

Guarantees and procedures for a fair trial in cyber crime between national legislation and international conventions

ضمانات وإجراءات المحاكمة العادلة في الجريمة المعلوماتية بين التشريعات الوطنية والاتفاقيات الدولية.

TAYEB SAKHRAOUI *

Faculty of Economic Sciences, Commercial Sciences and Management Sciences,
University of Algiers 03.
tayebsakhraoui@univ-alger3.dz

Date of send:05/11/2025 Date of acceptance:03/12/ 2025 Date of publication:30/12/2025

Abstract:

Summary: The concept of the right to a fair trial in cybercrime is considered one of the basic human rights, based on the availability of a set of constitutional and legal procedures by which the criminal case is conducted within the framework of protecting the person - especially in light of the contemporary digital environment - from anything that would affect or diminish his freedom, dignity and personal rights. It has been stipulated in most contemporary national legislations as well as international agreements with the aim of protecting the accused from all unlawful transgressions and enjoying all constitutional and legal guarantees before the start of the trial, during the trial and after the completion of its procedures.

Keywords: Guarantees and procedures, Fair trial, cyber crime , national legislation, international conventions.

* *Corresponding author*

Introduction

The dimensions of criminal policy in every place and time require the criminalization of certain acts that are harmful to the interests of society and the interests of individuals, and the imposition of penalties for them. It is inconceivable that society could experience stability, development, prosperity, and civilization outside the framework of criminalization and punishment. On the other hand, criminal justice necessitates viewing the accused as a human being with dignity, feelings, an individual, and a personality, entitled to a fair trial, regardless of the alleged act or their political, civil, or financial status. This fairness extends to all stages of the process, from investigation and inquiry to trial and the execution of the sentence.

Within the framework of national legislation and international human rights law and its relationship to criminal justice, the objective remains to ensure that individuals enjoy legal guarantees at all stages: pre-trial, trial, and post-trial. Therefore, the national penal legislation of any country must respect, incorporate, and take these standards into account. Hence, it can be said that a fair trial is one that respects the international standards stipulated in human rights law, as it serves as evidence of the soundness of a country's criminal justice system and the level of respect for human rights and fundamental freedoms. Conversely, the failure to apply these standards is evidence of the injustice of a country's criminal justice system and a flagrant violation of these rights. For human rights.

Despite the centrality of the term "cyber crime" in many academic studies addressing modern cyber threats, there is no universally agreed-upon definition of its nature, elements, and forms. However, in general, cybercrime can be defined as any crime in which the aforementioned electronic tools and technologies are used to launch a cyberattack primarily for financial gain.

The principles of a fair trial, as in ordinary crimes and especially cybercrime, require that suspects or even defendants be treated as innocent until a guilty verdict is issued against them by the competent judicial authority, after all evidence against them has been presented, and after they have been afforded all the guarantees to which they are legally entitled. It also requires that their case be presented before an independent and impartial court, that it be examined objectively, fairly, and expeditiously, that the verdict be reasoned, and that the accused be afforded the right to appeal.

This study aims to highlight the guarantees of a fair trial in cybercrime stipulated in Algerian law, particularly the new Code of Criminal Procedure 25/14 dated August 3, 2025, with those stipulated in the laws of countries and international agreements whose systems are based on the protection of freedoms and human rights, and to highlight the similarities and differences between the laws of these countries on the one hand, and Algerian law on the other. This leads us to examine the extent to which the guarantees stipulated in the national law are provided, what prevents the application of these guarantees in reality, and to develop solutions to overcome them.

Based on the above, we pose the following question :What are the most important basic guarantees for a fair trial in cybercrime, and to what extent has Algerian criminal legislation guaranteed fair trial guarantees for the accused in accordance with what is included in the relevant international conventions?

Firstly. The basic guarantees of a fair trial in cyber crime under national law.

The Algerian legislator has guaranteed numerous safeguards for the accused before, during, and after trial, in order to protect their fundamental rights and freedoms and to ensure a fair trial that meets all legally stipulated requirements. Among the most prominent of these safeguards are the expedited referral of the accused to the court, their trial before a competent, independent, and impartial tribunal, and the issuance of a just verdict in accordance with the law, which guarantees human rights and freedoms, while also ensuring the accused's right to defense, a fundamental requirement of a fair trial¹.

A fair trial in cybercrime and the contemporary digital environment is based on a set of procedures that govern criminal proceedings within the context of protecting personal freedoms in the digital space, as well as other human rights, dignity, and the integrity of the individual. Most countries have worked to enshrine this principle in their legal systems to guarantee a fair trial for the accused. These guarantees are included in their constitutions and criminal procedure laws. Algeria is among these countries, and it has been keen to enshrine these principles and establish guarantees for them.²

There are a number of binding international agreements, whether treaties, customary law, or general principles of law, that have become ingrained in human conscience and include standards, criteria, and elements to guarantee a fair trial.

Cyber crime is defined, based on the Arab Convention, the US Crimes Act, the Budapest Convention, and the International Telecommunication Union, as: "Any felony or misdemeanor committed against an individual or group with criminal intent and the aim of harming the victim's reputation, body, intellect, property, or life,³ whether directly or indirectly, using modern communication technologies such as the internet." This definition is further reinforced by increasing globalization in a society transitioning from a traditional social system to a more open, advanced, and rapidly integrated one, both with the outside world and local communities. This integration is facilitated by readily available and permissible social media technologies, operating with complete freedom and without clear restrictions, controls, or laws defining the scope of penalties for violations of privacy, rights, or freedoms Massa argues that cybercrime refers to "illegal attacks committed using information technology for profit." However, cybercrime is often committed not for profit, but for psychological gratification, revenge, mockery of competitors, or other motives⁴.

1. Legal safeguards for a fair trial in the digital environment:

The human right to a fair and impartial trial necessitates certain guarantees that serve as a protective shield for judicial and procedural matters, particularly in

cybercrime. These guarantees include the right to equality before the law, the right to appear before a competent judge, the right to protect one's procedural status by preventing the retroactive application of procedural laws, and the right to be informed of the proceedings (the principle of adversarial proceedings), which ultimately lead to achieving the desired outcome⁵.

The right to a fair trial encompasses a set of procedural guarantees that ensure a balance between the parties to a dispute regarding their procedural rights and obligations, regardless of the nature of the case. The essence of this balance lies in ensuring equal treatment by the judiciary and providing them with opportunities to defend their interests in a manner that guarantees equality before a public trial before a competent, independent, and impartial court established according to the law.⁶

From the perspective of Algerian legislation, Article 2(a) of the rules relating to crimes related to information and communication technologies defines a cybercrime as: "Any crime committed or facilitated through an information system or an electronic communication system."⁷ Therefore, the concept of cybercrime is inextricably linked to information systems. Cybercrime can only be committed through information systems, which are the sole gateway (the information system) present in all computers and through which they connect to the global communication network.

The information that constitutes the basis of a cybercrime is defined in Article 2, paragraph (c) of Law No. 09-04 of August 5, 2009, concerning the prevention and combating of crimes related to information and communication technologies, as: "Any process of presenting facts, information, or concepts in a form ready for processing within an information system, including the programs that enable the information system to perform its function."

Article 144 includes a fundamental guarantee, considered one of the most important guarantees of a fair trial. The constitutional legislator stipulated that judicial rulings must be reasoned and pronounced in open court. This is because public proceedings are a fundamental guarantee of the judge's impartiality and freedom from bias and influence. Furthermore, it fosters trust and confidence in the judge's rulings, a principle enshrined in Article 10 of the Universal Declaration of Human Rights.

Articles 148 and 149 stipulate that the judge is bound only by legal and legislative texts when issuing rulings and is protected from all forms of pressure and interference that could compromise the integrity of the judgments.

Article 150 states that the law protects litigants from any arbitrary actions by the judge. Article 151 guarantees the right to defense in all criminal cases. In this, the constitutional drafters aligned themselves with all international declarations and conventions that consider the right to defense one of the most important human rights and a fundamental guarantee of a fair trial.

These guarantees are what characterize a trial as fair, as they ensure, in their entirety, a concept of justice that generally aligns with contemporary standards

applied in the most developed legal systems in terms of preserving human dignity and protecting fundamental rights during litigation.⁶ The most important legal guarantees can be summarized as follows:

1/ Judicial Independence and Judge Impartiality: Judicial independence is a key guarantee for achieving justice in society and a fundamental safeguard for protecting human rights. Without an independent judiciary, citizens' rights and freedoms become vulnerable to violation and infringement, whether by the executive or legislative branches, or by those wielding influence within the government.⁸

Judicial independence is a key element in achieving a fair trial in cybercrimes, and it is one of the essential guarantees that contribute to that goal, as evidenced by the fact that the right of the accused to a fair trial cannot be truly realized in the digital environment and its complex problems except with the existence of a competent, impartial court that relies on judges who cannot be subject to suspicion, accusation, or lack of integrity, as they rely in their work on impartiality and independence.⁹

2/ Equality between litigants: Equality before the judiciary is one of the manifestations of equality before the law, and it entails that all defendants have the same rights within the scope of the substantive and procedural rules in force in combating cybercrime. The restrictions placed on the freedom of the Public Prosecution in initiating criminal proceedings, such as cases of complaint, request, and authorization, or the variation in imposing the penalty, do not violate the principle of equality, as the assessment of the penalty must differ according to the personal circumstances of each offender. Based on this principle, the Egyptian Constitution established several principles to achieve equality before the judiciary, which are that the right to litigation is guaranteed for all, bringing the judiciary closer to litigants, expediting the resolution of cases, preventing the legislative and executive authorities from immunizing their actions from judicial oversight, in addition to free access to the judiciary.¹⁰

3 / The Presumption of Innocence: It is an established principle that every human being is born innocent, and this presumption remains with them throughout their life. It is only negated by a final judicial ruling that convicts them of conduct deemed a crime by law. Therefore, one of the requirements of this principle is that if a crime is attributed to a person, the prosecution must provide evidence of it. Conviction is only established if the evidence is so compelling that it fully convinces the judge beyond any doubt¹¹.

The principle of the presumption of innocence rests on a legal assumption consistent with the fundamental nature of things. Thus, the presumption of the accused's innocence until proven guilty is a condition that accompanies the accused throughout all stages of the criminal proceedings and is reflected in the rules governing their treatment at all these stages. Consequently, it leaves its mark on all rules of criminal procedure, although this effect appears most significant during the trial phase.¹²

2. Procedural safeguards for a fair trial in the digital environment:

The concept of the right to a fair trial in the contemporary digital space, from a procedural point of view, is one of the most important pillars of ensuring the enjoyment of human rights, which has been emphasized in most constitutions, charters, and international declarations related to human rights and personal human freedoms. This is because the practical application and actual practice of investigation, inquiry, and trial in cybercrime, from a practical point of view, is more important than the existence of the text. Therefore, exercising this right requires providing several procedural guarantees related to the trial, which we will focus on in detail through this requirement.

1/ Rules of Attendance and Public Proceedings in Electronic Trials: The competent judicial authority for the trial of the crime has a duty to enable the parties to attend its proceedings and allow them access to its documents, so that the rules of attendance and access are considered among the applications of publicity in the case of the accused, and the court hears the case publicly so that the proceedings are bound by the rules of justice.¹³

The concept of the right to a fair trial, with its inherent sensitivity and complexity, necessitates providing the accused with all the necessary guarantees to enable them to exercise this right. This concept, in turn, requires a plurality of rules. No single constitutional or legal system can enshrine all the guarantees of a fair trial. Rather, the rules of a fair trial have an external basis and source, guaranteed by the Universal Declaration of Human Rights and elaborated upon in the International Covenant on Civil and Political Rights, and enshrined in numerous regional agreements, including American, European, African, and Arab conventions¹⁴.

These rules are further supported by external sources, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and numerous regional agreements, including those of the United States, Europe, Africa, and the Arab world. Article 285 of the Code of Criminal Procedure stipulates the principle of public hearings for the Criminal Court, and Articles 342 and 430 of the Code of Criminal Procedure stipulate the principle of public hearings for the Misdemeanor Court and the Criminal Chamber. Public hearings mean opening the opportunity for all people to attend the trial, except that the court may decide to hold a closed session if public order and morals so require, provided that the litigants and their representatives attend. Articles 461 and 463 of the Code of Criminal Procedure also stipulate an exception to the principle of public hearings, relating to the confidentiality of pleadings before the juvenile courts.¹⁵

2/ Expeditious Proceedings: The virtual environment of cybercrime, especially given the presumption of innocence and the obligation to treat the accused before investigating bodies and the presiding judge accordingly, necessitates a swift trial. The principles of a fair trial demand the expeditious prosecution of those presumed innocent, so that their innocence is either proven or they are convicted. Delay in the trial of a person accused of a cybercrime, followed by their eventual acquittal,

constitutes a form of injustice perpetrated by an entity that is supposed to uphold justice.¹⁶

3/ Oral Proceedings and the Right to Defense: The principles of a fair trial in cybercrime cases require that proceedings, as we have seen, be conducted publicly in the presence of the litigants and others, and that arguments be presented orally. This necessitates confronting the accused with the facts and actions attributed to them in the digital environment, allowing them to exercise their right to respond, clarify, and defend themselves, thus lending greater legitimacy to the judicial ruling.

Accordingly, a judge may not base his ruling solely on preliminary investigation reports obtained from electronic devices or on any evidence presented outside the session. Rather, he must base his ruling on the investigations, discussions, and oral arguments that took place before him in the session and in the presence of the opposing parties.¹⁷

Evidence refers to the means a judge uses to arrive at the truth he seeks. In this context, truth encompasses everything related to the procedures and facts presented to him for the application of the law. Evidence also refers to any action taken in or aimed at a legal proceeding, regardless of its form or meaning, through which the legislator aims to reach the truth. It must be a legitimate means of proof whose purpose is to identify the perpetrator of the crime. Furthermore, evidence is the legitimate means obtained through lawful methods for presenting it to the judge to establish certainty and enable him to rule accordingly.¹⁸

4/ Reasoning for the Judgment: Reasoning for judgments refers to the body of factual evidence and legal arguments upon which the court based its conviction regarding the solution contained in its judgment, as well as a reference to the legal texts that gave rise to the dispute. Before the judge states the operative part of the judgment, he must first list the reasons and evidence that led him to be convinced of the content of this judgment over others. This must be based on established evidence in the case file, and he must cite the legal texts that he applied to the dispute before him.¹⁹

Secondly. International standards for fair trials in cyber crimes

Recognizing the difficulty of obtaining and seizing evidence of cybercrimes using traditional methods, the Budapest Convention on Cybercrime, signed on November 23, 2001, included two sets of new procedures: preliminary procedures for gathering evidence and procedures for gathering evidence itself.

Preliminary procedures for gathering evidence: These are a type of monitoring and surveillance of the use of communication technology (computers and the internet). These procedures are carried out by computer and internet service providers, commissioned by the competent authority. Initiating these procedures does not constitute initiating legal proceedings. Preliminary procedures are divided into two types:

The first type: Rapid data preservation procedures. This type consists of two things: First, issuing orders to service providers, whether individuals or companies, to preserve data stored in computer systems and the internet for a specific period²⁰.

Second, enabling the competent investigative authority to determine the content of data sent or received by the subscriber, whether through service providers or through the results of an inspection. The second type of procedure for gathering evidence is rapid data preservation procedures related to data flow. This aims to obligate service providers, whether individuals or companies, to preserve stored data and information, including the time of transmission, the time of reception, and the person who transmitted it. This helps identify the perpetrator of the cybercrime and those who contributed to its commission. Some legislators have responded to the provisions of the Budapest Convention in Article 17(1) and (2).²¹

1. The concept of a fair trial in international law:

The concept and nature of a fair trial, as indicated by international texts, particularly the Budapest Convention on Combating Cyber crime, is a trial that includes respect for procedures during the application of laws and is surrounded by a number of guarantees that would make the trial fair, such as the public nature of the trial, equality between the parties in the case, and other guarantees. The importance of a fair trial lies in the fact that it is related to one of the most important issues in the current century at both the international and national levels, as it is related to the judicial authority and shows the extent of its integrity and impartiality.³² The right to a fair trial is one of the most important human rights, and the protection of human rights constitutes the basic basis on which freedom, justice, and peace are based. A state that cares about human rights is a state that strives for progress, democracy, and the rule of law.

1/ Definition of a fair trial in the Budapest Convention:

Simply obtaining and presenting digital evidence to the court is insufficient for its admissibility as evidence of guilt. The inherent technical nature of digital evidence makes it susceptible to manipulation that distorts the truth, often without the discernment of a non-expert. Furthermore, the margin of error in obtaining credible evidence is high with this type of evidence, thus raising doubts about its reliability as evidence in criminal proceedings.

If international human rights law (the set of international conventions, customs and principles) is the source on which you rely to measure and evaluate the fairness or unfairness of criminal justice in terms of its compliance with international standards, then defining the conditions of a fair trial as a concept remains a necessary matter.

Therefore, for a criminal trial for cybercrime to be fair (from an international perspective), two essential conditions must be met:

First, the trial proceedings must adhere to international standards, whether they are treaty-based, customary, or general principles of law pertaining to international human rights law.

Second, the criminal trial and the implementation of international conventions must be conducted by a judicial body that is independent, impartial, and legally authorized to carry out the trial.²²

Evidence-gathering procedures include, most importantly:

First – Issuing an order to provide specific data: This means that the authorized authority issues an order to the service provider or any person in possession of or under their control to provide specific data, whether this data relates to content or route²³.

Second – Searching and seizing stored data: This means searching for and seizing data stored in a computer information system or on an information storage medium, whether this data is stored on a single device or in a communications system.²⁴

By examining the relevant texts of international law, Article 10 of the Universal Declaration of Human Rights (1948) and Article 14 (paragraph 1) of the International Covenant on Civil and Political Rights (1966) shed light on defining and defining the elements of a fair trial under international human rights law.

Article 10 of the Universal Declaration of Human Rights states: “Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him”.

Article 14(1) of the aforementioned International Covenant states: “Everyone is entitled to a fair and public hearing by a competent and impartial tribunal established by law.” From these two articles, we observe that a fair trial under international human rights law must be independent, impartial, and established by law. This pertains to the substantive elements. As for the procedural aspects, the trial must be public and non-discriminatory.

2/ International standards of a treaty nature:

The concept of a fair trial differs from that of criminal justice. Since the focus here is on international standards for a fair trial, rather than international standards for criminal justice in the broader sense, international standards that are treaty-based are divided into global (treaty-based) standards and regional standards. We will address this further below: First, global (treaty-based) standards. Among the most important international agreements to which Algeria is a party are the following:

.1The International Covenant on Civil and Political Rights 1966

.2The Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment 1984.

.3The Convention on the Elimination of All Forms of Discrimination against Women 1981

.4The four Geneva Conventions relating to armed conflict (1949) and their two Additional Protocols.

4. The International Convention on the Elimination of All Forms of Racial Discrimination (1966).

Precautionary measures: These aim to preserve stored data deemed important by the competent authority for the investigation by keeping it in its designated location within the computer information system or on the storage medium, and preventing access to, deletion of, or disposal of it.

Security measures: These are procedures that follow inspection and entry, and refer to the collection of data, whether by taking the information storage medium itself or by making a copy of the data stored on it or in the computer information system on paper or disks.

/3Regional International Standards: Among the sources of international standards of a treaty nature are regional treaties that do not have universality but rather a specific regional framework, such as those contained in the European Convention on Human Rights, the African Charter on Human and Peoples' Rights, or the Convention on the Rights of the Peoples of America.

In the interest of time and the focus of the symposium, we will concentrate on the 1981 African Charter on Human and Peoples' Rights, to which Algeria is a party.²⁵

This Charter is a regional international treaty that stipulates guarantees of a fair trial within the framework of the human right to litigation and the right to a fair trial.

Therefore, the Charter established an African Commission on Human and Peoples' Rights to monitor its implementation, receive complaints from concerned individuals, and oversee its implementation, including the guarantee of a fair trial, through the States Parties. A significant development on the African continent was the establishment of the African Court on Human and Peoples' Rights by virtue of an Optional Protocol in 1998, to which Algeria is a party. This Court represents a complementary and important victory for the effectiveness of the African human rights system.²⁶

2. Guarantees of a fair trial for cybercrime in international law:

Article 1 of the Universal Declaration of Human Rights states: "All human beings are born free and equal in dignity and rights...". Article 7 states: "All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination." These two texts make it clear that equality among people is a fundamental principle at the global level that must prevail in all legal systems of states that have adopted this Universal Declaration. These states, in accordance with their international obligations, must strive to embody this principle within their judicial laws and procedural legislation, making it a dominant principle in all legal regulations pertaining to fundamental human rights and freedoms, including the right to a fair trial whenever a criminal

charge is brought against an individual or any dispute concerning their civil rights is resolved²⁷.

The International Covenant on Civil and Political Rights stipulates in Article 14, paragraph 1, that "All persons are equal before the courts and tribunals..." Paragraph 3 of the same article stipulates that everyone, in the consideration of any criminal charge against them, is entitled to a minimum of guarantees on a basis of full equality.

The principle of equality appears as a guarantee of a fair trial in that the parties to the criminal dispute enjoy the same rights and freedoms. Each party must have a reasonable opportunity to present his claims and defenses in circumstances that do not put him in a weak position compared to his opponent. Whenever one of them is deprived of these rights and freedoms while another enjoys them, the trial lacks equality between the parties, which is an integral part of the guarantees of a fair trial.²⁸

The legality of evidence is considered one of the most important recommendations of the 15th International Congress of the International Association of Penal Law, held in the Brazilian capital from September 4-9, 1994, within the framework of criminal procedure reform. Recommendation No. (18) states: "All evidence obtained through the violation of a fundamental right of the accused, and any evidence resulting from such violation, is inadmissible and cannot be relied upon or considered." The Congress also emphasized the necessity of respecting the principle of legality when seeking evidence in computer crimes and traditional crimes within the information technology environment; otherwise, the procedure is invalid, and the public official who violated the law is held accountable.²⁹

/1Guidelines on the Role of Prosecutors (1990): These guidelines were unanimously adopted at the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in 1990. A key principle is the need to ensure that prosecutors in criminal cases are characterized by competence, integrity, and diligence, and to promote these qualities. This is a crucial standard for a fair trial.

Guarantees for the Protection of the Rights of Persons Facing the Death Penalty (1984): These guarantees were adopted by the United Nations Economic and Social Council and endorsed by the United Nations General Assembly in a resolution of 1984. The most important aspect of these guarantees, concerning international standards for a fair trial, is that "the death penalty shall not be carried out except after a trial in which the accused is afforded all possible judicial guarantees that ensure a fair trial." At a minimum, these guarantees must include "those judicial guarantees set forth in Article 14 of the International Covenant on Civil and Political Rights of 1966," including the right of a person accused of a crime punishable by death to "adequate judicial and legal assistance at all stages of the proceedings."

These non-treaty-based standards, which pertain to a fair trial as a human right, are binding not by form but by substance, as they undoubtedly form part of customary international law and the general principles of law. Therefore, they are

binding under Article 38 of the Statute of the International Court of Justice concerning the sources of international law. The most important of these principles are as follows:³⁰

This means that evidence obtained from computer and internet crimes, whether printed, displayed on a computer screen, stored on data carriers, or in the form of magnetic or optical tapes, disks, or microfilms, will all be subject to discussion when used as evidence before the criminal court. Therefore, all evidence obtained through the information technology environment must be presented in court, not merely as part of the case file during the preliminary investigation, but directly before the judge. These provisions apply to all evidence generated by digital devices. Furthermore, witnesses to cybercrimes who have already given statements during the preliminary investigation must repeat their testimonies before the court. Similarly, information systems experts, regardless of their specialization, must appear before the courts to discuss their findings and reports, in order to reveal the truth and uncover the facts.³¹

Therefore, it can be said that legal protection extends to cover the presumption of innocence even outside the scope of judicial proceedings. Violating the presumption of innocence through publication or media in any publicly available medium is considered a crime punishable by law according to the provisions on defamation and slander, as applicable.

Applying the principle of legality: For an offense involving defamation or slander, a tortious act warrants compensation. A fair criminal trial requires adherence to the principle of legality (no crime or punishment except by law) and the principle of non-retroactivity of criminal law, as well as the application of the most lenient punishment for the accused. This standard, or element related to the principle of legality and non-retroactivity of criminal law, was clearly emphasized in the International Covenant on Civil and Political Rights of 1966 as a treaty source and is considered one of the core, inviolable rights under Article 2, Paragraph 4. It was also previously considered one of the fundamental pillars of human rights in the Universal Declaration of Human Rights. A court that does not observe this element and this standard can be described as unjust under international law.³²

Public prosecutors are responsible for applying the law in criminal cases, protecting the rights of those involved in criminal proceedings, respecting human dignity and fundamental rights, and ensuring public safety. In many countries, public prosecutors play a crucial role in implementing and defining criminal policy through the use of their discretionary powers, including adapting to social and societal changes. In some countries, public prosecutors are also responsible for civil proceedings to ensure the protection of rights and freedoms and the interests of juveniles, the elderly, persons with disabilities, or those unable to take necessary actions due to their health condition.³³

Conclusion:

The subject of cybercrime is of great importance, not only for the sake of academic study and information, but its importance is highlighted in the search for a

cure and putting an end to these crimes, the proof of which almost constitutes an obstacle for specialists from the judicial police, investigation and inquiry bodies, defense bodies and ruling authorities, due to the infiltrations of these crimes, which are difficult to reach their professionals.

Therefore, it has become necessary to search for an effective criminal policy, high scientific and technical training, data updates, information storage in secure places, and to provide everything that makes data immune to fraud and manipulation. This can be achieved by updating legal systems, deterring perpetrators of crimes, opening university specializations for outstanding and intelligent students to keep pace with digital modernization, and sending them on training missions to countries active in the field of digital technology. In addition, it is necessary to raise awareness in society about the danger that surrounds it as a result of malicious use by unscrupulous individuals in infiltrating personal privacy.

The international agreements and national legislation related to combating cybercrime, referenced in this study, are important sources for defining the legal framework of the concept, nature, and guarantees of a fair trial at the national and international levels, as they represent the will of all members of the United Nations General Assembly. However, many countries have failed to implement their obligations under the agreements they have signed and have not incorporated them into their national laws.

Through studying and analyzing international texts and national legislation related to cybercrimes, we conclude that it is important to embody and enshrine the guarantees of a fair trial in the digital environment. We find that these conventions have stipulated either this right itself or emphasized its standards and the rights that guarantee the establishment of the foundations of an effective modern criminal justice system, and thus enjoyment of fair trials, especially in light of rapid technological developments. We mention the most important international conventions that stipulated or referred to this right or one of its elements, which will be the basis of the study in this memorandum. Among the international conventions, we mention: "The Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights," and the Budapest Convention. As for the regional conventions, we mention: "The European Convention on Human Rights, the American Convention on Human Rights, as well as the African Charter on Human and Peoples' Rights, and the Charter of Human and Peoples' Rights in the Arab World."

Margins:

1 - Amar Boudiaf, Fair Trial in the Islamic Criminal System and International Conventions, an article published online, accessed 10/08/2022. 4shared.search.com.

2- Ahmed Fathi Sorour, Constitutional Legitimacy and Human Rights in Criminal Procedures, Dar Al Nahda Al Arabiya, Cairo, 1993, p. 3.

3 -Iman Fadel Al-Samarrai, Haitham Muhammad Al-Zaghbi, Management Information Systems, First Edition, Dar Safaa for Publishing and Distribution. Amman 2005. p. 259.

4- Mahmoud Ahmed Mohammed Al-Quraan, Cybercrimes, First Edition, Dar Wael for Publishing and Distribution, Jordan, 2017, p. 47.

- 5- Mahmoud Mustafa Younis, Procedural Protection of Human Rights in Judicial Law (A Comparative Jurisprudential and Fundamental Study), 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, 2003, p. 13
- 6 - Sami Hosni Al-Husseini, "Guarantees of Defense", Journal of Law and Sharia, Kuwait University, Vol. 2, No. 1, 1978, p. 22.
- 7 -Law No. 09-04 dated 14 Sha'ban 1430 corresponding to 05 August 2009, containing the special rules for the prevention and combating of crimes related to information and communication technologies, Official Gazette No. 47 dated 16 August 2009.
- 8- Nasreen Abdel Hamid Nabih, The Rights of the Accused Before the Judiciary, First Edition, Al-Wafaa Legal Library, Alexandria, 2010, p. 10.
- 9- Omar Fakhri Abdul-Randizaq Al-Hadithi, "The Right of the Accused to a Fair Trial," a comparative study, Master's thesis, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 2005, p. 98.
- 10 -Hassan Bashit Khwein, Guarantees of the Accused in Criminal Cases During the Trial Stage. Dar Al-Thaqafa for Publishing and Distribution, Amman, 1997, p. 65.
- 11 - Hatem Bakkar, Protecting the Right of the Accused to a Fair Trial, PhD Thesis, Faculty of Law, Alexandria University, 1996, p. 58.
- 12 - Kamal Abdel Wahed Al-Gohary, Establishing Judicial Conviction and Fair Criminal Trial, Dar Mahmoud for Publishing and Distribution, Cairo, 1999, p. 30.
- 13- Hassan Hammad Hamid Al-Hammad, "Publicity in the Law of Criminal Procedures," a comparative study, Al-Halabi Publications, no edition, 2012, p. 101.
- 14- Essam Afifi Abdel Basir, The Principle of Criminal Legality in Positive Law and Islamic Jurisprudence, Dar Al Nahda, Cairo, 2007, p. 120.
- 15- Amr Wasel Sharif, Pretrial Detention, Al-Halabi Publications, Beirut, Second Edition, 2010, p. 06.
- 16- Abdel Ghani Bassiouni Abdullah, Equality before the Judiciary and Guaranteeing the Right to Litigation, 2nd ed., Dar Al-Nahda Al-Arabiya, Cairo, 2001, p. 25.
- 17 -Jurisprudence of Criminal Justice, Publications of the Journal of Legal Sciences, Issue Two, Al-Amniya Press, Rabat, 2019. Prospects of Criminal Justice in Light of the Constitutionalization of the Principle of Criminal Legality, pp. 36-37.
- 18 - Mohammed Obaid Saeed Saif, The Legality of Evidence in the Criminal and Disciplinary Fields, A Comparative Study, Page 136.
- 19 - Raouf Obeid, Rules for Justifying Criminal Judgments and Orders for Disposition in Investigations, Third Edition, Dar Al-Fikr Al-Arabi, Cairo, 1986, p. 3.
- 20- Article 16 of the Budapest Convention.
- 21- Article 17 of the Budapest Convention.
- 22 -Abdel Nasser Abu Zeid, Human Rights in Egypt Between Law and Reality, Dar Al Nahda Al Arabiya, Cairo, 2006, p. 110.
- 23- Article 18 of the Budapest Convention.
- 24 - Article 19 of the Budapest Convention.
- 25- Hilali Abdellah Ahmed, The Budapest Convention on Cybercrime (with commentary), Dar Al Nahda Al Arabiya, First Edition, Cairo, 2007. p. 89.
- 26- Younes El Ayachi, "The Fair Trial Between Theory and Practice in Light of International Conventions, Treaties and Judicial Practice," Dar Al Salam Library for Printing, Publishing and Distribution, Rabat, End of Training Research for Judicial Attachés, 2012, p. 18.
- 27- A Fair Trial Guide, published by Amnesty International, www.amensty-arabic.org
- 28- Salvator zappala.la justice pénale internationale.montchrestien. : paris.2007. P124.

-
- 29- Hassan Taher Daoud, Information Systems Crimes, Naif Arab Academy for Security Sciences, First Edition, Riyadh, 2000, p. 145.
- 30- Pierre Marie Dupuy, Droit International Dalloz, Paris, 1998,P204.
- 31- Mohammed Al-Amin Al-Bashari, Digital Forensic Evidence, Its Concept and Role in Proof, Arab Journal of Security Studies and Training, Volume 17, Issue 33, Year 17, Riyadh 2002, p. 74.
- 32- Bahnos Amal, Digital Evidence in Criminal Procedures, Academic Journal of Legal Research, Volume 16, Issue 02, 2017, p. 186.
- 33- It was adopted by the General Assembly and opened for signature, ratification and accession in resolution 39/46 of 10 December 1984