DETERMINING THE JURISDICTIONAL RULES OF STATE IN THE CYBERSPACE

Dr. Naima MAIDI[1], Dr. Slimane CHELBAK[2] , Dr. Mourad GUERIBIZ[3]
[1]Laboratory of Law and Political Science, Amar Telidji University, Laghouat, Algeria, E-mail: maidimaidi178@gmail.com
[2]Center for Research in Islamic Sciences and Civilization (CRSIC), Algeria, E-mail: s.chelbak@crsic.dz
[3]Amar Telidji University, Laghouat, Algeria.
Received: 09/2024, Published: 10/2024

Abstract:
Jurisdiction is considered one of the most important topics that must be defined to confront crime, and after the technological development witnessed by humanity, it has become a duty and imperative for jurisprudence and the judiciary to develop new mechanisms to determine the relevant law to be applied, and to determine the competent judiciary, to follow up and punish the perpetrators of these crimes.
With this amazing and rapid development that human societies have known, crime has also known an unprecedented rapid development, which has created many problems, especially when modern technologies appeared and the resulting major change in the classification of crimes, as transnational crimes have emerged, crimes affecting the automated data processing system, and organized crime, which are new crimes that human societies have not known, which has forced jurisprudence and the judiciary to find mechanisms and principles to determine judicial jurisdiction in terms of place and applicable law.
Keywords: *cyberspace, technological development, jurisdiction, Internet crimes.*

INTRODUCTION:

Researchers agree that cybercrime has overturned many prevailing legal concepts, whether at the level of substantive law in terms of criminalization and punishment, due to the dual nature of its nature between a pure cybercrime targeting information systems and data in themselves, or as a traditional crime committed using information technology, as a mechanism for communication and planning to implement criminal projects, or at the level of procedural law due to its overcoming of the established rules as a general principle for research, investigation, prosecution and trial of perpetrators of traditional crimes, which proves that cybercrime has revolutionized the philosophy of criminalization, punishment and criminal procedures.
If research into the issue of the extent to which traditional jurisdiction rules accommodate the specificity of cybercrime is difficult, the difficulty stems from the definition of cybercrime itself, so most interested parties go on to say that cybercrime, as a new aspect of criminal behavior, can only be imagined through:
- To be embodied in the form of a traditional crime committed by electronic or digital means.
- To target the digital means themselves, primarily the database and information programs.
- To commit traditional crimes in an electronic environment, such as press crimes.

Since the jurisdiction of the judiciary is the authority of the court to rule on a case brought before it or the jurisdiction granted by the legislator to a court to adjudicate the cases brought before it, the nature of the cybercrime and the privacy it is characterized by have become the most prominent problems and challenges that raise questions about determining the court with jurisdiction to consider and adjudicate it, once its perpetrators are arrested and brought to justice.
One of the difficulties posed by cybercrime and its relationship to the subject of judicial jurisdiction are those cases in which the material behavior of the crime is distributed in more than one city, while its criminal result is achieved in another city, and thus each city has achieved one of the elements of the material element of the crime that is applicable, such as the case of

committing the act of threatening via electronic messages, as the material act may be committed in one city and the victim receives it in another city, after often passing through several cities.

On this basis, we can raise the following problem:

To what extent can the rules of jurisdiction be applied in the field of cyberspace?

The first section: The problem of the establishment of traditional jurisdiction in cyberspace

The spatial application of national criminal law is often determined according to one of four principles:

- The principle of territoriality;
- The principle of personalization;
- The principle of objectivity;
- And the principle of universality.

The importance of these principles varies among themselves, and their importance is graded according to their order, and most criminal legislations take the principle of territoriality as a general principle and then complement it with other principles.

The first requirement: Difficulties of establishing traditional jurisdiction in cyberspace

Determining the location of the crime in application of the territoriality principle came with some ambiguity in some legislations, such as the Kuwaiti Penal Code, which stipulated in its fifth article (5) that: "The provisions of this law also apply to the following persons:

First - Anyone who commits outside the country an act that makes him a perpetrator of a crime that occurred in whole or in part in Kuwait or an accomplice in it...", while some legislations came in detail in determining when the crime is considered to have occurred on the territory of the state, as jurisprudence and the judiciary, especially in France, did not tend to limit the determination of the location of the crime to known cases[1], but rather tended to expand in determining the location of the crime - one of the manifestations of which is the internationalization of the idea of the location of the crime in terms of reality - and considering each country competent to consider this crime.

The manifestations of this expansion can also be observed in the field of temporary crimes with transgressive effects, as despite the crime being executed on the territory of a state, the effects of this crime may extend beyond the borders of the executing state, here, the French judiciary did not deny its jurisdiction to consider such a crime because its effects were realized on French territory, as in one of the publishing crimes that occurred through a newspaper that was printed and distributed in a foreign state, but some of its copies were distributed in France, according to the jurisprudence of the European Court of Human Rights in July 2011, local courts must settle issues related to jurisdiction within the framework of applying the rules of private international law[2].

The spatial application of criminal law according to one of the four principles mentioned above is difficult, and sometimes leads to the raising of a positive conflict of jurisdiction between more than one national legislation[3], and other times a negative conflict of jurisdiction arises, with which the

[1] - These cases are:

(1) The occurrence of the crime with all its material element on the territory of the state;

(2) The realization of only one of the elements of the material element on the territory of the state;

(3) The realization of part of the behavioral element on the territory of the state;

(4) The occurrence of a crime closely related to the territory of the state by a person abroad, who is considered its perpetrator or accomplice,

(5) The beginning of the implementation of an act constituting the crime of attempt on the territory of the state. The third case represents a noticeable manifestation of the expansion in the application of the principle of territoriality, and the French legislator stipulated it in Article 112/2 of the new Penal Code.

[2]- French Society of International Law, Rouen conference (internet and international law), A. Pedone editions - Paris, 2014, p 29.

[3] -Article 3-1-b of the 1973 Convention, Article 5-1-b of the 1979 Convention, Article 6-1-c of the 1997 Convention, Article 7-1-c of the 1999 Convention, Article 9-1-c of the 2005 Convention, see:

Manual for international cooperation in criminal matters against terrorism, United Nations Office on Drugs and Crime, Vienna, 2009, P 35.

jurisdiction of any of the countries to prosecute the offender is removed, although this last type of conflict rarely occurs, because national legislations establish their jurisdiction according to the known criteria of jurisdiction. In the event of a positive conflict of jurisdiction between more than one country to pursue the same criminal activity, or in a case where a conflict arises as in transnational crimes, in which the material conduct of the crime is distributed in the territory of more than one country, or in the event that some elements of this conduct are stripped of their material specificity, such as electronic piracy, and forms of criminal participation that are carried out using modern communications devices, such a phenomenon imposes a conflict of jurisdiction and even ambiguity in determining its standard, requiring innovative solutions and the creation of new legal concepts, without prejudice to the principles of criminal legitimacy on which most national criminal systems are based. A controversy has arisen over the issue of storing information or electronically processed data outside the territory of the state, and here two opinions have emerged:

The first opinion: It is illegal for the authorities of a country to intervene and search the information systems located in the territory of another country, to uncover and seize evidence of a crime committed on its territory, based on the principle of territoriality of law[1], as a German court ruled in this opinion in a fraud crime committed in Germany that obtaining data related to this crime and stored in communication networks located in Switzerland can only be achieved by requesting assistance from the Swiss government.

In the incident of spreading the (love bug) virus in 2000, which caused the destruction of information on computers, when American experts discovered that this virus was sent from the Philippines, searching the suspect's house required the cooperation of the Philippine authorities and obtaining permission from the investigating judge in the Philippines.

The second opinion: International law must be formed through consensus at the international level towards allowing the implementation of these procedures if certain conditions are met, such as notifying the state whose information and data stored in its information systems are to be inspected[2]. In this manner, the European Council issued a recommendation on September 11, 1995, among several recommendations that addressed the problems of criminal procedures related to information technology, which stated that investigation procedures should assume the extension of procedures to other computer systems that may be located outside the state, and assume rapid intervention, and so that such a matter does not constitute an attack on the sovereignty of the state or international law, an explicit legal basis must be established for inspection and seizure procedures, and this authority must also be allowed to make records of current transactions and determine their source, which can only be achieved by activating and consecrating international cooperation agreements.

The question that arises here is how can the principle of territoriality be applied to crimes committed via the international information network, and how can the territory of the state in which such crimes occurred be determined, with their multiplicity, diversity and complexity?

The answer is that the current scientific progress and the development of modern means of communication such as the Internet and other forms of electronic communication via satellites have provided enormous opportunities to go beyond the principle of territoriality and adopt new proposals such as this conflict or at least arrange its criteria, because the criterion of territoriality of the law is no longer sufficient, nor perhaps the most acceptable in some crimes, but rather the

[1]- Hicham Mohamed Farid Rostom, Procedural Aspects of Cybercrimes, Arab Renaissance for Publishing and Distribution House, Cairo, 1998, pp. 170-171.

[2]- Abd Elfattah Hegazy, Combating Computer and Internet Crimes, An In-Depth Study in Cyber Law, 1st ed., Dar Al Fikr, Alexandria University, 2006, p. 14

importance of other criteria that were previously considered reserve has increased, such as the criteria of objectivity and universality[1].

The development of the concept of territoriality has also witnessed a remarkable development in terms of determining the location of the crime, as it is no longer necessary for a material act or even one of the elements that make up this material act to occur, but rather it has reached the point of completely removing the material character from the act, and thus a mere phone call with a person in another country was considered a justification for considering that the crime actually occurred within the territory of the state, and thus any attempt to formulate a criterion of territorial jurisdiction to prosecute cybercrime must reflect such new data to overcome the positive conflict of jurisdiction, and thus two approaches appear, which are:

- The first approach: is represented in trying to give priority to any of the conflicting countries according to one of the most effective and feasible jurisdiction criteria to ensure the prosecution of the crime, and it seems that the principle of territoriality is the most acceptable, as the state in which the crime occurs entirely or the greater part of the activity constituting its material element or the entire subsidiary activity, or in general the state in whose territory the proceeds of the crime are located, appears to be the most likely state to have jurisdiction to prosecute the crime and try its perpetrators, and this solution is not only justified in considerations of national sovereignty inherent in the principle of territoriality, but also in its practical feasibility, and that the evidence of proof is available in The place where the crime occurred (all or most of it), and it becomes easy to conduct investigations capable of revealing the truth.

Regarding the subject-matter jurisdiction, the Algerian legislator stipulated it for the first time as a new additional jurisdiction in the law on the special rules for the prevention and combating of crimes related to information and communication technologies of 2009, where Article 15 states: “In addition to the rules of jurisdiction stipulated in the Code of Criminal Procedure, Algerian courts have jurisdiction to consider crimes related to information and communication technologies committed outside the national territory, when the perpetrator is a foreigner and targets Algerian state institutions, national defense, or the strategic interests of the national economy.” Since this law applies to the prevention of acts described as crimes of terrorism or sabotage according to Article 4, paragraph (a) of the same law, this jurisdiction will be practical in confronting perpetrators of terrorist acts abroad.

The principle of territoriality comes after the principle of universality, as it is appropriate for most cybercrimes in which the activity constituting the material element is distributed across more than one country, after that, the principle of personalization follows in its positive aspect, as jurisdiction over the crime is vested in the country of which the perpetrator holds the nationality, and if his nationalities are multiple, it is the right of the countries of which he holds the nationality, so that some do not take the acquisition of a new nationality as a way to escape prosecution, and this criterion can also be resorted to in order to avoid the accused escaping prosecution when it is not possible to prosecute him according to any of the previous criteria.

The second solution or approach in trying to overcome the perceived positive conflict of criminal jurisdiction between two or more states is to support and confirm criminal prosecution in every case in which there is fear, for one procedural reason or another, that the perpetrator of the crime will escape trial[2], such as the crime occurring in the territory of a certain state and the accused being arrested in another state and having its nationality, as in this case, the conflict of jurisdiction arises according to two conflicting principles:

- The principle of territoriality, which grants jurisdiction to the State where the crime occurred;

[1]- Abd Allah Abd Elkarim Abd Allah, Cybercrimes and the Internet, a comparative study of the legal system for combating cybercrimes and the Internet - with reference to the efforts to combat them locally, Arab and internationally, 1st ed., Al-Halabi Publications, Lebanon, 2007, p. 47.

[2]- Djamal Mahmoud Al-Kurdi, The Competent Court and the Applicable Law Regarding Liability and Compensation Claims for Transboundary Environmental Pollution Damages, 1st ed., Arab Renaissance House, Alexandria, 2004, p. 123.

- The principle of universality of the right to punish, which grants jurisdiction to prosecute the crime to the State where the accused is arrested, and at the same time allows it to evade extradition on the basis that most States are not bound by any agreement to extradite their nationals[1].

In this case, it is necessary to recognize the principle of trial or extradition as required, and to recognize the possibility of referring the criminal case for the crime committed from one country to another, as well as to emphasize the necessity of exchanging all forms of legal assistance, pursuant to agreements between countries, and in particular with regard to obtaining the testimonies of persons and notifying judicial papers, examining objects, exchanging evidence, and resorting to judicial delegation, all of which is done in accordance with the law of the country requested to carry out these procedures, the deputized country, and not in accordance with the law of the country that delegated it, and there is no doubt that creating new active mechanisms by the United Nations within the framework of material and technical assistance, exchanging expertise and preparing databases will enable everyone to contribute effectively to combating cybercrime.

The second requirement: the extent of the possibility of restoring the adaptation of the traditional jurisdiction to the cyberspace

Monitoring the content and use of information published on the Internet highlights the difficulties surrounding the definition of the conditions for the application of the law, which have the character of escaping from the traditional way in which they are conceived, therefore, the question of the identification of the imperial state in an immaterial space, which is the Internet, which is born from the interactions generated by that network.

In principle, territory reflects the place of the state as a fundamental model for the concept of law, which sets conditions for the organization and functioning of society for its interests, and we will not return to examining this model in the era of "electronic borders" or the difficulties it raises in international law.

In the absence of a territorial or personal connection of a legal status to a state, the jurisdiction of a state may be based on its actual jurisdiction, which aims to protect its interests, whether they are the fundamental interests of the state or of the international community.

In this regard, Jan Kumbakka recalls that international law includes, in particular, crimes of endangering the external security of a State, including certain acts that constitute acts of disclosure of confidential information within the framework of national defense, violations of maritime or air security, as well as espionage activities. State intervention may also be based on the exercise of its universal jurisdiction, to prosecute perpetrators of international crimes of which terrorism is an element, and it should be recalled that terrorist acts constitute a threat to international peace and security, in accordance with Security Council Resolution 1373[2].

[1] -The principle of universal criminal jurisdiction is based on the need to protect the common interests of the international community, and when talking about universal criminal jurisdiction in international law, a distinction must be made between customary international law and treaty international law. In the field of customary international law, we find that states allowed the exercise of universal criminal jurisdiction in combating piracy crimes to protect the common interests of states. This principle was established as a customary rule on the occasion of the Lotus case in 1927 before the Permanent Court of International Justice, where the court made it clear that states have the freedom to extend their jurisdiction outside their territory. Universal criminal jurisdiction was established in treaty international law, in the 1948 Genocide Convention, the 1949 Geneva Conventions, and the 1984 Torture Convention, as this jurisdiction was stated in these conventions in a binding and not optional form, such as piracy crimes, on the other hand, this jurisdiction was included in the Statute of the International Criminal Court signed on July 17, 1998, where its preamble expresses this concept, through international solidarity, whereby the state bears responsibility for suppressing international crimes that affect common interests; See:

- Damien Vendermeersch, universal jurisdiction, national jurisdiction and international crimes, under the direction of Antonio Cassese and Mireille Delmas-Marty, University Press of France, No. 49-298, June, 2002, P 556.

[2]- French Society of International Law, op cit, p 401.

Under this resolution, States are not only authorized but also obliged to work to prevent and combat terrorist acts, and in particular they must complement international cooperation by taking additional measures to prevent and suppress all forms of crime committed on their territory by all legitimate means, in order to prevent the financing and preparation of any terrorist act, therefore, the link between the misuse of the Internet and the fight against terrorism justifies State intervention in monitoring activities and behaviors on the Internet, as well as the dependence of private actors on the measures adopted.

International agreements are considered the most important means in this field and work to unify international efforts to combat these crimes, and the United Nations, as a center for coordinating efforts between countries, works on this, and this is clearly evident through a number of international resolutions, recommendations, and agreements, including:

1- Havana Resolution 1991: Resulting from the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Prisoners, which established an international framework to combat computer crimes; and included the following(1):

- Emphasizing the establishment of an appropriate international legal framework, which requires a collective effort between countries.
- Requesting member states to take the following measures:
- Updating laws to keep pace with the stage, especially in the field of investigation, acceptance of evidence and judicial procedures.
- Improving security and prevention measures for computers, taking into account privacy and human rights.
- Raising public awareness by highlighting the importance of combating electronic crimes.
- Adopting special measures to train judges and judicial police to keep pace with the requirements of the stage.
- Increasing cooperation between relevant organizations, and establishing rules for ethics of dealing.

2- Holding the Fifteenth Congress of the International Association of Criminal Law in Brazil 1984: It formulated a set of principles that must be respected and observed in combating computer-related crimes (1), including:

- The necessity of identifying the authorities that conduct inspection and seizure in the information technology environment.
- Allowing public authorities to intercept communications within the computer system itself, with the evidence obtained being used in court.
- Taking into account issues of information structure, the loss of economic opportunities, the violation of privacy and privacy, as well as the cost of rebuilding the database, before any inspection or investigation.
- Reviewing the rules of electronic evidence and the credibility of evidence, taking into account legislative rules.

The second topic: Developing regional jurisdiction in cyberspace

The principle of territoriality has been known since ancient times, and is considered the origin in which jurisprudence and the judiciary found themselves in determining jurisdiction, and it focuses on the territory of the state, as the territory is the basis for the establishment of this principle.

First requirement: Qualifying and developing the principle of effects within the data of virtual reality

Article 22 of the European Convention on Cybercrime[1] confirms the principle of traditional territorial jurisdiction, in its text on a series of standards that the contracting states are obligated to impose their jurisdiction over criminal offenses committed via the Internet, as stipulated in Articles 2-11 of the Convention. Based on the principle of territoriality, each state is required to punish the perpetrator of the crimes stipulated in this agreement that were committed in its

[1]- See: Computer-related crime, Report of the European Committee on Criminological Problems, European Treaty Series No. 185, Budapest, 2001, p. 286.

territory, for example, the territorial jurisdiction of the state is confirmed if the criminal against the victim state's system is from within or outside its territory, and even if the aggressor is a resident of the victim state or outside its territory, if a person commits the crime of publishing harmful content such as pornographic material on the Internet, the state has the right to intervene to prosecute him if the crime occurred within its territory, and it also has the right to intervene if the effects of this crime occur within its territory.

We find that this principle is based on its provisions in the traditional effects theory, but the problem lies in achieving the connection and link between the act and the criminal result to implement this principle, as we find that the European Council of Ministers Committee confirmed the application of the effects approach in its commentary on Article 22 of the Convention, saying that: "The State should not assert its territorial jurisdiction if the crime occurs outside its computer system - outside its territory - while this jurisdiction is established for it if the attacker or the attack is from outside its territory".[1]

The problem in this case is that there will be no real connection between the criminal and the victim state, and the situation becomes more difficult when the harmful content is published on the Internet by an anonymous publisher. In this doctrine (effects), jurisdiction will be based on the bare fact, and this has been confirmed by many points of view in many judicial decisions of national courts, as the British Attorney General confirmed the jurisdiction of his courts to prosecute a French publisher who published obscene material, so that a police officer at Tobin Station in the City of London could access those pages, likewise, German courts convicted the Australian publisher of material about the Nazi Holocaust on the Australian Yahoo sites, and the French court decided that publishing Nazi memorabilia on an American service provider is punishable under French criminal law if no restrictions are placed, which means that the content of the World Wide Web must comply with the legal orders of more than 190 countries in the world, given the global nature of the Internet across borders, and even without any sufficient connection between the publisher and the publication on the web pages, and then prosecute the responsible party, and this point of view has gained wide popularity and acceptance from the courts, however, efforts are being made to limit the application of the doctrine of effects in one way or another by some governments, so that many restrictions have been imposed on the application of this principle in its entirety.

The United States courts have applied the effects doctrine with some wisdom, although its legal system considers that the practice is not uniform worldwide, and there is a strong tendency to use several criteria to determine the link and connection between a publication and its publisher and its relation to the jurisdiction of a particular country. These criteria include the language used in the publication, the worldwide reputation of the site, which may refer to a country, or any definitive indication that may indicate the domicile of the site, as in the case of the Federal Court of Tobin, which relied at least in its determination of jurisdiction on the fact that the affected country was the German state, although the practice of courts is not uniform worldwide, there is a strong tendency to use several criteria to determine whether a web page contains a sufficient link to a country.

The second requirement: The scope of the country's top-level domain (the virtual territorial boundaries of cyberspace)

The country's top-level domain and the domain name on the Internet have become a principle that is relied upon in international Internet law[2], in line with the traditional principle of territoriality within the natural environment[3], where it was understood that the Internet includes people who

[1]- Paris High Court (summary order) of May 22, 2000.at the link: https://www.cairn.info/revue-legicom-2000-1-page-220.htm

[2]-The Algerian top-level domain name is: Algerian Top-level domain, and the national top-level domain name of the People's Democratic Republic of Algeria is: dz

[3]-See Tariq Serour, Universal Criminal Jurisdiction, Arab Renaissance House, 1st ed., Cairo, Egypt, 2006, p. 44.

work or reside on a certain territory in a specific virtual space, which contradicts John Perry Barlow's declaration in 1996 about the independence of cyberspace, and what he used for the concept of sovereignty and social contract to assert that the Internet is a world outside the control of the state, and at the same time, states have become able to exercise some of their judicial and legislative powers in cyberspace, but what is even more striking than before is that large parts of cyberspace are now considered part of the state's territory. For example, the country code (the domain name) now refers to the state in cyberspace and is the private property of that state. Other countries, such as France, actually have control over their registries. In principle, the creation and delegation of TLDs is still the responsibility of ICANN, which is supported by the Governmental Advisory Committee(GAC), established under the national laws of the state of California, and ICANN is close in structure, organization and membership to an international organization[1].

In 2005, the Governmental Advisory Committee adopted the principles and guidelines for the management of CCTLDS (top-level domain names), as according to these principles, the general political authority over these domains is vested in the relevant government, thus, the sovereignty of the state over its own name has been confirmed in this way, as indicated by the final documents of the World Summit on the Information Society, which was held in two stages in Geneva 2003 and Tunis 2005, where paragraph 62 of the Tunis Programme of Action for the Information Society, issued on October 18, 2005, states the following:

States should not participate in decisions regarding the top-level domain names of another State, and the legitimate interests of States, as expressed and determined by the States concerned, should be respected, preserved and addressed, by various means, in decisions affecting their own top-level domain names, through improved and flexible frameworks and mechanisms that recognize the need to develop and strengthen cooperation among stakeholders to develop public policies regarding top-level domain names. Article 72 of the World Summit on the Information Society Declaration states: "We request the Secretary-General of the United Nations to convene in the second quarter of 2006 a new multi-stakeholder dialogue forum on public policy, to be called the Internet Governance Forum (IGF), in an open and inclusive process, with the mandate to discuss public policy issues relating to the key elements of Internet governance, to promote its sustainability, robustness, security, stability and development".

The project of September 30, 2005 went further and recognized that each government has sovereignty over the top-level domain code assigned to it, while all documents refer to the administration of state codes, and there is a real link between those domains and the state concerned, where the state may assert full jurisdiction over those domains in its own domain, because in those domains the state's territory is located in cyberspace, accordingly, the United Kingdom exercised its criminal jurisdiction over any crime committed in its virtual domain[2], and through this, cyberspace does not defeat the principle of territorial jurisdiction, but rather, it adapted to the special situation of the Internet, and it is known in jurisprudence that the rules of national criminal jurisdiction, external or internal, are related to public order, whether in the rules of international jurisdiction, personal or local, and that these rules are applicable before all criminal judicial authorities, whether ordinary, special or exceptional.

Conclusion

Engaging in the world of the Internet is inevitable to keep pace with human development and technological acceleration, in light of the important advantages that information technology provides in various fields, as it has brought new patterns of communication through this network and has gained great popularity, as it has forced the legislator to adapt its legislative texts

Also: Ahmed Sobhi Al Attar, The State's Authority to Prosecute Its Nationals for Crimes Committed Outside the State, The Lockerbie Case and the Future of the World Order, previous reference, p. 271 and following.

[1]- Bylaws For Internet Corporation For Assigned Names And Numbers | A Californianonprofit Public-Benefit Corporation, At The Link: https://www.icann.org/resources/pages/bylaws-2012-02-25-en Access date: May 13, 2024, at: 22:32.

[2]- Jean Christophe Martin, International rules relating to the fight against terrorism, work of CERIC, Bruylant, Paris, 2006, p43.

according to the requirements of cyberspace, and to introduce new terms and concepts to legal thought.

The world of the Internet, in addition to its advantages, has generated a new and dangerous phenomenon called cybercrime, which has been growing and increasing rapidly among countries, as the cybercriminal exists in a virtual world that knows no borders, with the difficulty of pursuing him and seizing evidence of conviction, as the only evidence to identify the perpetrator is the electronic address or digital evidence that he used. In parallel, other challenges appear on the horizon regarding determining judicial jurisdiction, as an attempt has been made to highlight the most important principles that govern it and to highlight the efforts made to keep pace with technological development with legislative development.

It seems that the problem of determining jurisdiction and the appropriateness of the applicable law remains in the field of cybercrimes, and determining jurisdiction and the applicable law remains subject to the principle of reciprocity, as any state that violates this principle makes the criminal immune from legal prosecution and immune from punishment and penalty.

RESOURCES AND REFERENCES:

1. Abd Allah Abd Elkarim Abd Allah, Cybercrimes and the Internet, a comparative study of the legal system to combat cybercrimes and the Internet with reference to the efforts to combat them locally, Arab and international, 1st ed., Al-Halabi Publications, Lebanon, 2007.
2. Computer-related crime, report of the European Committee on Crime Problems, European Treaty Series No. 185, Budapest, 2001.
3. Djamal Mahmoud Al-Kurdi, the competent court and the applicable law regarding claims of liability and compensation for harm caused by transboundary environmental pollution, 1st ed., Arab Renaissance House, Alexandria, 2004.
4. Tariq Serour, Universal Criminal Jurisdiction, Dar Al-Nahda Al-Arabiya, 1st ed., Cairo, Egypt, 2006.
5. -Ahmed Sobhi Al-Attar, The State's Authority to Prosecute Its Citizens for Crimes Committed Outside the State, Journal of Legal and Economic Sciences, Issue 02, Volume 34, 1993.
6. Société française de droit international,colloque de rouen,(internet et le droit international), éditions A.Pedone- Paris, 2014.
7. Manuel pour la coopération internationale en matière pénale contre le terrorisme, office des nation unies, centre la drogue et le crime, Vienne, 2009.
8. -Damien Vendermeersch, la compétence universelle, juridiction nationales et crimes internationaux, under the direction of Antonio Cassese and Mireille Delmas-Marty, University Press of France, No. 49-298, June, 2002.
9. Paris High Court (summary order) of May 22, 2000, at the link: https://www.cairn.info/revue-legicom-2000-1-page-220.htm
10. Bylaws for internet corporation for assigned names and numbers, a californianonprofit public-benefit corporation. at the link: https://www.icann.org/resources/pages/bylaws-2012-02-25-en Access date: May 13, 2024, at: 22:32.
11. Jean Christophe Martin, International rules relating to the fight against terrorism, work of CERIC, Bruylant, Paris, 2006.