How to Cite:
Abdallah, M., & Abdallah, A. Y. (2025). The international legal frameworks to combat cybercrime in the era of artificial intelligence. *International Journal of Economic Perspectives*, *19*(5), 2534–2548. Retrieved from https://ijeponline.org/index.php/journal/article/view/1074

The international legal frameworks to combat cybercrime in the era of artificial intelligence

Dr. Mekhaneg Abdallah
Faculty of Law and Political Sciences, Legal System Laboratory for Contracts and Transactions in Private Law, University of Djilali Bouanaama Khemis Miliana - Algeria
Email: a.mekhaneg@univ-dbkm.dz

Dr. Amar Youcef Abdallah
Faculty of Economic, Business and Management, Legal System Laboratory for Contracts and Transactions in Private Law, University of Djilali Bouanaama Khemis Miliana - Algeria
Email: a.amar-youcef@univ-dbkm.dz

***Abstract*---**In the era of Artificial Intelligence, cybercrime has emerged as a new phenomenon, and has spread at a speed that exceeds the imaginations. It has crystallized as a result of the unprecedented scientific leap that has made a difference in the field of Information and Communication Technology, and has reduced the distances between people. This crime is still a source of widespread threats that damage personal data destabilize societies. This new crime has various forms, and its consequences are difficult to accurately determine, which requires the international legal system to be adapted to these complexities. Face to the repeated electronic piracy attacks, it has become necessary for the International Community, more than ever, to rely on international legal frameworks in light of the comprehensive approach, through International Conventions on combating transnational crimes. This involves an attempt to reduce the scale and repercussions of these crimes and ensure the security of cyberspace, while respecting the standards of international law. In regard of the current challenges, combating cybercrime requires all international actors to adopt effective strategies that take into account the respect for the principle of sovereignty, the protection of the rights and freedoms of individuals, and at the same time preserving the National Security of States.

***Keywords*---**Artificial Intelligence, cybercrime, legal frameworks, International Conventions, National Security.

Corresponding author: *Abdallah, M., Email: a.mekhaneg@univ-dbkm.dz*
Submitted: 10 November 2024, Revised: 27 April 2025, Accepted: 28 May 2025

Introduction

Artificial intelligence, or AI, is a field of study aimed at the reproduction of the cognitive faculties of human intelligence with the objective of creating systems or machines capable of performing functions normally related to it. The advent of the digital era brings as many advantages as disadvantages effects. In an increasingly connected world, it is essential for states to be able to protect themselves against AI threats. Artificial intelligence constitutes a double-edged sword that can be used both by governments and companies to protect their platforms and by cybercriminals to carry out attacks. It has undoubtedly transformed various aspects of our lives for good. Whether it's content writing assistance, movie recommendations, or voice-activated digital assistants to make our lives easier. However, this technological marvel enables malicious persons to launch sophisticated and devastating cyber-attacks. The AI revolution in cyber-attacks is reshaping the cybersecurity landscape and posing new challenges for individuals, businesses and national security of States.

The research question is:
What are the legal frameworks to combat cybercrimes in International Conventions in the era of Artificial Intelligence?
This article will explain more about how AI will change the landscape of cybersecurity in the words and examine the International Legal Instruments to fight against cyber criminality.

1. The Budapest Convection on Cybercrime and its Protocols

The Budapest Convention is more than a legal document; it is a framework that allows hundreds of practitioners from the Parties to share their experience and create relationships that facilitate cooperation in specific cases, including in emergency situations, beyond the specific provisions provided for in this Convention.

1.1. The Budapest Convention on Cybercrime of 2001

The States parties recognizing the benefit of intensifying cooperation; convinced of the need to pursue, as a matter of priority, a common criminal policy intended to protect society from crime in cyberspace, in particular through the adoption of appropriate legislation and the improvement of international cooperation. They are also concerned by the risk that computer networks and electronic information may also be used to commit criminal offenses and that evidence of such offenses may be stored and transmitted through these networks; and believing that a well-conducted fight against cybercrime requires increased, rapid and effective international cooperation in criminal matters; to prevent acts affecting the confidentiality, integrity and availability of computer systems, networks and data, as well as fraudulent use of such systems, in ensuring the criminalization of these behaviours, as well as the adoption of sufficient powers to enable an effective fight against these criminal offenses, by facilitating their detection, investigation and prosecution, both at national and international by providing provisions for rapid and reliable international cooperation[1].

[1] Preamble to the Budapest Convention on Cybercrime of 2001.

Each Party shall adopt such legislative and other measures as may be necessary to criminalize, in accordance with its domestic law, intentional and unauthorized access to all or part of a computer system. A Party may require that the offense be committed in violation of security measures, with the intent to obtain computer data or other criminal intent, or in connection with a computer system connected to another computer system[2].

Each Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offense, in accordance with its domestic law, the intentional and unauthorized interception, carried out by technical means, of computer data, during non-public transmissions to from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offense be committed with criminal intent or be in relation to a computer system connected to another computer system[3].Each Party shall adopt such legislative and other measures as necessary to establish a criminal offense, in accordance with its domestic law, the intentional and unlawful act of damaging, erasing, deteriorating, altering or deleting computer data[4].

Each Party shall adopt the legislative and other necessary measures to establish a criminal offence, in accordance with its domestic law, the intentional and unauthorized alteration, erasure or deletion of computer data, generating non-data , taken into account or used for legal purposes as they were authentic, whether or not they are directly legible and intelligible[5].

Each Party adopts the legislative and other measures which prove necessary to establish as a criminal offence, in accordance with its domestic law, the intentional and unauthorized act of causing financial damage to others by any introduction, alteration, erasure or deletion of computer data; or by any form of attack on the functioning of a computer system, with the fraudulent or criminal intention of unlawfully obtaining an economic benefit for oneself or for others[6].

Each Party shall adopt the legislative and other measures which prove necessary to establish as a criminal offence, in accordance with its domestic law, infringements of intellectual property, defined by the legislation of that Party, in accordance with the obligations that the latter has subscribed to in application of the Paris Act of July 24, 1971 revising the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Commercial Aspects of Intellectual Property Rights and the WIPO Treaty on the intellectual property, with the exception of any moral rights conferred by these conventions, when such acts are committed deliberately, on a commercial scale and by means of a computer system[7].

---

[2] Art 2 of the Budapest Convention on Cybercrime of 2001.
[3] Pallavi Murghai Goel et al, A Literature Review of Cyber Security, International Journal of Research and Analytical Reviews, Vol 6, No 3, 2019, p 138.
[4] Sayyed Mohammed, Cyber Security and Cyber Crime, International Research Journal of Engineering and technology, Vol 8 No 4 | Apr 2021, p 179.
[5] Widya Setlabudi, Ctbercrime, and Global Security Threats, A challenge in Intranational Law, Russian Journal, Vol 9, No 3, 2023, p 441.
[6] Art 8 of the Budapest Convention on Cybercrime of 2001.
[7] *Ibid*., Art 10.

Each Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offense, in accordance with its domestic law, any complicity when committed intentionally with a view to the commission of one of the offenses established pursuant to Articles 2 to 10 of this Convention, with the intention that such an offense be committed[8].

Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons may be held liable for offenses established under this Convention when committed on their behalf by any natural person, acting either individually, either as a member of an organ of the legal entity, which exercises management power within it, founded[9]. Each Party shall adopt such legislative and other measures as may be necessary to ensure that criminal offenses established pursuant to Articles 2 to 11 are punishable by effective, proportionate and dissuasive sanctions, including custodial sentences. Each Party shall ensure that legal entities held responsible pursuant to Article 12 are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including financial sanctions[10].

Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this section are subject to the conditions and safeguards provided for by its domestic law, which must ensure adequate protection of the rights of the individuals and freedoms, in particular rights established in accordance with the obligations which it has subscribed to in application of the Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe (1950) and the International Covenant relating civil and political rights of the United Nations (1966), or other international instruments applicable concerning human rights, and which must integrate the principle of proportionality[11].

Every Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or otherwise require the expedited retention of specified electronic data, including traffic data, stored by means of a computer system, particularly when there is reason to believe that these are particularly susceptible to loss or modification[12] .Each Party shall adopt such legislative and other measures as may be necessary to authorize its competent authorities to search or otherwise gain access to: a computer system or part thereof and the computer data stored therein ; and computer storage support allowing computer data to be stored on its territory[13].

The Parties shall cooperate with each other, in accordance with the provisions of this Chapter, in accordance with relevant international instruments on international cooperation in criminal matters, arrangements based on uniform or reciprocal legislation and their national law, to the greatest extent possible. as widely as possible, for the purposes of investigations or proceedings concerning

[8] Art 11 of the Budapest Convention on Cybercrime of 2001.
[9] Alisdair A. Gillespie, Cybercrime, Key Issues and Debates, Taylor & Francis, 2015, p 215.
[10] Herbert B. Dixon Jr., Cybersecurity, How Important Is It?, The Judges' Journal, Vol. 51 No. 4, 2012, p 37.
[11] Art 16 of the Budapest Convention on Cybercrime of 2001.
[12] *Ibid.*, Art 17.
[13] *Ibid.*, Art 19.

criminal offenses relating to computer systems and data or to collect evidence, in electronic form, of a criminal offense[14]. The Parties provide each other with the widest possible mutual assistance for the purposes of investigations or proceedings concerning criminal offenses linked to computer systems and data, or in order to collect evidence in electronic form of a criminal offense. Each Party shall also adopt such legislative and other measures as may be necessary to fulfil the obligations[15].

1.2. The 1st Additional Protocol to the Convention on Cybercrime, relating to the criminalization of acts of a racist and xenophobic nature of 2003

Taking into account the relevant international legal instruments in this area, and in particular the Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 relating to the general prohibition of discrimination, the existing conventions of Council of Europe on co-operation in criminal matters, in particular the Convention on Cybercrime and the United Nations International Convention of 21 December 1965 on the Elimination of All Forms of Racial Discrimination, the Joint Action of 15 July 1996 of the European Union adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning action against racism and xenophobia[16].

The purpose of this Protocol is to supplement, for the Parties to the Protocol, the provisions of the Convention on Cybercrime, opened for signature in Budapest on November 23, 2001 with regard to criminalization acts of a racist and xenophobic nature disseminated through computer systems[17].

For the purposes of this Protocol, the expression: "racist and xenophobic material" means any written material, images or other representation of ideas or theories that advocates or encourages hatred, discrimination or violence, against a person or group of people, on the basis of race, colour, ancestry or national or ethnic origin, or religion, to the extent that the latter serves as a pretext for any of these elements, or which incites such acts[18].

Each Party shall adopt such legislative and other measures as may prove necessary to establish as criminal offenses in its domestic law, when committed intentionally the following conduct: the dissemination or other forms of making available to the public, through a computer system, racist and xenophobic material. A Party may reserve the right not to impose criminal liability for conduct provided for in paragraph 1 of this Article where the material, as defined in Article 2, paragraph 1, advocates, encourages or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available[19].

---

[14] Art 23 of the Budapest Convention on Cybercrime of 2001.
[15] *Ibid.*, Art 25.
[16] Preamble to First Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems of 2003.
[17] Art 1 of the 1st Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems of 2003.
[18] Art 2 of the First Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems of 2003.
[19] *Ibid.*, Art 3.

Each Party shall adopt the legislative and other measures which prove necessary to establish as a criminal offense, in its domestic law, when committed intentionally and without right, the following conduct: the threat, through a computer system, of commit a serious criminal offense, as defined by national law, against a person because of his or her membership in a group that is characterized by race, colour, ancestry or national or ethnic origin, or religion to the extent that the latter serves as a pretext for one or other of these elements, or a group of people which is distinguished by one of these characteristics[20].

Each Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offense in its domestic law, when committed intentionally and without right, conduct that insults it in public, through a computer system, of a person by reason of his or her membership in a group which is characterized by race, colour, ancestry or national or ethnic origin, or religion to the extent that the latter serves as a pretext for the one or other of these elements, or of a group of people who are distinguished by one of these characteristics[21].

Each Party shall adopt the legislative measures which prove necessary to establish as criminal offenses, in its domestic law, when committed intentionally and without right, the dissemination or other forms of making available to the public, by means of a computer system, material that denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognized as such by a final and definitive decision of the International Military Tribunal , established by the London Agreement of August 8, 1945, or by any other International Tribunal established by relevant international instruments and whose jurisdiction has been recognized by that Party[22].

Each Party shall adopt such legislative and other measures as may be necessary to criminalize, under its domestic law, assisting in the commission of an offense as defined in this Protocol when committed intentionally and without law, or being complicit, with the intention that such an offense be committed[23].

1.3. The 2nd Additional Protocol to the Convention on Cybercrime, relating to enhanced cooperation and disclosure of electronic evidence of 2023

Recognizing the growing use of information and communications technologies, including internet services, and the increase in cybercrime, which constitutes a threat to democracy and the rule of law, and which many States consider also as a threat to human rights. Also recognizing the growing number of victims of cybercrime and the importance of obtaining justice for these victims. Aware that evidence collected in electronic form of any criminal offense is increasingly stored

[20] Maurice Dawson et al, Cybersecurity Capabilities in Developing Nations and its Impact on Global Security, IGI Global,2022,p 82.
[21] Art 5 of the First Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems of 2003.
[22] Art 6 of the First Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems of 2003.
[23] *Ibid.*, Art 7.

on computer systems located in foreign, multiple or unknown jurisdictions, and convinced that additional measures are necessary to legally obtain such evidence to enable a response effective through criminal justice and to defend the rule of law;

Taking into account the need for increased and more effective cooperation between States and the private sector. In this context, greater clarity or legal certainty is necessary for service providers and other entities regarding the circumstances in which they can respond direct requests for disclosure of electronic data from criminal justice authorities of other Parties. Intending to further strengthen cooperation regarding cybercrime and the collection of evidence in electronic form of a criminal offense for the purposes of investigations or specific criminal proceedings through additional tools relating to more efficient mutual assistance and other forms of cooperation between competent authorities; cooperation in urgent situations; and direct cooperation between competent authorities and service providers, the States parties take the appropriate measures to combat cybercrimes[24].

Each Party shall adopt legislative and other measures necessary to authorize its competent authorities for the purposes of specific criminal investigations or proceedings, to be issued to an entity providing registration services located in the territory of another Party a request for information in the possession or control of the entity in order to identify or contact the person who registered a domain name. Each Party shall adopt such legislative and other measures as may be necessary to permit an entity located in its territory to disclose such information in response to a request under paragraph 1, subject to reasonable conditions provided for by domestic law[25].

Each Party shall adopt such legislative and other measures as may be necessary to authorize its competent authorities to issue an order directly to a service provider in the territory of another Party to produce specified and stored data relating to subscribers in the possession of or under the control of the provider, where such information is necessary for specific investigations or criminal proceedings carried out by the issuing Party[26].

Each Party shall adopt such legislative and other measures as may be necessary, in the event of an emergency, can transmit a request to a Contact Point in another Party and receive a request from the latter for immediate assistance in obtaining from a service provider located in the territory of the Party concerned the expedited disclosure of specified stored computer data that is in the possession or control of said service provider, without a request for mutual legal assistance. A Party may, at the time of signing this Protocol or when depositing its

[24] Preamble to the 2nd Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence of 2023.
[25] Art3 of the 2nd Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence of 2023.
[26] *Ibid.,* Art 7.

instrument of ratification, acceptance or approval, declare that it will not execute requests[27].

Each Party may request mutual legal assistance by the most rapid means when it considers it urgent. A request for assistance under this section must present, in addition to other required content, a description of the facts supporting the existence of an urgent situation and an explanation of how the requested assistance relates to that situation. The requested Party accepts such assistance in electronic form. It may require appropriate levels of security and authentication before accepting it.

The requested Party may, by the most rapid means for additional information in order to evaluate the request for mutual assistance. The requesting Party provides this additional information by the most rapid means. After having ensured that the other conditions of mutual assistance are satisfied, the requested Party responds to the request for assistance by the quickest means.

Each Party shall ensure that a person from its central authority or other authorities responsible for requests for mutual assistance is available twenty-four hours a day, seven days a week, to respond to a request made under this article. The central authority or other authorities responsible for requests for assistance from the Requesting and Requested Parties may decide to provide that the results of the execution of a request for assistance made under this Article, or a preliminary copy of those results, may be transmitted to the requesting Party by a channel other than that used for transmission of the request[28].

A requesting Party may request, and the requested Party may authorize, the taking of the testimony of a witness or expert by videoconference. The requesting Party and the requested Party shall consult together to facilitate the resolution of any problems that may arise regarding the execution of the request, including where applicable the choice of the Party which directs the operation if one or both Parties must require the witness or expert to take a particular oath, issue warnings or instructions; the manner of questioning the witness or expert; the manner in which the rights of the witness or expert will be duly guaranteed; the treatment of claims of privileges or immunity; handling objections to questions or answers; and whether one or both Parties provide translation, interpretation and transcription services[29].

The coordination is considered particularly useful, by mutual agreement as the competent authorities of two or more Parties may establish and operate a joint investigation team in their territories to facilitate investigations or prosecutions. The competent authorities are determined by the respective Parties concerned[30].

---

[27] Art 7 of the Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence of 2023.

[28] Art 10 of the Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence of 2023.

[29] *Ibid.,* Art 11.

[30] Art 12 of the 2nd Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence of 2023.

2. Malabo Convention on Cybersecurity and Personal Data Protection of 2014

Cybersecurity being defined as all the means used to ensure the security of the computer systems and data of a State or a company[31]. personal as well as private life therefore presents itself as a major issue in the information society, both for public authorities and for other stakeholders; that this protection requires a balance between the use of information and communication technologies and the protection of the private lives of citizens in their daily or professional lives while guaranteeing the free circulation of information. Concerned by the urgency of setting up a system to deal with the dangers and risks arising from the use of computers and files on individuals with the aim of respecting private life and freedoms while promoting the promotion and development of ICT in the member countries of the African Union [32].

One of the particularities of AI-based cybersecurity solutions also lies in their ability to adapt to new threats. As new dangers appear, machine learning algorithms are trained by exploiting the new data. Thus, they improve their ability to detect these risks and respond to them continuously[33]. AI is a powerful tool for more effective cybersecurity, particularly with regard to the cyber defence both from an organizational point of view, for the allocation of resources or data protection, as well as for more specific methods such as incident response or cyber threat management. Artificial intelligence makes it possible to process a large volume of data continuously. Thus, it can detect new security risks, especially since the algorithms learn over time in order to avoid repetitive procedures. These increased capabilities therefore improve certain aspects of cybersecurity. These advantages are useful for incident management processes as well as threat management[34].

Data management is a major contemporary issue in cybersecurity. Faced with massive flows of information, it is imperative to be able to manage and protect this data. Data management will enable optimization of the use of data in security processes. As for data protection, essential as it is a major asset for a company, AI will make it possible to map, reference, save and encrypt data[35].

The dangerousness of the attack is observed in the possibilities of influencing the AI by subtly injecting it with scenarios going in the desired direction. It is also impossible to remedy this type of attack when the corrupted data has been injected, therefore rendering the work of the AI lost. This attack is often used to paralyze a company's cybersecurity measures by confusing the precision of the protection system which will then no longer be able to detect certain security vulnerabilities on the network[36].

---

[31] Peter W. Singer, Allan Friedman, Cybersecurity, What Everyone Needs to Know, Oxford University Press, 2014,p 93.
[32] Preamble to the Malabo Convention on Cybersecurity and Personal Data Protection of 2014.
[33] Prakhar Agarwal et al, Cyber Security, a Need in Globalization, Vidya Journal of Engineering and Technology, Vol 3, No 1,2017, p 51.
[34] Noah Berlatsky, Cybercrime, Greenhaven Press, 2013, p125.
[35] Rajeswari Raju et al, Cyber Security Awareness in Using Digital Platforms Among Students in A Higher Learning Institution, Asian Journal of University Education (AJUE), Vol 18, No 3, 2022,p 757.
[36] Nir Kshetri, Cybercrime and Cybersecurity in the Global South, Palgrave Macmillan, 2013, p 152 .

Nowadays, artificial intelligence offers a real advantage for anyone who wants to carry out a cyber-attack. Due to the availability and accessibility of these AI techniques, anyone could become a hacker. Faced with all these different uses, whether offensive or defensive, artificial intelligence remains an area in which we have little perspective today. If these assets are obvious, its limits show us all the failures that will have to be corrected in order to mitigate the risks of attacks or even ethics[37].

2.1. Managing electronic translations

Member States shall ensure that electronic commerce activity is exercised freely in all States Parties which ratify or accede to this Convention with the exclusion of the following areas: gambling, even in the form of betting and lotteries, legally authorized; and legal representation and assistance activities; as well as activities carried out by notaries or equivalent authorities in application of the texts in force[38].

Electronic commerce activity is subject to the law of the State Party in whose territory the person carrying it out is established, subject to the common intention of that person. Without prejudice to the Article 3, all advertising, in whatever form, accessible via an online communication service, must be clearly identified as such. It must clearly identify the natural or legal person on whose behalf it is carried out. The conditions to which the possibility of benefiting from promotional offers as well as that of participating in competitions or promotional games are subject, when these offers, competitions or games are offered electronically, must be clearly specified and easily accessible. The States Parties of the African Union undertake to prohibit direct prospecting via any form of indirect communication using, in any form whatsoever, the contact details of a person who has not expressed prior consent to receive direct marketing by this means are intended for the goods or services[39].

The information requested for the conclusion of a contract or that which is sent during its execution may be transmitted by electronic means if their recipients have accepted the use of this means. The use of electronic communications is presumed admissible unless the beneficiary has already expressed his or her preference for another means of communication. The supplier, who offers, on a professional basis, by electronic means, the supply of goods or the provision of services, makes available the contractual conditions applicable directly or indirectly, in a manner which allows their conservation and reproduction in accordance with national legislation. For the contract to be validly concluded, the recipient of the offer must have had the opportunity to check the details of his order, in particular the price, before confirming it to express his acceptance[40].

The supplier of goods or provider of services by electronic means, who claims that the performance of an obligation must prove its existence and, when he claims to

[37] Bharat Bhushan, The Growing Importance of Cyber Security in the Digital Age, International Journal For Innovative Research in Multidisciplinary field, Vol 9, No 5, 2023, p 236.
[38] Art 2 of the Malabo Convention on Cybersecurity and Personal Data Protection of 2014.
[39] Art 5 of the Malabo Convention on Cybersecurity and Personal Data Protection of 2014.
[40] *Ibid.*, Art 6.

be discharged, must prove that the obligation is non-existent or extinguished. When the legal provisions of member States have not established other principles. In the absence of a valid agreement between the parties, the judge resolves conflicts of literal proof by determining by all possible means the most probable title, whatever be the support. The copy or any other reproduction of documents passed electronically has the same probative force as the document itself when it is certified as true by organizations approved by an authority of the State Party[41].

2.2. Personal Data Protection

With the use of artificial intelligence, companies have entered the era of proactivity. to detect a cyber-attack very quickly, even though it is only at the weak signal stage, before it spreads and causes too much damage. Early detection is one of the great strengths of AI when used for cybersecurity. Artificial intelligence misused by cybercriminals to spot, identify and exploit vulnerabilities and security flaws in companies[42].

Each State Party undertakes to establish a legal framework aimed at strengthening fundamental rights and public freedoms, in particular the protection of data and to suppress any offense relating to any invasion of privacy without prejudice to the principle of the freedom of movement of personal data. This system must guarantee that any processing, in whatever form, respects the fundamental rights and freedoms of individuals while taking into account the prerogatives of the State, the rights of local authorities and the purposes for which the companies have been created[43].

The following acts are considered as a treat according to this Convention:
-Any collection, processing, transmission, storage or use of personal data carried out by a person, by the State, local authorities, legal entities under public or private law;
-Any automated or non-automated processing of data contained or intended to appear in a file, with the exception of the processing mentioned in Article 9.2 of this Agreement;
-Any processing carried out on the territory of a State Party of the African Union;
Any processing of data concerning public security, defence, research and prosecution of criminal offenses or state security, subject to exemptions defined by specific provisions set by other legal texts in force[44].

Each State Party undertakes to establish an authority responsible for the protection of personal data. The national protection authority is an independent administrative authority responsible for ensuring that the processing of personal data is implemented. in accordance with the provisions of this Convention. The national protection authority informs data subjects and data controllers of their rights and obligations. Without prejudice to the provisions of Article 11.6, each State Party determines the composition of the national authority responsible for the protection of personal data. Sworn agents, in accordance with the provisions

[41] *Ibid.*, Art 7.
[42] *Ibid.*, Art 8.
[43] David S. Wall, Cybercrime, The Transformation of Crime in the Information Age, 2007, p 95.
[44] Art 9 of the Malabo Convention on Cybersecurity and Personal Data Protection of 2014.

in force in the States Parties, may be called upon to participate in the implementation of verification missions[45].

National protection authorities are responsible for ensuring that the processing of personal data is implemented in accordance with the provisions of this Convention in the States Parties of the African Union. National protection authorities ensure that Information and Communication Technologies do not pose a threat to public freedoms and the private lives of citizens. As such, they are responsible for: responding to any request for advice relating to the processing of personal data; inform data subjects and data controllers of their rights and obligations; authorize file processing in a certain number of cases, particularly sensitive files; receive the formalities prior to the creation of processing of personal data[46].

The processing of personal data is considered legitimate if the data subject gives consent. However, this consent requirement may be waived when the processing is necessary: for compliance with a legal obligation to which the data controller is subject; the execution of a mission of public interest or relating to the exercise of public authority, vested in the controller or the third party to whom the data are communicated; the execution of a contract to which the data subject is a party or the execution of pre-contractual measures taken at his or her request; to safeguard the interests or fundamental rights and freedoms of the person concerned[47].

States Parties undertake to prohibit the collection and any processing which reveals racial, ethnic or regional origin, parentage, political opinions, religious or philosophical beliefs, trade union membership, sexual life, data genetic or more generally those relating to the state of health of the person concerned[48]. The interconnection of files referred to in Article 10/4 of this Agreement must make it possible to achieve legal or statutory objectives presenting a legitimate interest for those responsible for processing. It cannot lead to discrimination or reduction of the rights, freedoms and guarantees for the persons concerned nor be accompanied by appropriate security measures and must also take into account the principle of relevance of the data subject to the interconnection[49].

The data controller must provide the person whose data is processed, at the latest, upon collection and regardless of the means and media used, the following information:
-The specific purpose of the processing for whom the data is intended;
-The categories of data concerned;
-The recipient to whom the data may be communicated;
-The fact of being able to ask to no longer appear on the file;
-The existence of a right of access to data
-The duration of data retention;

[45] *Ibid.,* Art 11.
[46] Art 12 of the Malabo Convention on Cybersecurity and Personal Data Protection of 2014.
[47] *Ibid.,* Art 13.
[48] *Ibid.,* Art 12.
[49] *Ibid.,* Art 15.

-The possibility of any transfer of data to third countries[50].

Conclusion

To cope with the resurgence of the cyber criminality and ensure the protection of the national security, the States are increasingly turning to solutions using artificial intelligence a double-edged sword. However: at the same time, cybercriminals are also taking advantage of the possibilities of AI. The growing role of AI in cybercrime requires continued attention. While AI offers incredible potential for progress, it also amplifies the risks posed by cybercriminals. Equipping national institutions with the right technological tools is the key to staying informed and getting ahead. The States need to be aware of how AI can be exploited by threat actors at different stages of an attack, so they can place their defence in the right place.

Cybercriminals have understood the power of artificial intelligence. They misuse it to spot, identify and exploit vulnerabilities and security gaps inside countries. AI allows them to adapt quickly and efficiently to the cybersecurity environments of the structures they target. Hackers are able to act based on the behaviour of targets, and achieve more intelligent and personalized targeting of their future victims. Thus, thanks to Artificial Intelligence, the detection mechanisms can be more easily identified and circumvented.

Despite all precautions, individuals as well governments may be the victim of a cyber-attack. Companies therefore have an interest in having contingency plans in the case of a cyber-attack. These plans avoid or limit the loss of data and ensure the continuation of the company's activity to evaluate current cybercrime legislation and adapt it to recent technological advances. Also, it is crucial to insist on the importance of strengthening the capacities of units fighting against cybercrime.

At the end of this research paper, we propose the following recommendations:
- It is advisable to draft and add to the internal regulations a charter of compliance with the rules relating to the IT system.
- Raise awareness among company individuals and employees of cyber risks.
- The Training of experts to detect cyber anomalies.
- The Implementation of the legal provisions of International Conventions to mitigate the effects of cybercrime.
- The Identification of possible cyber defence providers and services.
- The use of Artificial Intelligence to determine the specific risks associated with digital tools.
- The Adaptation of defence systems of States with new technologies.
- Adoption the best security practices and their capabilities and their limitations.
- The Implementation and maintain risk management tools.
- The encouragement of collaboration between States in matter to ensure cybersecurity.
- The development of standards operating procedures for cybercrimes investigations.

[50] George Kostopoulos , Cyberspace and Cybersecurity, Taylor & Francis, 2012 , p 35.

- The use of digital forensic tools to improve knowledge transfer and efficiency.
- The creation of an online training platform to learn how to fight cybercrime.

References

1. International Conventions:

-Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981

-The Budapest Convention on Cybercrime of 2001

-Malabo Convention on Cybersecurity and Personal Data Protection of 2014

-The UN Norms of Responsible State Behaviour in Cyberspace.

2. International Protocoles:

-Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and trans-border data flows 2001

-The 1st Additional Protocol to the Convention on Cybercrime, relating to the criminalization of acts of a racist and xenophobic nature of 2003

-The 2nd Additional Protocol to the Convention on Cybercrime, relating to enhanced cooperation and disclosure of electronic evidence of 2023

3. Books:

Alisdair A. Gillespie, Cybercrime, Key Issues and Debates, Taylor & Francis, 2015, p 215.

David S. Wall, Cybercrime, The Transformation of Crime in the Information Age, 2007, p 95.

George Kostopoulos, Cyberspace and Cybersecurity, Taylor & Francis, 2012, p 35.

Maurice Dawson et al, Cybersecurity Capabilities in Developing Nations and its Impact on Global Security, IGI Global,2022,p 82.

Noah Berlatsky, Cybercrime, Greenhaven Press, 2013, p125.

Nir Kshetri, Cybercrime and Cybersecurity in Global South, Palgrave Macmillan,2013, p 152

Peter W. Singer, Allan Friedman, Cybersecurity, What Everyone Needs to Know, Oxford University Press, 2014,p 93.

4. Research papers:

Bharat Bhushan, The Growing Importance of Cyber Security in the Digital Age, International Journal For Innovative Research in Multidsciplnary field, Vol 9, No 5, 2023, p 236.

Bharat Bhushan,The Growing Importance of Cyber Security in the Digital Age, International Journal For Innovative Research in Multidsciplnary field, Vol 9, No 5, 2023, p 236.

Herbert B. Dixon Jr., Cybersecurity, How Important Is It?,The Judges' Journal, Vol. 51 No. 4, 2012, p 37

Sayyed Mohammed, Cyber Security and Cyber Crime, International Research Journal of Engineering and Technology, Vol 8 No 4 | Apr 2021, p 179.

Prakhar Agarwal et al, Cyber Security, a Need in Globalization, Vidya Journal of Engineering and Technology, Vol 3, No 1,2017,p 51.

Rajeswari Raju et al, Cyber Security Awareness in Using Digital Platforms Among Students in A Higher Learning Institution, Asian Journal of University Education (AJUE), Vol 18, No 3, 2022, p 757.

Widya Setlabudi, Ctbercrime, and Global Security Threats, A challenge in Intranational Law, Russian Journal, Vol 9, No 3, 2023, p 441.