Inspection in Cybercrime

Dr. Jafar Ali Hammouri

Professor Emeritus In Criminal Law Jadara University

2022-2023

Introduction :

Cybercrime is characterized by the fact that it is committed in an electronic environment that is completely different from the traditional environment in which the crime is committed , and that the criminal procedure law came to be applied to a materially tangible world, the problem is about the adequacy of the traditional procedural texts to be applied to the technical inspection. Therefore, we must address the procedural legislation in order to be able to know the appropriateness of these procedures for the crime committed in the virtual electronic world .

In this time, the computer, mobile phone, or any electronic means is the repository of a person's secrets and his rule in the rule of the private house, so it isn't ppermissible to take any action that is not based on a legal text, It is established that the general rule in the interpretation of criminal law is that If the punitIve text is incomplete or ambiguous, then it should be interpreted broadly in the Interest of the accused, and that it may not be taken into account in the Code of Criminal Procedure by analogy against the interest of the accused; because there is no crime or punishment without a text. The fact that this principle guarantees man the right to a private life that is guaranteed by the constitutions, and this will only be achieved through a system that is well aware of and understands technical progress . Challenges to the Code of Criminal Procedure also appear, as there are no new legal rules for obtaining electronic evidence using any modern technology .

**The study consists of :**

**section One :** Action controls Inspection Cybercrime .

**Section two :** Network rules Inspection Cybercrime.

**Section three :** Remote inspection of electronic devices.

**Section One : Action controls Inspection Cybercrime**

Inspection is an investigation procedure aimed at seizing evidence, in order to reveal the truth, In order to attribute it to the accused. The purpose of the electronic search Is to seize the technical information or the files that contain the evidence of the crime, through which the crime was committed, and these files take the form of electronic impulses.

Inspection of cybercrime :

A procedure that allows the collection of evidence that is stored or recorded in electronic form (1)

Jurisprudence in France has seen that electronic signals are not considered tangible things, and therefore they are not considered a tangible physical thing, and traditional procedural texts do not apply to them . (2)

The Criminal Procedures Law plays a major role in preventing and combating cybercrimes, and is the dynamic tool that enables the state to limit these advanced crimes (3) .

Inspection in electronic crimes differs from inspection in traditional crimes, and it is a procedure for seizing evidence that is stored or recorded electronically for the purposes of obtaining it in a cartoon form within controls and conditions, according to a judicial authorization authorizing the inspection of electronic systems, and without the inspection permission, this procedure is considered invalid, and consequently the subsequent procedures are invalid (4).

The Inspection memorandum must be clear in identifying the system to be Inspected, and the inspection memorandum should be as general as possible so that its text Is not limited to a specific inspection scop .

The search warrant must include electronic devices and everything related to these devices, and to any other place within the territory of the state that is associated or related to this electronic device, in order to reach criminal evidenc .

And the Egyptian Court of Cassation ruled that (5), “when the appealed ruling was presented as a defense to invalidate the search of his home and the computer seized at his home because they were obtained without permission from the Public Prosecution, and he responded to it by saying :

And since it is about the defense of the invalidity of the search of the accused’s home for violating the text of Article 45 of the Code of Criminal Procedure, this defense is not appropriate and the reason for that is that the law prohibits the search of the house except on the basis of a judicial order, This means that the judicial order is necessary to search the house in all cases and that it is necessary to search the person in cases other than flagrante delicto (6)

It Is one of the investigation procedures and must in all Its cases in a way that does not contradict with public morals, does not threaten human dignity, does not cause harm to human health, and that the executor adheres to its content, and since that was and the permission of the Public Prosecution was issued by inspecting the Central …. Which is owned by…… To control fixed and portable computers, information storage units, magnetic disks, and memory flashes, as well as to track all links from the device in the central to any devices used In the commission of the incident, so the judicial officers moved to the location of that central and met with Its owner and responsible manager, so he decided that the accused was working for him In the central and that he was staying in the apartment Above, he has an Internet connection taken from him, so they went up to that apartment to track that connection, not to search his house, and they knocked on Its door, so the accused opened It for them and allowed them to enter. By examining the computer connected to the internet, taken from the central to be searched, It was found that the device was recorded and posted on it provocative phrases against state institutions and leaflets urging citizens Against the system of government in the country, which are crimes punishable by law, so they arrested him, and the crime was flagrante delicto, and flagrante delicto here is not an obligation. By witnessing the material element of the crime, but rather dependent on external manifestations that do not enter into the formation of the material element, but they themselves predict the occurrence of the crime and its affiliation with the accused, and then the entry of the judicial police officers into the accused’s residence has taken place in accordance with the correct law, and the payment is worthy of rejection .

Then he offered to plead the invalidity of examining the accused's computer before obtaining permission from the Public Prosecution, and he put it forward by saying: The permission issued by the Public Prosecution is that it was issued to the incident officer to search the central and track all connections taken from it, examine and seize them, which is with him examining the accused's computer. It was according to and based on the permission issued by the Public Prosecution, and the court turned away from this argument, since that was the case, and it was clear from the judgment notes that the two officers of the incident had obtained permission from the Public Prosecution to search a central (...) owned by (...) to control computers Fixed and portable machines and information storage units, as well as tracking all links issued by the central to any devices used in the commission of the incident, so they moved to his place and met with his owner and responsible manager, and he decided that the accused belongs to a group (...) and he has an internet connection taken from him, so they went up to his house to track that link and knocked on his door The accused opened them and allowed them to enter, and the second witness checked the appellant's computer, which indicated that unless the search was carried out and did not take place from the arrest warrants, there is a procedure in the accused's residence that in and of itself betrays that they searched and searched inside it in search of the seized items.

As this was the case, what the appellant mourns in this regard Is unfounded, and that the entry of the two officers of the incident Into the accused’s residence was with the consent of the latter, and what the judgment said in that Is justified and correct in the law, because the consent to enter and search the residence Is sufficient for the court to have determined it. from the facts and circumstances of the case and its conclusion from the evidence leading to it , Therefore, the entry of the two officers into the appellant's residence and the seizure of the computer used is correct and legitimate, and the court, if it considered it as such and convicted the appellant based on the evidence derived from it, did not violate the law. In addition, the appealed judgment was proven against the appellant through the security follow-up carried out by the first witness, the officer in the Information and Documentation Department of the Security Directorate…… Monitoring a page on social networking sites – Facebook (7) – in the name of Al-Thawra Network. Managing it by instigating hostilities against police personnel and the state system and using violence and incitement to demonstrate against the country's ruling system, It is useless that the officer's examination of the computer was Invalid because the cornea extracted from the computer was verified by the security monitoring of social networking sites;Because it Is decided that the invalidity of the search assuming it took place does not prevent the judge from taking all other elements of evidence that are independent of him and lead to the result of the search, and among these elements are what the security follow-up monitored, nor does It prevent the court from relying on the statements of the arresting officer in the procedures he initiated And he gained information that was not related to the alleged invalidity of the computer examination.

So it is clear from the foregoing that the technical inspection is without less than the competent authority based on the consent and express acceptance free from any defect of the satisfaction of the owner of the computer connected to the Internet taken from the exchange to be inspected, otherwise the inspection procedure is invalid.

**Section two**

**Network rules Inspection Cybercrime**

**One : Network Objective rules Inspection Cybercrime**

The objective rules for searching the electronic network include several conditions, the most important of The occurrence of a cybercrime and the percentage of the crime committed to a specific person, sufficient evidence or information should be available to the inspection,also they must place of inspection be determined, which is the electronic devices with all their material and moral components and communication networks (1) such as system programs and applications used by the owner of the device, and it is also represented by every electronic device, the devices connected to it, and the network that includes its components .

Accordingly, if the electronic device is linked to another device on the network, it may not be searched except with permission from the competent authority spatially, recorded in writing and dated, and for a short period of time, and specifying the purpose of the search,and it must be reasoned through the availability of evidence through suspicions derived from reality or evidence that indicates the existence of an electronic crime of the type of felony or misdemeanor, or that the crime has been initiated or has already been achieved until the issuance of the search warrant, and that the place of inspection Is specific and accurate, except Therefore, the inspection procedure is invalid.

**Second: the formal rules for inspecting the electronic network**

The formal rules for the inspection of the electronic network include that the inspection is carried out in an automated, electronic manner, and quickly, in order to preserve the evidence from destruction, deletion or modification, the inspection of all devices and data stored in them, and the transfer and copying of data, the inspection must be carried out by members who are technically specialized in electronic systems.

**Section three**

**Remote inspection of electronic devices.**

The data containing forensic evidence may be distributed over the network in places far from the location of the electronic device and from the physical and moral location of the inspection. The actual location of the data may be within another jurisdiction, or even in another country, which increases the complexity of crime control procedures. Referring to the general rules for inspection in the Code of Criminal Procedure, which require that no person be searched or entered into his home except based on an order issued by the competent authority, except for what is excluded by a legal text, and the search may be carried out without physical moving to the crime scene, so it is through virtual transportation, so an inspection takes place. Inspection of the virtual place electronically, through the computer of the person conducting the investigation and inspection, or by resorting to the office of the technical expert .

Article (57) of the French Code of Criminal Procedure stipulates that: “Disciplinary officers, or under their responsibility, and judicial police agents during execution, under the circumstances stipulated in this law, can access, through the computer system located in the places under inspection, the data of importance to the investigation and which are being stored In the system.” Aforementioned or in another computer system, and therefore such data can be accessed from the Initial system or available at the initial system"

Also they can under the terms of the Inspection provided for in this law, access via a system located in the Anti-Cybercrime Unit to the data of interest to the investigation that is being stored in another computer system, if this data can be accessed starting from the primary system or is available to the system, and stored In Another computer system located outside the national territory that is collected by the judicial control officer, taking into account the conditions stipulated in the international agreements in force .

Article (32) of the Budapest Convention stipulates that “any party may, without authorization from another party" :

Access to computer data stored publicly available, regardless of where the data is geographically located or received by a computer system in its territory, computer data stored in another party upon the legal and voluntary consent of the person who has the legal authority to disclose the data to that party through the system aforementioned computer. (9)

In view of the protection of the private life that a person enjoys, he is prohibited from accessing his electronic devices or e-mail, except after issuing a judicial permission to view the information contained therein that reveals the truth .

And the data that has been allowed to be accessed under the conditions stipulated in this article can be copied from any medium and information storage media that can be controlled and sealed under the conditions stipulated in this law" (10)

It is clear from the foregoing that remote searches within the territory of the state are contrary to the provisions of the constitution, unless it is with judicial permission and reason. And that remote search leads to prejudice the rights of individuals and their freedoms and privacy.

that remote communication or telecommuting: is the process of transferring data from a specific point in space and time called the source, to anotherr point called the destination.(11)

If the physical components of electronic devices are inspected in a private place, it requires the same procedures as the search for traditional crimes. What raises obstacles and difficulties is the inspection of the moral components of electronic devices, if they are connected in another place within the region. The matter is more difficult if it is connected to another place outside the region (12) in a way that makes the geographical boundaries disappear and disappear; In the Code of Criminal Procedure, the Jordanian legislator did not address the issue of extending the inspection to the electronic system that is authorized to be inspected and which is connected to another system remotely and in another place outside its territory.

As this Is in order to preserve national security and in view of the seriousness of cybercrime, the Code of Criminal Procedure and the Jordanian Cybercrime Law must include provisions that allow inspection and inspection procedures for the competent authority to the maximum extent possible, given that tracking the extended crime is very Important for the purposes of collecting evidence and revealing the truth, but In a manner It does not affect the freedom of individuals, as their freedom is protected under the provisions of the Constitution, the possibility of extending the search to any device connected and linked to the original electronic device, the subject of the crime, that is authorized to be searched within the territory of the state, provided that the data Is available from the main system, and in the event that there are risks that lead to the loss of evidence; As for the extension of inspection to the territory of another country, this Is done through agreements and treaties and reciprocity between grants and prohibitions, in order to preserve the security and stability of countries, and in the event of inspection of electronic means without the existence of agreements or treaties between the state parties, this is a violation of the sanctity of foreign laws And it contradicts the sovereignty of states, and it is possible to harm the national security of states through espionage on top secret Information.

Also, the formulation and implementation of search warrants in cybercrime pose great challenges. The search warrant must be issued after the actual occurrence of the crime and from the competent authority to issue It, and signed by the signature of the one who Issued it. Large quantities of information and data may be mixed up, or traces left behind that may be subject to erasure, damage, or deletion. The period of permission for the search must also be specified, because the person authorized to be searched does not remain threatened with his freedom and the sanctity of his residence. After the issuance of the search warrant and its failure to implement It, he The person conducting the search, except after renewing the search warrant again .

We also see that adjusting the electronic components in their intangible form is not conceivable in terms of the location, because the description of the physical thing does not apply to them, because the nature of the intangible things is data, information, and technical communications, so it must take a physical nature that can be referred to as evidence in proof before the subject judge, as if It is copied, whether visually or read, and gives it a physical characte.

**Findings and Recommendations:**

The phenomenon of cybercrime has produced a number of procedural challenges and difficulties, due to the immaterial nature of the means through which it is committed. There is difficulty in electronic inspection, whether directly or remotely, The fact that these crimes are committed in a virtual place and does not leave a tangible physical effect on the technical inspection of electronic means.

This has led to the difficulty of applying the current legal texts to the immaterial values ​​generated by cybercrimes. It is also a cross-border crime, and it may be linked to external parties, which also creates difficulty in tracking illegal activities, so we hope that the Jordanian legislator updates the traditional legislative texts, both substantive and procedural, to keep pace with technological development, so that they can coexist with each other in the same development, and the legislative text on Expanding the powers of conducting inspections to include all electronic devices associated with the device to be inspected within the territory of the state, and at the same time the concerted efforts of national and international legislators, to reduce cybercrime as it transcends countries and continents.

**Arabic references :**

1. د. أمير فرج يوسف، الإثبات الجنائيِّ في الجريمة الإلكترونيِّة والاختصاص القضائيِّ بها " دراسة مقارنة للتشريعات العربية والأجنبية, مكتبة الوفاء القانونية, الإسكندرية, 2016.
2. د هلالي عبد اللاه أحمد, المواجهة التشريعية لجرائم المعلوماتية في النظام البحريني على ضوء اتفاقية بودابست, مجلة الحقوق, جامعة البحرين, المجلد السادس, العدد الثاني, يوليو 2009.
3. د. إيهاب السنباطي, الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونيِّة ( بودابست 2001) والبروتوكول المحلق بها, دار النهضة العربية, القاهرة, 2008-2009.
4. د. يوسف عبد المنعم الأحول, قانون الإجراءات الفرنسي, دار النهضة العربية, القاهرة, 2016.
5. د. محمود مدين, فن التحقيق والإثبات في الجرائم الإلكترونيِّة, المصرية للنشر والتوزيع, القاهرة, 2020.
6. د. أمير فرج يوسف, الإثبات الجنائيِّ في الجريمة الإلكترونيِّة والاختصاص القضائيِّ بها " دراسة مقارنة للتشريعات العربية والأجنبية", مكتبة الوفاء القانونية, الإسكندرية, 2016.
7. د. علي جبار الحسيناوي, جرائم الحاسوب والإنترنت, دار اليازوري العلمية للنشر والتوزيع, الأردن, 2009.

**Foreign references**:

1. Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and legal response, International Telecommunication Union, 2012
2. Steven Malby Et d'autres, Étude détaillée sur la Cybercriminalité, United Nations Office on Drugs and Crime, Février 2013