

Technological Development and its Impact on Cross-Border Crimes

التطور التكنولوجي وأثره على الجرائم العابرة للحدود

Salama Abdelaziz Hassan Aly

Assistant professor, Egypt / lawyersalama@gmail.com

Received: 20/11/2022

Accepted: 21/12/2022

Published: 01 /01/2023

Abstract:

As a résultat of thé global technological development, a new type of crimes has emerged, which is scientific crime, which requires accurate and highly developed scientific informational knowledge that keeps pace with the development taking place in the digital space. As for the importance of the study, it focuses on elaborating the relationship between contemporary technological development and the growth of transnational crimes, and aims to clarify the political, economic and military effects of scientific crime on states and how to address them. The problem of the study lies in the possibility of reconciling and harmonizing between the requirements of contemporary technology and the speed it requires in concluding international trade deals and paying their value electronically, and what international cooperation requires of examining and reviewing suspicious behavior.

key words: Technological development, cross-border crime

ملخص:

كنتيجة للتطور التكنولوجي العالمي، ظهر نوعاً جديداً من الجرائم وهو الجريمة العلمية، والتي تتطلب معرفة معلوماتية دقيقة ومتطورة تواكب التطور الحاصل في الفضاء الرقمي. أما عن أهمية الدراسة فتركز على توضيح العلاقة بين التطور التكنولوجي المعاصر وبين تنامي الجرائم العابرة للحدود، وهي تهدف إلى توضيح الآثار السياسية والاقتصادية والعسكرية للجريمة العلمية على الدول وكيفية معالجتها. وتكمن مشكلة الدراسة في صعوبة التوفيق والمواءمة بين متطلبات التكنولوجيا المعاصرة وبين ما تحتاجه التجارة من سرعة في إبرام الصفقات التجارية الدولية ودفع قيمتها إلكترونياً، وما يتطلبه التعاون الدولي من فحص ومراجعة للسلوك المشبوه.

الكلمات المفتاحية: التطور التكنولوجي ، الجريمة عابرة الحدود

1- Introduction:

Contemporary technology has gone through many developments that prompted international criminals to develop tools and means to commit transnational crime so that it has become more complex and harmful than before, and countries have realized that these developments require the enactment of new laws and the search for mechanisms to combat it. Providing citizens with information that helps them discover and report these crimes.

The study problem:

The problem of research is that technological development has led to the emergence of many crimes that are difficult to prosecute or determine the applicable law in terms of location because these crimes are usually committed by people belonging to more than one country, and then the problem lies in that the perpetrators of these crimes are among the smartest groups of society And the more countries devised the means to pursue them, the more these criminals developed themselves to keep pace with these means.

There are many questions that cannot be answered. How can we deal with the requirements of international trade in terms of speeding up the completion of transactions and paying their value electronically, and following up on suspicious transactions?

How can the proceeds of legal commercial transactions be distinguished from the proceeds of drug, arms and human trafficking? .

The difficulty lies in the fact that international gangs always cover up with legitimacy and take for themselves a legal entity, often a commercial company with branches in all countries of the world and has hundreds of bank accounts and has a legitimate activity, but that activity is not the basis for its work.

The study aims:

The research aims to shed light on the impact of technological development on the growing size and rate of information crime. And to clarify the relationship between technical development and the emergence of new means that help criminals achieve material, moral and political gains , The study also aims to search for a mechanism for international cooperation in order to protect international trade from suspicious deals that cover money laundering, arms sales, or slave trade. It also aims to clarify the latest methods used by international criminals to deceive victims and commit information piracy crimes to achieve material or political goals.

Study Methodology:

I noticed that the descriptive analytical approach is the most appropriate by analyzing the legal texts that deal with the criminalization of information piracy, analyzing the methods developed for electronic burglary, and showing the most appropriate ways to address these crimes and clarifying the role of countries in reducing the risks of technological development and benefiting from its advantages and reducing information crime.

2.-Technological development and its effects:

2.1- Technological development:

Technological innovations have occurred throughout history and have increased rapidly over the course of the modern era. Modern technology has evolved and coexisted with old technology before it replaced it. transport

provides exchange; From sailing to boats with to cars that replace horse transport. Technological Transformations (TT) describes how technological innovations occur and shield them in society. Besides technological developments, technological shifts take thinking in broader terms such as “user practices, organization, industrial networks, infrastructure, meanings, or symbolic culture.” technology, information technology, The technical development included commercial transactions, which require speed in payment, and bank transfers, with their pros and cons.

2.2- Technological effects:

technologies have advanced faster than any innovation in our history – reaching about 50 percent of the developing world's population in just two decades and transforming societies. By enhancing electronic connectivity, financial inclusion, and access to business and public services, technology can be a major factor in achieving equality.

In the health sector, for example, groundbreaking technologies powered by artificial intelligence are helping to save lives, diagnose diseases and extend life expectancy. In education, virtual and distance learning environments have facilitated access to programs for students who would otherwise be excluded. With the help of artificial intelligence, public services are becoming more accessible, more accountable through block chain-enabled systems, and are moving away from onerous bureaucracy. Big data can also support more responsive and accurate policies and programs ⁽¹⁾.

Today, technologies such as data aggregation and artificial intelligence are used to track and diagnose problems in agriculture, health, and the environment, or to perform everyday tasks such as handling traffic or paying bills. They can be used to defend and exercise human rights - but they can also be used to violate those rights, for example, by monitoring our movements, purchases, conversations and behavior. Governments and companies increasingly have the tools to extract and exploit data for financial and other purposes.

3- Technical crime:

3.1- Technical crime concept: Any illegal behavior that requires knowledge of computer technology⁽²⁾.

Some believe that technical crimes are crimes of money and people that are committed through the use of the Internet, whether inside or outside the country⁽³⁾.

Some believe that technical crime is any illegal and immoral behavior that is carried out through the automated processing and transmission of data⁽⁴⁾.

3.2- The legal nature of the technical crime:

The study of technical crime and its legal nature requires the researcher to know the applicable law⁽⁵⁾. This crime is related to the ability of the Internet to transmit information of a personal and public nature, Hence, studying the legal nature requires knowing the field of information transmission electronically, and whether it falls within the postal services or falls within the press and publishing services⁽⁶⁾.

Some believe that technical crime is committed via the Internet, and therefore the possession and transmission of information cannot be the same as possession of tangible things, Therefore, they exclude that the technical crime is like theft⁽⁷⁾.

Others believe that the information that is transferred and seized has a financial and economic value like money, and therefore the crime of transferring and possessing information is a crime of theft⁽⁸⁾.

Some believe that a distinction should be made between tangible material money such as magnetic tape, wires and cylinders on which information is stored, and intangible money such as information accessed by espionage, which is not considered money and does not apply to the description of theft. ⁽⁹⁾.

3.3-Characteristics of technical crime:

- The most important characteristic of information crime is that it crosses borders and is not bound by time or place, because the world is linked to each other by the Internet, satellites and satellite channels.

-Information technology crime is characterized as a soft crime that does not require violence or weapons, such as drug crimes, terrorism and theft, but it is done quietly.

-The information technology crime is distinguished from the ordinary crime in that it is difficult to prove because there are no physical traces such as

fingerprints and traces of vandalism, especially since the physical effects of that crime are easily erased.

3.4- Legality of Inspection of Information Systems:

There is a doctrinal dispute over the legality of state intervention to monitor information systems .

Some believe that the state does not have the right to interfere and inspect the information systems located in another country , Regardless of whether the purpose of the search is to seize evidence of a crime committed in the territory of the inspecting State.

Others believe that international law consists of consensus and permitting a particular country to inspect the information system of another country, provided that that country is notified⁽¹⁰⁾.

Some see the possibility of searching the accuser's computer, even if it is connected to a computer in another country, so it is permissible to search the connected data records ⁽¹¹⁾

The importance of the inspection arises when it is linked to a company that has many branches in more than one country, and the company's computer is linked to a network that extends abroad. Some believe that the inspection of the information network when it extends to the territory of another country, it violates the sovereignty of that country , Therefore, if the necessities of the investigation require conducting an inspection within the borders of another country, there must be international treaties permitting such inspection.⁽¹²⁾.

3.5- Reasons for the inability of Arab laws to address information crime:

a) - The principle of criminal legality dictates the inadmissibility of criminalization and punishment when the text is absent. This prevents the perpetrators of harmful behavior or danger to society from being punished by means of a computer or the Internet; As long as the criminal legislator has not enacted the necessary legislation to include this behavior within the circle of criminalization and punishment.

b)- The principle of territoriality is the dominant principle of modernization of place; However, this principle loses its applicability to cyber crime from

the application of the criminal law of the border. that go beyond the limits of place; Internet crime is transient.

c)- The lack of a clear and well-defined conception of the law and the judiciary towards cyber crime, as it is a modern crime, and this is more of a problem than a phenomenon, and because there are no traditions about it, as is the case with other crimes, and this is aided by the lack of centralization and ownership over the Internet.

d)- Despite the issuance of a number of Arab legislations regarding the protection of intellectual and industrial property that included the provision of computer programs and considered them among the works protected by law; However, the fight against cyber crime in Arab countries is still without legislative cover that defines it and criminalizes all its forms.

4.- The impact of technological development on the growth of crime:

4.1- The relationship between technological development and crime:

Technological development and the increasing use of the information network in all fields of life have resulted in an indispensable technological and information revolution⁽¹³⁾ . Technological development has directly affected crime, as it changes with the change of time and place and has evolved with the development of contemporary technology⁽¹⁴⁾.

With the advancement of technology and the transformation of countries towards digitization, another group has emerged in societies that seek to take advantage of this development in achieving criminal purposes by stealing information to achieve political, economic and terrorist purposes⁽¹⁵⁾.

Hence, technology has resulted in the emergence of many sects, including the extremist sect, who carry out activities that employ the Internet to publish, broadcast, receive and create websites and services that facilitate the transmission and promotion of intellectual materials that feed intellectual extremism, prompting some extremists to take the criminal path and there is what is known as the extremist information criminal. including for news media networks, that follow the activities of the collective and publish its statements and statements of its leaders, and these usually call

from Internet cafes and offices using all websites that seek to achieve propaganda purposes in their favor.

Another category appeared, namely spies who tamper and destroy the contents of the Internet on the one hand, and on the other hand they carry out information burglaries and download industrial secrets from a computer in one of the partners and send them by e-mail directly to their competitor, and one of the most important objectives of this category in the use of information systems to obtain information Enemies and friends alike.

4.2- Banking technology and its relationship to crime:

The emergence of online banking institutions, anonymous online payment services, and mobile transfers in virtual currencies such as bit coin has made it more difficult to detect an illegal transfer of funds. Moreover, the use of proxy servers and economization software makes money laundering complete, almost impossible to detect, as funds can be transferred or withdrawn without leaving a trace of an IP address.

The prevalence of drugs, and the rush to take them made them a popular market generating imaginary profits, and although they depend on adventures carried out by specialized mafias, they finally settle in certain markets to be sold in the sector the retail to facilitate daily consumption by addicts.

The technological development of banking has had a great impact on the growth of the volume of drug trafficking, as drug criminals hide in export and import companies to open fake commercial accounts for the purpose of promoting their illegal activity

4.2.1-Banking technology and the grows of crime :

Technological development has led to the emergence of Internet banks, which are considered one of the most important means of harnessing technology to serve the crime of money laundering ⁽¹⁶⁾.

With the development of banking technology, new methods of money laundering have emerged that banks resort to to help perpetrators of crimes. The bank only acts as a broker when it transfers funds between its branches in just countries in return for a high commission.

One of the methods on the basis of which these illegal funds obtained from theft operations, facilitating prostitution, bribery, drug smuggling, human smuggling, child trafficking, and gambling clubs are being laundered is that the owners of these illegal funds deposit them in banks or transfer them between banks to merge them with legitimate funds, and hide their sources. original. These funds may be transferred from internal banks to international banks with many branches in the world. Then the foreign banks themselves carry out another transfer of funds through their various branches, after which the owners withdraw their money from the banks to buy land, or contribute to transcontinental companies.

4.2.2-The role of the bank in the crime:

The bank receives the cash proceeds obtained from illegal activities and then enters them into the banking system or divides them into small amounts so that it is easy to transfer them by land, sea or air, and the division of amounts facilitates the possibility of sending them to multiple accounts belongs to one bank with branches in more than one country⁽¹⁷⁾. Hence, many of the world's banks involved in these crimes collude with smugglers to hide the true reason for the deposits and facilitate their transfer around the world. The bank also plays a vital role in keeping that money and hiding its source And cover up the criminals.

One of the most important contributions of the bank to these crimes is that it integrates suspicious funds into its activities such as lending and borrowing. This is for the purpose of introducing this money into the banking system to hide its illegal source ⁽¹⁸⁾.

4.2.3- E-commerce and high crime rate:

E-commerce has had a great impact on the growth of the volume and rate of information crimes, the impunity of perpetrators and the difficulty of prosecuting them. The economic openness to the world and the rapid technological development resulted in the difficulty of controlling commercial operations, which often cover up illegal activities.

We cannot deny that e-commerce has many advantages that make it much easier for the consumer than traditional shopping, and make it widely accepted, but - unfortunately - it has become a breeding ground for fraud

and money laundering, due to the lack of control over the actual sales volume, numbers and invoices issued and the inaccuracy of the record It is also possible for some e-merchants to hide under pseudonyms and fake e-cover companies, making identification critical. Electronic stores may not be able to access difficult, important and accurate data, and it is also impossible to know the nature of the electronic mediation relationship with the merchant, and the relationship of electronic stores to each other in the absence of legislative oversight

5.- Cyber crime risks:

5.1-The economic risks of technical crime:

A) The deterioration of the value of the national currency, as there is a link between information crime, such as money laundering, and the increase in demand for foreign currencies to which the smuggled funds are transferred with the intention of depositing or investing abroad, which leads to a decrease in the value of the national currency, which leads to a serious impact on the national economy due to laundering.⁽¹⁹⁾.

B) high rates of inflation; As this crime results in an increase in domestic liquidity in a way that is not commensurate with the increase in the production of goods and services; This leads to inflation in the country's economy due to the deterioration of the purchasing power of money and thus a consumer cash flow occurs, which contributes to the government's expansion of public spending in developing countries; This leads to the state's inability to pay public expenditures, which leads governments to compensate for the deficit by imposing many taxes, which leads to an increase in the general level of prices and thus inflation.⁽²⁰⁾.

C) Information crime, such as money laundering, results in a deficit in the balance of payments, especially the trade balance, the balance of capital transactions and foreign cash reserves, as well as an increase in the indebtedness of the state due to the increased demand for foreign currency. Which leads to the occurrence of a foreign exchange liquidity crisis, which leads to a shortage of the state's foreign currency reserves with its central bank.

D) low rate of saving and investment; As the money laundering process, which is a crime that affects the national income, as well as a kind of financial and economic corruption; Therefore, there is a decrease in saving due to the deduction of money from the national income, and with the decrease in the saving rate, there is an increase in the rate of consumption, which leads to a decrease in investment. There is no doubt that the exit of capital - national or foreign - leads to a decrease in investment ⁽²¹⁾.

E) The decrease in the rate of national income, if the latter is represented in the total returns obtained by the owners of the production elements from the citizens in return for the use of these elements in the production of goods and services, whether inside or outside the country during a certain period, the result of this is that the money smuggled abroad - from the state - to international banks In order to carry out the washing operations on them, they are considered as deductions from the national income; Thus, it represents a falsity in the national economy, which is detrimental to the latter. Because it is at the expense of the rest of the legitimate income holders in the country and thus contributes to increasing consumption rates in a way that exceeds the national income.

5.2- Security risks of technical crime:

Terrorism using social media has become one of the most worrying issues in various countries of the world. Local and international terrorist organizations use social media platforms in many of their activities. Such as: recruitment, training, and communication with its followers, supporters and donors. Social media is a cheap, easy and effective means, and through it, members of terrorist organizations spread their ideological ideas, propaganda and various activities. In contrast to the above, some terrorist organizations carry out what is called "internet terrorism", which is the use of the Internet as a means through which to launch an attack, carry out sabotage terrorist acts, penetrate security and information systems, and plant powerful viruses.

The new terrorism is no longer confined to the traditional organizations, which wage their struggles and carry out their operations within a specific country, instead the battlefield of the new terrorist groups has become

global, and the goals of the new terrorism are more global, and tend to be random. The new terrorism is more complex, and more difficult to confront and confront compared to the traditional terrorism. The new terrorism has become more liquid, and is based on a new network structure facilitated and linked by communication and information technology, and has a stock of people willing to do anything, and it causes expanded forms of destruction and devastation ⁽²²⁾.

5.3- Political risks of technical crime:

Technological development has led to the emergence of many crimes related to information technology and bank transfers, as global mafia gangs specialized in financing terrorist groups and recruiting young people spread to destabilize the political stability of countries and overthrow the ruling regimes in exchange for huge sums of money, and these gangs use electronic communications to communicate with their members and electronic banks to support them and their financing.

Many countries also resort to influencing electoral processes in other countries by communicating with their members and financing their electoral campaigns to help them reach parliament seats and influence political decisions in the country ⁽²³⁾.

Information crimes such as money laundering lead to the concentration of capital in the hands of a certain group in society, helping it to reach the highest positions in the state, controlling the political system, the police and the judiciary, and controlling all activities of state ⁽²⁴⁾.

Technological development has resulted in dangerous results, as many great countries have resorted to harnessing technology to inject huge sums of money to their followers in order to recruit them to corrupt the governments of other countries.

5.4- Social risks of technical crime:

Information crimes result in the flight of national income abroad and the state's inability to make the necessary investments to provide job opportunities, which leads to an increase in the unemployment problem ⁽²⁵⁾.

Information crimes such as money laundering lead to a widening of the gap between members of society, in addition to serious social consequences as a result of the wrong distribution of national income that they cause, which leads to the emergence of violence, terrorism and other crimes , As well as creating unfair competition in the market because criminals will get a lot of money unlike the rest of society ⁽²⁶⁾.

Also, the laundering of illegal funds may lead to the entry of funds to the state, but these funds are only short-term investments such as speculation in real estate and the purchase of tourist villages. It leads to social imbalance

6.- Arab efforts to combat technical crime:

Arab Convention on Combating Information Technology Offences stipulated in the first article that “The purpose of this convention is to enhance and strengthen cooperation between the Arab States in the area of combating information technology offences to ward off the threats of such crimes in order to protect the security and interests of the Arab States and the safety of their communities and individuals”⁽²⁷⁾ .

It is stipulated in the fourth article that " Every State Party shall commit itself, subject to its own statutes or constitutional principles, to the discharge of its obligations stemming from the application of this convention in a manner consistent with the two principles of equality of the regional sovereignty of States and the non interference in the internal affairs of other States " ⁽²⁸⁾.

The agreement, in Article (15) of it, regulates the use of information technology for terrorist purposes, stipulating that: Offences Related to Terrorism Committed by means of information technology

“Dissemination and advocacy of the ideas and principles of terrorist groups. Financing of and training for terrorist operations, and facilitating communication between terrorist organizations. Dissemination of methods to make explosives, especially for use in terrorist operations. Spreading religious fanaticism and dissention and attacking religions and beliefs”.

the Article 16 of the Arab Convention dealt with organized Offences crime committed by means of information technology “Undertake money laundering operations, request assistance or disseminate money laundering

methods. Advocate the use of and traffic in drugs and Psychotropic Substances. Traffic in persons. Traffic in human organs.

7. CONCLUSION :

From the foregoing, there is a relationship between contemporary technological development and information crime, and this has resulted in the emergence of modern means to commit crime, and it has become difficult to pursue the accused, which led to an increase in the volume and rate of crimes. As for the research results and recommendations, I summarize them as follows:

Research results:

- 1- The fragility of the systems for prosecuting perpetrators of technical crimes, whether at the level of national laws or international law
- 2-The phenomenon of information crime is taking on new patterns and a form of criminal intelligence, and this undoubtedly represents a serious and new challenge at the present time.
- 3- Perhaps one of the most complex problems facing the international community in pursuing transnational crime is that it is hiding in a seemingly legitimate business or transaction, and the sources of these crimes are difficult to examine because they occur in an intangible world. And the inspection violates the sovereignty of states.
- 4- Cyber crime is new and has not been dealt with in the traditional penal code, and therefore there are no provisions in the penal code related to it.
- 5- In electronic crimes, it is difficult to pass judgments against the perpetrators because it commit in more than one country and because the perpetrators destroy the evidence.
- 6- Law professors and judicial bodies are still unable to know the legal nature of cyber crime and whether it is theft or not. As a result, most of the jurisprudence does not see the application of theft provisions to the appropriation of electronic information.
- 7- Despite the successes that technology has achieved in all aspects of life, but it has been the cause of great harm to man, violation of his privacy, stealing his money and harming countries politically, economically and socially.

Research recommendations:

- 1- Training the judicial police, investigation and judiciary personnel on how to use information devices, tools, tapes and printing machines, and take note of how they are misused.
- 2- Training of judicial, investigation and judiciary policemen on how to detect and prove these crimes.
- 3- Urging countries to cooperate with each other, especially in the field of assistance and judicial representation to uncover these crimes, collect evidence to prove them, extradite the criminals who committed them, and implement foreign judgments of conviction and punishment of state nationals who commit them abroad.
- 4- At the national level, countries should adopt in their national legislation the criminalization of any behavior that would steal information, violate privacy or illegally break into other computers.
- 5- All Arab countries should seek to amend their national legislation in a manner commensurate with the prosecution of information crime and to expand the interpretation of the principle of territoriality to include crimes that occur outside the state as long as part of it has been completed within the state.
- 6- Every Arab country should adopt the teaching of computer and Internet crimes, including cyber-burglary and money laundering, as a basic subject for students of the Faculty of Law, in order to raise awareness of the dangers of these crimes and ways to confront them.
- 7- National laws must adopt electronic evidence as evidence in all information crimes, whether they occur within the country or extend their scope to other countries.
- 8- Countries should be keen to hold training courses in the field of detecting and proving information crimes and tracking their effects, and the Germans with programs that help restore evidence after it has been erased from the computer.
- 9- Policemen in the Arab countries need cooperation and exchange of experiences and information in the field of prosecuting cyber crimes and ways to prosecute their perpetrators, especially since money laundering

gangs belong to dozens of countries and exchange experiences in the field of impunity.

10- Technology is witnessing many developments and the development of new things. This portends the development of cyber crime tools and methods in a more complex and more virulent way than before, which requires countries to develop mechanisms to combat these crimes, follow all their developments, create strong lines of defense, enact laws and legislation, and educate people about the innovations of these crimes and encourage them. To report them. All this is to try to limit and reduce the amount of losses as much as possible at the individual, organizational and state level.

11- I recommend the establishment of advanced legislative systems to regulate the legal and regulatory environment that serves the security of information systems and technologies, I also recommend following up on the developments of cyber crime and developing the means, devices and legislation to combat it.

12- I recommend raising awareness and eradicating digital illiteracy, through media devices and social media platforms that contribute to the advancement of thought and technological awareness of citizens, on how to deal with the new digital world in which we have come to live, and which requires us to deal electronically, as many government electronic services and platforms have become available in a regular manner. Large to facilitate processing and faster completion of service delivery; Among the mechanisms are the work of programs to educate citizens on how to take precautionary measures to confront electronic crimes, how to deal with them when they occur, and the procedures followed to facilitate the work of the security services in identifying and controlling the perpetrator of the crime.

13- I recommend the legal and legislative confrontation to combat information crimes and the imposition of deterrent penalties for its perpetrators, that cooperation between Arab ministers be conducted to study all risks and threats resulting from the illegal use of the Internet, with the

aim of protecting the economy of Arab countries and with the aim of confronting risks that threaten Arab national security.

6. Bibliograp

- <https://www.un.org/ar/un75/impact-digital-technologies>.)¹
- ²) Ahmed Helali, 2003, Objective Procedural Aspects of Information Crimes, 1st Edition, Dar Al-Nahda for Printing and Publishing, Cairo, p. 13
- ³) Ghanem Mohamed, 2010, The Role of the Penal Code in Combating Computer Crimes, Legal Thought House, Egypt. p 12
- ⁴) Naela Adel, 2005, Economic Computer Crimes, Al-Halabi Publications, Beirut, p. 30
- ⁵) Hoda Hamed, 1992, Computer Crimes in Comparative Legislation, Dar Al-Nahda Al-Arabiya Edition, Cairo, p.13
- ⁶) Muhammad Zaki Abu Amer, 2017, University Press, p. 9
- ⁷) Dr. Muftah Al-Mutradi, 2012. Electronic crime, a working paper presented to the heads of the supreme courts in the Arab countries, p. 17
- ⁸) Dr.. Muhammad Abdullah Salameh, 2007, Encyclopedia of Information Crimes, Modern Arab Office, 1st Edition, Alexandria, pg. 43
- ⁹) Jalal Al-Zoubi 2013, Electronic Information Systems Technology Crimes, House of Culture for Publishing and Distribution, 1st Edition, Jordan, p. 36
- ¹⁰) Hilal Ahmed, 1997, Cyber crime and Overcoming Its Challenges, Dar Al-Nahda Al-Arabiya, Cairo, p. 23
- ¹¹) Abdel-Fattah Hegazy, 2006, Principles of Criminal Procedures in Computer and Internet Crimes, 1st Edition, Dar Al-Fikr El-Gamaeya, Alexandria, p. 381
- ¹²) Linda Bentaleb, 2017, Inspection in Information Crime, Journal of Legal and Political Sciences, Faculty of Law and Political Science, El-Wadi University, June 16, 2017, pg. 471
- ¹³) Hisham Rostom, 1994, Penal Code and Information Technology Risks, Modern Machines Library, Assiut, p. 28
- ¹⁴) Dr. Muhammad Sami Al-Shawa, 2018, Criminal Evidence in the Light of the Globalization System and Modern Technologies, An Applied Study on the European Union, Arab Renaissance House Edition, Cairo, p.5
- ¹⁵) Dr.. Adel Yahya, 2014, Criminal Policy in the Face of Information Crimes, 1st Edition, Dar Al-Nahda Al-Arabiya, Cairo, p.9
- ¹⁶) Jeddawi Mustafa, 2005, Electronic Money Laundering, Economic Horizons Magazine, Faculty of Economics and Facilitation Sciences, Blida University, No. (5), p. 60
- ¹⁷) Amjad Al-Khraisha, 2006, House of Culture for Publishing and Distribution, Egypt, p. 48
- ¹⁸) Kadur Ali, 2013, The Bank's Criminal Liability for Money Laundering Misdemeanor, p. 19
- ¹⁹) Dr. Safwat Abdel Salam, 2003, The Economic Effects of Money Laundering Operations, and the Role of Banks in C Dr. Sherif Sayed Kamel, 1977, Criminal Responsibility of Legal Persons, Dar Al-Nahda Al-Arabiya, first edition, 1997AD, p. 2015ombating it, Electronic Banking Conference, College of Sharia and Law, UAE University, p. 1343
- ²⁰) Dr. Sherif Sayed Kamel, 1977, Responsibility of Legal Persons, Dar Al-Nahda Al-Arabiya, first edition, 1997 , ,p.215
- ²¹) <https://www.ammonnews.net/article/417901>, on4, December,2018
- ²²) <https://idsc.gov.eg/DocumentLibrary/View/6244> , on 26, October , 2021
- ²³) Dr. El-Sayed Abdel-Khaleq, 1997, The Economic and Social Effects of Money Laundering Crimes, Dar Al-Nahda Al-Arabiya, p. 3

²⁴) Dr. Hamdi Abdel Azim, 2000, Money Laundering in Egypt and the World, Dar Al-Nahda Al-Arabiya, 2 nd publication , Egypt, p. 2013

²⁵) Dr. Ezzat Muhammad Al-Sayed Al-Omari, 2006, The Crime of Money Laundering, Dar Al-Nahda Al-Arabiya, 2006, p. 81

²⁶) Dr.. Nael Abdel Rahman Saleh, 2001, Money Laundering Crimes, Conference on Crime Prevention in the Era of Globalization. Sharia and Law, United Arab Emirates University, May 6-8, 2001, p. 20

Arab Convention on Combating Information Technology Offences Article No (1))²⁷

²⁸)The same Arab Convention Article No (2)