master's thesis, University of Aleppo, Syria.

- Musa, Khaled Al-Sayyid Muhammad, Provisions of a Remote Work Contract, Library of Law and Economics, Riyadh, 1st edition, 2014.

- Musa, Talib Hassan, Al-Mawjiz fi International Trade Law, Dar Al-Thaqafa Publishing and Distribution Library, Amman - Jordan.

- Mustafa, Ahmed Mahmoud, Computer Crimes in Egyptian Legislation, Arab Nahda Publishing and Distribution House, Cairo, 2010.

- Mustafa, Aisha Ben Qara (2010), The authenticity of electronic evidence in the field of criminal proof, New University House, Alexandria, 2010

- Mustafa, Aisha Bin Qara (2009), The authenticity of electronic evidence in the field of proof, Master's thesis, Alexandria University

- Mustafa, Fahmy Khaled (2007), The legal system for electronic signature in light of international agreements and Arab legislation, New University Publishing and Distribution House, Alexandria - Egypt

- Mustafa, Hosni, Crimes of Injury and Battery, University Press House for Publishing and Distribution - Alexandria - Egypt, 1988.

- Mustafa, Khaled Hamed, Criminal Liability of Publishers and Providers of Technical Services for Misuse of Social Networks, Master's Thesis, Ajman University, UAE, 2013

- Najm al-Din, Najwa, the crime of theft via electronic means, research published in the Journal of the College of Law for Legal and Political Sciences, 2017.
- Nassif, Elias, International Contracts, Electronic Contract in Comparative Law, Al-Halabi Legal Publications, Beirut, Lebanon.
- Nayel, Ibrahim Eid, Criminal Protection of the Sanctity of Private Life in Light of the French Penal Code, Dar Al Nahda Al Arabiya - Cairo
- Nuseirat, Alaa Muhammad (2005), The validity of the electronic signature in proof, Dar Al-Thaqafa for Publishing and Distribution, Amman.
- Obaid, Raouf (1974), Causation in Criminal Law, Arab Nahda Publishing and Distribution House - Cairo - Egypt,
- Obaid, Raouf, Criminal Captivity between Jurisprudence and Judiciary, Dar Al-Fikr Al-Arabi, Beirut, Lebanon
- Obaidat, Lawrence (2009), Proving the Electronic Hub, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan.
- Odeh, Abdul Qadir, Islamic criminal legislation compared to positive law, Al-Resala Foundation - Beirut - Lebanon, 9th edition, (1987)
- Odeh, Nassar Muhammad, The extent of the authority of modern technological means in proving civil matters, doctoral thesis, Amman Arab University, 2006.
- Omar, Ahmed Mukhtar (2008), Contemporary Arabic Language Dictionary, World of Books for Publishing and Distribution - Cairo - Egypt, 1st edition.
- Qadri, Fella (2017), Electronic Contract, research published in the Journal of Business Disputes, Issue 22
- Qandil, Saeed, Electronic Signature, New University House, Alexandria, 2004.
- Qashqoush, Hoda Hamed, Computer Crimes in Comparative Legislation, Arab Nahda House, Cairo, 1992 AD.
- Qashqoush, Hoda, Computer Crimes and Other Crimes in the Field of Information Technology, Dar Al-Nahda Al-Arabiya, Cairo, 1993.
- Qayed, Osama Abdullah (1994), Criminal Protection of Private Life and Information Banks, Dar Al Nahda Al Arabiya, Egypt.

- Qazoura, Naila Adel Muhammad Farid (2005), Economic Computer Crimes, Al-Halabi Human Rights Publications for Publishing and Distribution, Beirut - Lebanon, 1st edition.

- Raafat, Radwan (1999), The World of Electronic Commerce, research published in the Center for Research and Studies at the Arab Administrative Development Organization, Cairo, Egypt.

- Rabie, Hassan Muhammad, General Principles of Crime, Dar Al Nahda Al Arabiya, Cairo, Egypt) 1996

- Ramadan, Medhat Abdel Halim, Crimes of Assault on Persons and the Internet, Dar Al Nahda Al Arabiya, Cairo, 2000.

- Rashida, Booker (2017), Criminal Protection of Electronic Transactions, PhD thesis, Sidi University - Algeria

- Rateb, Ahmed, Al-Sarayrah, Mansour Abdel Salam (2008), computer-based contracting, a study in Syrian and Jordanian legislation, research published in Mu'ta Journal for Research and Studies, Volume 23, Issue 5

- Reda, Afan Abdel Aziz, Legal Controls for the Validity of Electronic Signatures, research published in the Scientific Journal of Cihan University, Sulaymaniyah, Volume 2, Issue 2, December, 2019

- Rostom, Hisham Farid (2010), Procedural Aspects of Information Crimes, Library of Modern Machines, Assiut, Egypt

- Rostom, Hisham Muhammad Farid (1992), Penal Code and Information Technology Risks, Library of Modern Machines, Egypt

- Rostom, Hisham, Mohamed Farid, Penal Code and Information Risks, 1995, Typewriters Library, Assiut

- Rustom, Hisham (1999), Information Crimes, Principles of Rich Criminal Investigation, research published in the Journal of Security and Law, Dubai, Issue 2.

- Saad, Ahmed Mahmoud (1995), Towards Establishing a Legal System for Information Consultation Contracts, Automated Processing of Data Using Computers, Dar Al-Nahda Al-Arabiya for Publishing and Distribution, Cairo, Egypt.

- Saadi, Muhammad (2013), Digital Sovereignty or Internet Challenges to the Principle of State Sovereignty in Public International Law, research published in the Journal of Jurisprudence and Law, fifth issue, March

- Sadiq, Hisham, The Law Applicable to International Trade Contracts, research published in the Journal of Legal Studies, Issue 1, 2004.

- Saghir, Youssef (2013), Electronic crime via the Internet, Master's Thesis, University of Tizi Ouzou, Algeria

- Saidani, Naeem, (2013), Mechanisms for Research and Investigation of Information Crime in Criminal Law, Master's Thesis, Hajj Lakhdar University - Algeria.

- Saladin, Kazan Zainal Abidin (2021), The legal nature of electronic commercial contracts and their challenges, research published in the Journal of Legal Studies, Volume 7, Issue 1

- Salah, Yasser Wagih, digital signature is a technological development for legal authority, research published in the Journal of Arts, Literature, Humanities and Social Sciences, Issue 50, 2020.

- Salama, Ahmed Abdel Karim, the Theory of the Free International Contract, Dar Al-Nahda Al-Arabi, Cairo, 1989.

- Salama, Muhammad Abdullah, Encyclopedia of Information Crimes, Computer and Internet Crimes, Dar Al-Maaref Publishing, Istanbul, 2006.

- Salama, Saber Abdel Aziz, The Electronic Contract, 1st edition, without publishing house, 2005.

- Saleh, Nael Abdel Rahman, The reality of computer crimes in Jordanian legislation, research published in the Emirates University Journal, Volume 1, 2004.

- Salem, Abdul Karim (2018), The basis for determining the law applicable to electronic international trade contracts, research published in the International Journal of Legal and Political Research, Volume 2, Number 2

- Salhab, Lama Abdullah Sadiq (2008), Electronic Contract Shop, Master's Thesis, An-Najah National University, Nablus - Palestine

- Sassi, Toshin, Abu Bakr, Soleimani (2013), Criminal Protection of Private Life via the Internet, Master's Thesis - Abderrahmane Mira University - Bejaia - Algeria

- Sédallian, Valérie (1997), Droit de l'Internet: réglementation, responsabilités, contrats, Éd. Net press

- Shanab, Muhammad Labib, Al-Wajeez fi Sources of Commitment, Arab Nahda Library, Cairo, 1999.

- Sharaf El-Din, Ahmed (2010), Electronic Commerce Contracts, Dar Al-Fikr University for Publishing and Distribution, Alexandria - Egypt, 1st edition.

- Sheta, Muhammad, Criminal Protection for Computer Programs, 1st edition, New University Publishing and Distribution House, Cairo, 2001.

- Siham, Musa (2020), The impact of the Corona pandemic on the growth of e-commerce in the world, research published in the Journal of Sharia and Law Sciences, Issue 9, Volume 4

- Skeker, Muhammad Ali, Information Crime and How to Confront it, 1st edition, Dar Al-Gomhouria for Press and Publishing, Egypt.

- Sorour, Ahmed Fathi (1985), The Mediator in Criminal Procedure Law, Dar Al-Nahda Al-Arabiya, Cairo, Egypt.

- Strowel, Alain / Ide, Nicolas (2000), La responsabilité des intermédiaires sur Internet: actualités législatives et jurisprudentielles, RIDA, n° 185.

- Suleiman, Ali Ali, Memoirs on Private International Law, Office of University Publications, Algeria, 5th edition, 2008.

- Swailem, Muhammad Ali, Criminal Liability in Light of Criminal Policy, a comparative study between legislation, jurisprudence, and the judiciary, University Press House - Alexandria - Egypt, (2007)

- Taha, Mahmoud, Ahmed (2017), Legislative confrontation of computer and Internet crimes, a comparative study, Dar Al-Fikr and Law, Egypt.

- Tammam, Ahmed Hossam, Crimes Arising from the Use of Computers, 1st edition, Dar Al-Nahda Al-Arabiya, Cairo, 2000.

- Tawahir, Abdel Jalil (2012), an attempt to measure customer satisfaction with the quality of electronic services using the (Nerankl) scale, research published in the Journal of the Performance of Penal Institutions, Jilali University - Algeria, Issue 2

- Tawakkol, Fadi Imad Al-Din, Electronic Commerce Contract, 1st edition, Al-Halabi Legal Publications, Beirut, 2010.

- Thieffry, Patrick (2002), Commerce électronique: droit international et européen, LexisNexis, Paris.
- Tolba, Mohamed Fahmy, Computer Viruses and Data Security, Modern Egyptian Office Press, Cairo, 1992.
- United Nations Office on Drugs and Crime, Use of the Internet for Terrorist Purposes, United Nations, New York, 2013
- Van Overmeire, Xavier (2008), Le monde virtuel met au défit les législateurs: la problématique de la loi applicable dans le cyberespace, Lex Electronica, 13 (1).
- Verbiest, Thibault (2002), La protection juridique du cyber-consommateur, LexisNexis, Paris.
- Wahabia, Abdullah, Explanation of the Algerian Penal Code, Al-Kahina Press, Algeria, 2003.
- Waidi, Ezz El-Din (2017), Leakage as a Special Research and Investigation Method, research published in the Academic Journal of Legal Research, Issue 2, Abdel Rahman Hirah University, Algeria.
- Yaqut, Muhammad Mahmoud, The freedom of contractors to choose the law of international contracts between theory and practice, Mansha'at Al-Ma'arif, Alexandria, 2000.
- Yassin, Saad Ghaleb, Bashir Abbas (2006), Electronic Works, Dar Al-Manhaj for Publishing and Distribution, Amman - Jordan
- Younis, Arabs, Encyclopedia of Law and Information Technology, Part 1, 1st Edition, Publications of the Union of Arab Banks, 2002.
- Youssef, Amir Farag (2008), Electronic Commerce, University Press House, Alexandria, Egypt.
- Zahran, Hammam Muhammad Mahmoud (2004), General Principles of Commitment, Contract Theory, New University Publishing and Distribution House, Cairo - Egypt.
- Zamanaki, Abdul Rahim (2021), Electronic Evidence in the Criminal Field, research published in Legal Notebooks Magazine, Issue Seven.
- Zouina, The Law Applicable to International E-Commerce Contracts, University of Algiers, 2011

Research seminars, conferences and forums:-

- Al-Ali, Youssef, The extent of the validity of conflict of laws rules to govern transactions that take place via the Internet, research presented to the first scientific conference on legal and security research for electronic operations, Center for Research and Studies, Police Academy, 4-26-28-2003.

- Al-Hadithi, Ali Khalil Ismail (2011), The nature of electronic transactions and the consequences of legal conflict therein.

- Arhouma, Musa Masoud (2009), Procedural Problems Raised by Transnational Information Crime, research presented to the First Maghreb Conference on Informatics and Law, Academy of Graduate Studies, October 28, 29, 2009, Tripoli, Libya.

- Badawi, Bilal Abdel Muttalib, electronic banks, their nature, their transactions and the problems they raise, research on electronic banking between Sharia and law, United Arab Emirates University, 10-12-5-2003

- Fahmy, Dina Abdel Aziz, criminal liability arising from misuse of social networking sites, Fourth Scientific Conference on Law and Media, Tanta University, 4-23-24-2017

- Qayed, Osama Abdullah, Criminal Liability for Disclosing Professional Secrets, Electronic Banking Conference, Dubai, 12/10/2003, Volume 4

- Suleiman, Abdullah (2006), The Economic Impact of Implementing Electronic Government Business, Third Government Business Forum, Riyadh, Saudi Arabia, September 18-20.

Laws, regulations, legislation, international declarations, and legal drafts:

- Budapest Convention of 2001

- Draft of the Iraqi electronic crime project.

- Electronic crime Law No. 17 of 2023

- Electronic Transactions Law No. (20-43) of 2020.

- European Directive No. 3000/29.

- European Directive on Electronic Commerce No. 3000/29.

- Iraqi Civil Law No. (40) of 1951 AD
- Iraqi Civil Law No. (40) of 1951 and its amendments.
- Iraqi Consumer Protection Law No. 1 of 2010.
- Iraqi Electronic Signature and Electronic Transactions Law No. (87) of 2012
- Iraqi Penal Code No. 111 of 1969 and its amendments.
- Iraqi Signature and Electronic Transactions Law No. (87) of 2012.
- Jordanian Arbitration Law No. (31) of 2001 AD and its amendments
- Jordanian Civil Law No. (43) of 1976 AD and its amendments
- Jordanian Consumer Protection Law No. 7 of 2017.
- Jordanian Electronic Transactions Law No. 15 of 2015.
- Jordanian Penal Code No. 16 of 1960 and its amendments.
- Jordanian Telecommunications Law No. 13 of 1995 and its amendments.
- Kuwaiti Electronic Transactions Law No. (20) of 2014.
- Law No. 50 of 2003 regarding trust in the digital economy.
- Law No. 50 of 2003.
- Qatari Electronic Transactions and Commerce Law No. (16) of 2010.
- Syrian Electronic Transactions Law No. (3) of 2014.
- The European Convention on Human Rights, which was approved in 1950
- The Jordanian Constitution of 1952 and its amendments.
- The Universal Declaration of Human Rights, adopted by the United Nations General Assembly in 1948
- UAE Electronic Commerce and Transactions Law No. (1) of 2006.
- UNCITRAL Law on Electronic Commerce 1996

Judgments of courts of cassation and appeal

- Adecision by the Jordanian Court of Cassation - a general body - in its penal capacity - Resolution No. 1008 of 2020 dated 7-28-2020.
- Babylon Federal Court of Appeal ruling No. 1887/C/2017 dated 8/1/2017
- Cassation Penalty No. 1549 of 2014 dated 9/8/2014. https://qarark.com/
- Cassation Penalty No. 4333 of 2019 dated 3/9/2020. https://qarark.com/
- Decision of the Court of Cassation in its criminal capacity No. 3087 of 2022, dated 9/19/2022
- Decision of the Court of Cassation in its criminal capacity No. 570 of 2018, dated 2/21/2018
- Judgment No. 12 of 2021 - Tafila begins its appellate capacity on 1/17/2021.
- Rights Cassation No. 356 of 2021 dated 3/2/2021.
- Rights Cassation No. 8508 of 2022 dated 5/17/2023. https://qarark.com/

Through the World Wide Web, one can access many websites and conduct many electronic transactions in short time, and since many electronic transactions have a contractual nature, it was necessary to provide legal protection. Many countries enacted legislation through which they aimed to protect electronic transaction, the Jordanian legislator and the Iraqi legislator were not far from it. Both legislators decided to provide legal protection by enacting a legislation for electronic transactions in both countries with the aim of providing legal protection for electronic transactions in their civil aspect. This protection was not limited to the civil aspect in Jordanian legislation, but rather the protection included penal legislation as well through the enactment of a law for electronic crimes.