Last updated on 16th November 2023

Cybercrime legislation - legislative profile

TUNISIA

This profile has been prepared in the framework of the Council of Europe project on capacity building in cybercrime with the aim of sharing information and assessing the current state of implementation of the Convention on Cybercrime in national legislation. This does not necessarily reflect the official positions of the country covered or of the Council of Europe.

Contact at the Council of Europe:

Head of the Economic Crime Division
Directorate General for Human Rights and Legal Affairs
Council of Europe, Strasbourg France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

State:	
Signature of the Budapest Convention:	Not signed
Ratification/accession:	Not ratified

Chapter I – Terminology	
Article 1 – "Computer system", "computer data", "service provider", "traffic data" : For the purposes of this Convention : computer system" means any device or set of interconnected or related devices, one or more of which, when executing a program, performs automatic data processing; computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme for causing a computer system to perform a function; service provider" means: any public or private entity that offers users of its services the possibility of communicating by means of a computer system, and any other entity processing or storing computer data for this communication service or its users. "traffic data" means any data relating to a communication passing through a computer system, generated by the computer system as part of the communication chain, indicating the origin, destination, route, time, date, size and duration of the communication or the type of underlying service.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 5 the following definitions;** Information system: a set of software, tools and equipment, isolated, interconnected or related, ensuring automated data processing operations. Computer data: any presentation of facts, information or concepts in a form that lends itself to automated processing, including software that enables an information system to perform a specific function. Communication system: a set of metallic, optical, radio or any other technology supports that can ensure the transmission, emission or reception of signals or data. Communications service provider: any natural or legal person providing a telecommunications service to the public, including internet services. Traffic flow or access data: data produced by an information system indicating the source of the communication, its destination, its route, its time, its date, its volume, and its duration as well as the type of communication service .
Chapter II - Measures to be taken at national level	
Section 1 - Substantive criminal law	
Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems	

Article 2 - Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the intentional and unauthorised access to all or part of a computer system. A Party may require that the offence be committed in breach of security measures, with intent to obtain computer data or with other criminal intent, or in connection with a computer system connected to another computer system.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 16;** Anyone who knowingly accesses or illegally remains in a computer system in whole or in part is punishable by three months to one year of imprisonment and a fine of ten thousand dinars. Anyone who knowingly exceeds the limits of the right of access granted to them is liable to the same penalty. **Tunisia Decree Law 54 – 13 or 2022 relating to Cybercrime states in article 21;** Anyone who deliberately misappropriates computer data belonging to others is punished by five years of imprisonment and a fine of thirty thousand dinars. The attempt is punishable.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the intentional and lawless interception by technical means of computer data, in 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 offence be committed with criminal intent or in connection with a computer system connected to another computer system.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 18;** Anyone who knowingly and without right uses technical means for the interception of communication data in a sending not intended for the public within , from or to an information system including lateral radiation emitted by the system and carrying communication data. Interception includes obtaining data relating to traffic flows or their content, as well as copying or recording them. The attempt is punishable.
Article 4 – Violation of data integrity Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the damaging, deletion, deterioration, alteration or suppression of computer data. A Party may reserve the right to require that the conduct described in paragraph 1 results in serious harm.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 19;** Anyone who knowingly damages, modifies, deletes, cancels or destroys computer data is punished by three years of imprisonment and a fine of twenty thousand dinars. The attempt is punishable. **Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 22;**

	Anyone who intentionally causes financial harm to others by introducing, altering, erasing or deleting computer data or by any form of interference with the functioning of a computer is punishable by six years of imprisonment and a fine of one hundred thousand dinars. computer system, with the intention of obtaining financial or economic benefit for oneself or for others.
Article 5 – Violation of system integrity Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the intentional and unlawful serious interference with the functioning of a computer system by means of the input, transmission, damage, deletion, deterioration, alteration or suppression of computer data.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 20;** Whoever knowingly and illegally hinders the operation of a computer system, by introducing computer data or sending it, damaging it, is punished by three years of imprisonment and a fine of thirty thousand dinars, modified, deleted, canceled, destroyed, or by other electronic means. The attempt is punishable.
Article 6 – Abuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right : production, sale, obtaining for use, import, distribution or other forms of making available: a device, including a computer programme, primarily designed or adapted to enable the commission of one of the offences established in accordance with articles 2 to 5 above; a password, access code or similar computer data enabling access to all or part of a computer system, with the intention that they should be used to commit any of the offences referred to in Articles 2 to 5; and possession of an item referred to in paragraph a.i or ii above, with the intent that it be used to commit any of the offences referred to in Articles 2 to 5. A Party may require under its domestic law that a certain number of such items be possessed in order to incur criminal liability. 2 This Article shall not be construed as imposing criminal liability where the production, sale, procurement for use, import, dissemination or other making available referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with Articles 2 to 5 of this	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 17;** Anyone who knowingly produces, sells, imports, distributes, supplies, exhibits, obtains for use, or possesses the following is punished with three years of imprisonment and a fine of twenty thousand dinars, and this illegally or outside the cases where the need for scientific research or IT security requires it: • Equipment or a computer program designed or tamed to commit the offenses governed by this decree-law. • A password, an access code or any similar computer data allowing access, in whole or in part, to an information system with a view to committing the offenses governed by this decree-law. The attempt is punishable.

Convention, as in the case of authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that such reservation does not relate to the sale, distribution or other making available of the items referred to in paragraph 1.a.ii of this article.	
Title 2 - Computer-related offences	
Article 7 - Computer forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the intentional and unlawful input, alteration, deletion or suppression of computer data, generating non-authentic data, with the intent that such data be taken into account or used for legal purposes as if they were authentic, whether or not directly readable and intelligible. A Party may require fraudulent intent or similar criminal intent for criminal liability to arise.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 23;** Introduction, alteration, erasure, or deletion of computer data resulting in inauthentic data. Anyone who commits falsification capable of causing harm through the introduction, alteration, erasure or deletion of computer data, leading to the production of non-authentic data, with the intention of exploiting it as if it were authentic.
Article 8 - Computer fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law the intentional and wrongful causing of economic damage to another person: a by any introduction, alteration, deletion or suppression of computer data; b by any form of interference with the functioning of a computer system, with the intention, fraudulent or criminal, to obtain without right an economic benefit for oneself or for others.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 22;** Anyone who intentionally causes financial harm to others by introducing, altering, erasing or deleting computer data or by any form of interference with the functioning of a computer is punishable by six years of imprisonment and a fine of one hundred thousand dinars. computer system, with the intention of obtaining financial or economic benefit for oneself or for others.
Title 3 - Content-related offences	
Article 9 - Offences concerning child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the following conduct when committed intentionally and without right: a the production of child pornography for distribution via a computer system;	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 26;** Subject to specific legislation, anyone who intentionally produces, displays, provides, publishes, sends, obtains or possesses computer data with pornographic content showing a child or a person having the appearance of a child engaging in or being the victim of explicit or suggestive sexual practices.

b offering or making available child pornography via a computer system; c the distribution or transmission of child pornography via a computer system; d procuring child pornography for oneself or others by means of a computer system; e the possession of pornography child pornography in a computer system or computer data storage medium. 2 For the purposes of paragraph 1 above, the term "child pornography" includes any pornographic material depicting a visual image: a a minor engaging in sexually explicit conduct; b a person who appears to be a minor engaging in sexually explicit behaviour; c realistic images depicting a minor engaged in sexually explicit behaviour. 3 For the purposes of paragraph 2 above, the term "minor" means any person under the age of 18 years. A Party may, however, require a lower age limit, which shall be at least 16 years. A Party may reserve the right not to apply, in whole or in part paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	Anyone who intentionally uses information systems to publish or broadcast images or video sequences of physical or sexual assault on others is liable to the same penalties provided for in the first paragraph of this article.
Title 4 - Offences related to infringements of intellectual property and related rights	
Article 10 - Offences related to infringements of intellectual property and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, in accordance with its domestic law, infringements of intellectual property, as defined by the law of that Party, consistent with its obligations under the Paris Act of 24 July 1971 revising the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Treaty on Intellectual Property,	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 25;** Subject to the penalties provided for by special texts, anyone who intentionally uses information systems and communication to violate copyright and related rights without obtaining authorization from the rights holder(s) with the aim of profiting from them or harming the economy or the rights of others.

with the exception of any moral rights conferred by these Conventions, where such acts are committed deliberately, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights as defined by the law of that Party, in accordance with the obligations undertaken by that Party under the International Convention for the Protection of Performers, producers of phonograms and broadcasting organizations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by these Conventions, where such acts are committed deliberately, on a commercial scale and by means of a computer system. 3 A Party may, in well-defined circumstances, reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article, provided that other effective remedies are available and that such reservation does not affect the international obligations of that Party under the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 - Other forms of liability and sanctions	
Article 11 - Attempt and complicity 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 to 10 of this Convention, with the intent that such an offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law any intentional attempt to commit any of the offences established in accordance with Articles 3 to 5, 7, 8, 9.1.a and c of this Convention. 3	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states that attempting to commit the following articles is criminalised;** Article 16 - Illegal access to data/computer system Article 17 - Possession of program or password to commit offence in this act Article 18 - Illegal Interception Article 19 - Damage, modify, alter a computer system Article 20 - Illegally hinders operation of computer system Article 21 - Altering, erasing or deletion of data for financial gain

Each Party may reserve the right not to apply, in whole or in part, any of the provisions of this Agreement in part, paragraph 2 of this Article.	
Article 12 – Liability of legal entities 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for offences established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, founded: a on a power of representation of the legal entity; b on an authority to take decisions on behalf of the person moral; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall adopt such measures as may be necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of the offences established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. Depending on the legal principles of the Party, the liability of a legal entity may be criminal, civil or administrative. This liability is established without prejudice to the criminal liability of the natural persons who committed the offence.	Not identified
Article 13 – Penalties and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 to 11 are punishable by effective, proportionate and dissuasive sanctions, including custodial sentences. 2 Each Party shall ensure that legal persons held liable	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime provides punishments for all respective articles in accordance with the Cybercrime Convention;**

pursuant to Article 12 are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	
Section 2 - Procedural law	
Title 1 - Common provisions	
Article 14 – Scope of application of procedural law measures 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings. 2 Except as otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this Article: a criminal offences established in accordance with Articles 2 to 11 of this Convention; b all other criminal offences committed using a computer system; and c the collection of electronic evidence of any criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to the offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not narrower than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider limiting such a reservation so as to enable the widest possible application of the measure referred to in article 20. b Where a Party, because of restrictions imposed by its legislation in force at the time of adoption of this Convention, is	

unable to apply the measures referred to in Articles 20 and 21 to communications transmitted on a computer system of a service provider: i is implemented for the benefit of a closed user group, and ii which does not use public telecommunications networks and which is not connected to another computer system, whether public or private, that Party may reserve the right not to apply such measures to such communications. Each Party shall consider limiting any such reservation so as to permit the widest possible application of the measure referred to in articles 20 and 21.	
Article 15 – Conditions and safeguards 1 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 by its domestic law, which shall ensure adequate protection of human rights and freedoms, in particular rights established in accordance with obligations under the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1950) and the United Nations International Covenant on Civil and Political Rights (1966), or other applicable international human rights instruments, and which must incorporate the principle of proportionality. 2 Where appropriate, having regard to the nature of the procedure or power concerned, such conditions and safeguards shall include, inter alia, judicial or other independent supervision, reasons for application and limitations on the scope and duration of the power or procedure in question. 3 Each Party shall, to the extent consistent with the public interest, in particular the proper administration of justice, consider the effect of the powers and procedures in this Section on the rights, responsibilities and duties of the judiciary and legitimate interests of third parties.	

Title 2 - Rapid preservation of stored computer data	
Article 16 – Rapid preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or otherwise require the expeditious preservation of specified electronic data, including traffic data, stored by means of a computer system, in particular where there is reason to believe that such data are particularly susceptible to loss or alteration. 2 Where a Party applies paragraph 1 above, by means of an order requiring a person to preserve specified stored data in its possession or control, that Party shall adopt such legislative and other measures as may be necessary to require that person to preserve and protect the integrity of that data for as long as necessary, but not longer than ninety days, to enable the competent authorities to obtain disclosure. A Party may provide for such an injunction to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the data custodian or other person responsible for storing the data to maintain the secrecy of the implementation of such procedures for the period provided for by its domestic law. 4 The powers and procedures referred to in this Article must be subject to articles 14 and 15.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 9;** The public prosecutor, the investigating judge or the judicial police officers authorized in writing are authorized to order: To seize an information system in whole or in part or a computer medium including stored data that can help reveal the truth. If entry into the information system proves unnecessary or impossible to carry out, the data relating to the offense as well as those allowing their reading and understanding will be copied onto a computer medium so as to ensure authenticity and integrity of their content. To collect or record in real time data relating to telecommunications traffic using appropriate technical means. They are also authorized to access directly or with the assistance of experts any system or IT support and carry out an investigation in order to obtain stored data that can help reveal the truth. The competent services of the Ministry of National Defense and the Ministry of the Interior ensure the seizure operation, its location and the process of access to information systems, data, stored information, software and all these materials relating to the two ministries, each according to its area of expertise.
Article 17 – Rapid retention and disclosure of traffic data 1 In order to ensure the retention of traffic data pursuant to Article 16, each Party shall adopt such legislative and other measures as may be necessary: a to ensure the rapid preservation of such traffic data, whether one or more service providers were involved in the transmission of that communication; and b to ensure the prompt disclosure to the competent authority of the Party, or to a person designated by that	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 9;** The public prosecutor, the investigating judge or the judicial police officers authorized in writing are authorized to order: To seize an information system in whole or in part or a computer medium including stored data that can help reveal the truth. If entry into the information system proves unnecessary or impossible to carry out, the data relating to the

authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the channel through which the communication was transmitted. 2 The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.	offense as well as those allowing their reading and understanding will be copied onto a computer medium so as to ensure authenticity and integrity of their content. To collect or record in real time data relating to telecommunications traffic using appropriate technical means. They are also authorized to access directly or with the assistance of experts any system or IT support and carry out an investigation in order to obtain stored data that can help reveal the truth. The competent services of the Ministry of National Defense and the Ministry of the Interior ensure the seizure operation, its location and the process of access to information systems, data, stored information, software and all these materials relating to the two ministries, each according to its area of expertise.
Title 3 - Production order	
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue orders: a a person present in its territory to disclose specified computer data in its possession or control that is stored in a computer system or computer storage medium; and b a service provider offering services in the territory of the Party, to communicate data in its possession or under its control relating to subscribers and concerning such services. 2 The powers and procedures referred to in this Article shall be subject to Articles 14 and 15. 3 For the purposes of this Article, "subscriber data" means any information, whether in the form of computer data or in any other form, held by a service provider relating to subscribers to its services, other than traffic or content data,	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 9;** The public prosecutor, the investigating judge or the judicial police officers authorized in writing are authorized to order: To seize an information system in whole or in part or a computer medium including stored data that can help reveal the truth. If entry into the information system proves unnecessary or impossible to carry out, the data relating to the offense as well as those allowing their reading and understanding will be copied onto a computer medium so as to ensure authenticity and integrity of their content. To collect or record in real time data relating to telecommunications traffic using appropriate technical means. They are also authorized to access directly or with the assistance of experts any system or IT support and carry out an investigation in order to obtain stored data that can help reveal the truth.

from which it can be established: a the type of communication service used, the technical arrangements made for it and the period of service; b the identity, postal or geographical address and telephone number of the company. the subscriber's telephone number, and any other access number, data concerning invoicing and payment, available on the basis of a contract or service arrangement; c any other information relating to the location of the communication equipment, available on the basis of a contract or service arrangement.	The competent services of the Ministry of National Defense and the Ministry of the Interior ensure the seizure operation, its location and the process of access to information systems, data, stored information, software and all these materials relating to the two ministries, each according to its area of expertise.
Title 4 - Search and seizure of stored computer data	
Article 19 - Search and seizure of stored computer data Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to carry out searches or similar accesses: a a computer system or part thereof or computer data stored therein; and b a computer storage medium for storing computer data on its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that, where its authorities search or similarly access a specific computer system or part thereof pursuant to paragraph 1.a, and have reason to believe that the data sought is stored in another computer system or part thereof located in its territory, and that such data is lawfully accessible from or available to the original system, the said authorities are able to extend the search or similar access to the other system expeditiously. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 9;** The public prosecutor, the investigating judge or the judicial police officers authorized in writing are authorized to order: To seize an information system in whole or in part or a computer medium including stored data that can help reveal the truth. If entry into the information system proves unnecessary or impossible to carry out, the data relating to the offense as well as those allowing their reading and understanding will be copied onto a computer medium so as to ensure authenticity and integrity of their content. To collect or record in real time data relating to telecommunications traffic using appropriate technical means. They are also authorized to access directly or with the assistance of experts any system or IT support and carry out an investigation in order to obtain stored data that can help reveal the truth. The competent services of the Ministry of National Defense and the Ministry of the Interior ensure the seizure operation, its location and the process of access to information systems, data, stored information, software and all these materials relating to the two ministries, each according to its area of expertise.

seize or similarly obtain computer data accessed pursuant to paragraphs 1 or 2. Such measures shall include the following powers: a seizing or obtaining in a similar way a computer system or part thereof, or a computer storage medium; b make and keep a copy of this computer data; c preserve the integrity of relevant stored computer data; d make the data inaccessible or remove it from the computer system consulted. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person with knowledge of the functioning of the computer system or of the measures applied to protect computer data contained therein to provide all information reasonably necessary to enable the application of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 12 - 15;** **Article 12** – The authority responsible for the execution of judicial orders must keep a listed and initialed internal register, including the identity of the agents attached to it and who are involved in access, collection, interception and treatment, their qualities and their signatures, on a case by case basis. **Article 13** – The results of access, collection or interception operations and the attached technical data are transferred to the interested authorities identified in the relevant judicial order, with a view to their exploitation. **Article 14** – An inventory is made, as much as possible, in the presence of the accused, or the person in whose possession the seizure is found. A seizure report is drawn up. The seized objects are kept, depending on their nature and characteristics, in supports or containers which ensure their security and on which the data relating to the date and time of the seizure, and the number of the report must be noted. or the case. Necessary precautions are taken to maintain the authenticity and integrity of the input, including technical means to protect their content. **Article 15** – In the event of the impossibility of effective seizure of a computer system subject to the sovereignty of the Tunisian State, it is required, in order to preserve evidence of the offense, to use all appropriate means in order to prevent breach or access to stored data
Title 5 - Real-time collection of computer data	
Article 20 - Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities:	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 10;** In cases where the necessity of the investigation requires it, the public prosecutor or the investigating judge may resort to the interception of suspects'

a to collect or record using technical means available on its territory, and b to oblige a service provider, within the framework of its existing technical capabilities: i to be collected or recorded using technical means available on its territory, or iii to assist the competent authorities in collecting or recording data, in real time, traffic data associated with specific communications transmitted on its territory by means of a computer system. 2 Where a Party, due to established principles of its internal legal order, cannot adopt the measures set out in paragraph 1.a, it may instead adopt such legislative and other measures as may be necessary to ensure the collection or recording in real time of traffic data associated with specific communications transmitted on its territory through the application of technical means existing on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to require a service provider to keep secret the fact that any of the powers provided for in this Article have been as well as any information on this subject. 4 The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.	communications, by virtue of a written and reasoned decision. In the same cases, upon reasoned report from the judicial police officer authorized to report offenses, the interception of suspects' communications may also take place, pursuant to a written and reasoned decision from the public prosecutor. or the investigating judge. The interception of communications includes obtaining access data, listening, or accessing their content, their reproduction, their recording using appropriate technical means and by resorting, if necessary, to competent structures, each according to the type of service they provide. Access data is data that makes it possible to identify the type of service, the source of the communication, its destination, its transmission network, the time, date, volume and duration of the communication. **Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 11;** As part of their obligations to ensure the requirements of public safety, national defense and the provisions of the judiciary, communication service providers must respond to requests from the services responsible for receiving and executing communications. court orders relating to access to data stored in an information system or to the collection of data from the flow of communications or their interception related to the accomplishment of their tasks. The authority responsible for the execution of judicial orders is required to draw up a report of the access or collection or interception or processing operations that it has carried out. This report must include the following information: The mechanism of the order for which it is responsible for its execution. The authority that ordered the technical processing. The technical arrangements she made to fulfill the order and the type of assistance she received from service providers. The technical measures taken to preserve the data collected and ensure their authenticity and integrity at all stages. The date and time of the start and end of operations. The report must be accompanied by the results of the access, collection, interception or processing operations as well as by the necessary programs and

	technical data which ensure their conservation and exploitation without affecting their authenticity and their quality or integrity.
Article 21 - Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities with respect to a range of serious offences to be defined in domestic law: a to be collected or recorded using technical means available on its territory, and b to oblige a service provider, within the scope of its technical capabilities: i to be collected or recorded using technical means available on its territory, or ii to assist the competent authorities in collecting or recording data, in real time, data relating to the content of specific communications on its territory, transmitted by means of a computer system. 2 Where a Party, by reason of the principles established in its domestic legal order, cannot adopt the measures set out in paragraph 1.a, it may instead adopt such legislative and other measures as may be necessary to ensure the collection or recording in real time of content data relating to specific communications transmitted in its territory through the application of technical means existing in that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to require a service provider to keep secret the fact that any of the powers provided for in this Article have been exercised and any information relating thereto. The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 9;** In cases where the necessity of the investigation requires it, the public prosecutor or the investigating judge may resort to the interception of suspects' communications, by virtue of a written and reasoned decision. In the same cases, upon reasoned report from the judicial police officer authorized to report offenses, the interception of suspects' communications may also take place, pursuant to a written and reasoned decision from the public prosecutor. or the investigating judge. The interception of communications includes obtaining access data, listening, or accessing their content, their reproduction, their recording using appropriate technical means and by resorting, if necessary, to competent structures, each according to the type of service they provide. Access data is data that makes it possible to identify the type of service, the source of the communication, its destination, its transmission network, the time, date, volume and duration of the communication. **Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 11;** As part of their obligations to ensure the requirements of public safety, national defense and the provisions of the judiciary, communication service providers must respond to requests from the services responsible for receiving and executing communications. court orders relating to access to data stored in an information system or to the collection of data from the flow of communications or their interception related to the accomplishment of their tasks. The authority responsible for the execution of judicial orders is required to draw up a report of the access or collection or interception or processing operations that it has carried out. This report must include the following information: The mechanism of the order for which it is responsible for its execution.

	The authority that ordered the technical processing. The technical arrangements she made to fulfill the order and the type of assistance she received from service providers. The technical measures taken to preserve the data collected and ensure their authenticity and integrity at all stages. The date and time of the start and end of operations. The report must be accompanied by the results of the access, collection, interception or processing operations as well as by the necessary programs and technical data which ensure their conservation and exploitation without affecting their authenticity and their quality or integrity.
Section 3 - Competence	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish its jurisdiction over any criminal offence established in accordance with Articles 2 to 11 of this Convention, when the offence is committed: a on its territory; or b on board a vessel flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence does not fall within the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply, or to apply only in specific cases or conditions, the jurisdictional rules set out in paragraphs 1.b to 1.d of this article or in any part of those paragraphs. 3 Each Party shall adopt such measures as may be necessary to establish its jurisdiction over any of the offences referred to in Article 24, paragraph 1, of this Convention, where the alleged	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 34;** Subject to international or bilateral conventions ratified by the Tunisian Republic, the competent Tunisian courts may prosecute and judge anyone who has committed, outside Tunisian territory, one of the offenses provided for by this decree-law, and this, in cases following: • If the offense is committed by a Tunisian citizen, • If the offense is committed against Tunisian parties or interests, • If the offense is committed against foreign persons or interests by a foreigner or stateless person whose habitual residence is on Tunisian territory, or by a foreigner or stateless person found on Tunisian territory and not meeting the legal conditions extradition. The extradition will take place according to the procedures in force in accordance with the code of criminal procedure, taking into account the agreements concluded for this purpose.

offender is present in its territory and cannot be extradited to another Party solely on the basis of his or her nationality, following a request for extradition. 4 This Convention shall not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. Where more than one Party claims jurisdiction over an alleged offence referred to in this Convention, the Parties concerned shall, where appropriate, consult with a view to determining the Party best able to prosecute.	
Chapter III - International cooperation	
Section 1 - General principles ***Title 1 - General principles relating to international cooperation***	
Article 24 – Extradition 1 a This article shall apply to extradition between the Parties for the criminal offences defined in accordance with Articles 2 to 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is required on the basis of an extradition treaty as applicable between two or more parties, including the European Convention on Extradition (ETS No. 24), or an arrangement based on uniform or reciprocal legislation, the minimum penalty provided for in that treaty or arrangement shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty that may be concluded between or among them. Where a Party makes extradition conditional on the existence	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 34;** Subject to international or bilateral conventions ratified by the Tunisian Republic, the competent Tunisian courts may prosecute and judge anyone who has committed, outside Tunisian territory, one of the offenses provided for by this decree-law, and this, in cases following: • If the offense is committed by a Tunisian citizen, • If the offense is committed against Tunisian parties or interests, • If the offense is committed against foreign persons or interests by a foreigner or stateless person whose habitual residence is on Tunisian territory, or by a foreigner or stateless person found on Tunisian territory and not meeting the legal conditions extradition. The extradition will take place according to the procedures in force in accordance with the code of criminal procedure, taking into account the agreements concluded for this purpose.

of a treaty and receives a request for extradition from another Party with which it has not concluded an extradition treaty, it may consider this Convention as the legal basis for extradition in respect of any criminal offence mentioned in paragraph 1 of this article. 4 Parties which do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions laid down by the domestic law of the requested Party or by extradition treaties in force, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought or because the requested Party considers itself competent in respect of that offence, the requested Party shall, at the request of the requesting Party, submit the case to its competent authorities for the purpose of prosecution, and shall report in due course to the requesting Party on the outcome of the case. The authorities in question shall take their decision and conduct the investigation and proceedings in the same way as for any other offence of a comparable nature, in accordance with the legislation of that Party. 7 a Each Party shall communicate to the Secretary General of the Council of Europe, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, the name and address of each authority responsible for sending or receiving a request for extradition or provisional arrest, in the absence of a treaty. b The Secretary General of the Council of Europe shall establish and keep up to date a register of the authorities so designated by the Parties. Each Party shall at all times ensure the accuracy of the data contained in the register.	**NOTE – Tunisia has extradition treaties with a limited number of countries**. The number of current treaties with parties to the Budapest Cybercrime Convention is not known.

Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another the widest measure of mutual assistance for the purposes of investigations or proceedings concerning criminal offences relating to computer systems and data, or for the purpose of obtaining evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to fulfil the obligations set out in Articles 3 articles 27 to 35. Each Party may, in case of urgency, make a request for mutual assistance or related communications by expeditious means of communication, such as facsimile or electronic mail, provided that such means offer adequate conditions of security and authentication (including, if necessary, encryption), with subsequent official confirmation if required by the requested State. The requested State accepts the request and responds by any of these rapid means of communication. 4 Unless expressly provided otherwise in the articles of this chapter, mutual assistance shall be subject to the conditions laid down by the domestic law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse cooperation. The requested Party shall not exercise its right to refuse mutual assistance concerning the offences referred to in Articles 2 to 11 solely on the ground that the request concerns an offence which it considers to be of a fiscal nature. 5 Where, in accordance with the provisions of this chapter, the requested Party is authorised to make mutual assistance conditional on the existence of dual criminality, this condition shall be considered satisfied if the conduct constituting the offence in respect of which mutual assistance is requested is classified as a criminal offence under its domestic law, whether or not the domestic law classifies the offence in the same category of offences or designates it by the same terminology as the law of the requested Party.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 35;** The specialized authorities ensure to facilitate cooperation with their counterparts in foreign countries within the framework of ratified international, regional and bilateral conventions, and according to the principle of reciprocity through the exchange of information and data with precision and speed. required, with a view to ensuring early warning of offenses relating to information and communication systems, preventing them, avoiding their commission, helping to investigate them and prosecuting their perpetrators. The cooperation provided for in the first paragraph of this article is dependent on the extent of the commitment of the foreign State concerned to preserve the confidentiality of the information transmitted therein and on its commitment not to transmit it to a third party or exploit them for purposes other than the fight against offenses governed by this decree-law and their repression.

Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, communicate to another Party information obtained in the course of its own investigations where it considers that this could assist the receiving Party in initiating or carrying out investigations or proceedings in respect of criminal offences established in accordance with this Convention, or where such information could lead to a request for co-operation by that Party under this chapter. 2 Before communicating such information, the Party providing it may request that it be kept confidential or that it be used only under certain conditions. If the receiving Party cannot comply with such a request, it shall inform the other Party, which shall then determine whether the information in question should nevertheless be provided. If the receiving Party accepts the information on the prescribed terms, it will be bound by them.	**Tunisia is not currently a party to the BCC on cybercrime – no legal framework is identified for sharing spontaneous information.**
Title 4 - Procedures relating to requests for mutual assistance in the absence of applicable international agreements	
Article 27 – Procedures for requests for mutual assistance in the absence of applicable international agreements 1 In the absence of a mutual assistance treaty or arrangement based on uniform or reciprocal legislation in force between the requesting Party and the requested Party, the provisions of paragraphs 2 to 9 of this article shall apply. They shall not apply where such a treaty, arrangement or legislation exists, unless the Parties concerned decide to apply all or part of the remainder of this article instead. 2 a Each Party shall designate one or more central authorities to send or respond to requests for mutual assistance, to execute them or to transmit them to the authorities competent to execute them; b The central authorities communicate directly with each other; c Each Party shall, at the time of signature or when	Tunisia has a Central Authority within the MOJ in Tunis - https://www.hcch.net/en/states/authorities/details3/?aid=1100

depositing its instruments of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in application of this paragraph; d The Secretary General of the Council of Europe shall establish and keep up to date a register of central authorities designated by the Parties. Each Party shall at all times ensure the accuracy of the information contained in the register. 3 Requests for mutual assistance under this article shall be executed in accordance with the procedure specified by the requesting Party, except where it is incompatible with the law of the requested Party. 4 In addition to the conditions or grounds for refusal laid down in Article 25(4), mutual assistance may be refused by the requested Party: a if the request concerns an offence which the requested Party considers to be of a political nature or related to an offence of a political nature; or b if the requested Party considers that compliance with the request would be likely to prejudice its sovereignty, security, public policy or other essential interests. 5 The requested Party may postpone execution of the request if this would might prejudice investigations or proceedings conducted by its authorities 6 Before refusing or postponing its cooperation, the requested Party shall consider, after consulting the requesting Party where appropriate, whether the request may be granted in part or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the action it intends to take on the request for mutual assistance. It shall give reasons for any refusal to comply or for any postponement of the request. The requested Party shall also inform the requesting Party of any reason which renders the execution of mutual assistance impossible or is likely to delay it significantly.	

8 The requesting Party may request that the requested Party keep confidential the fact and purpose of any request made under this chapter, except to the extent necessary to comply with the request. If the requested Party is unable to comply with such a request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In urgent cases, the judicial authorities of the requesting Party may send requests for mutual assistance or communications relating thereto directly to their counterparts in the requested Party. In such a case, a copy shall be sent simultaneously to the central authorities of the requested Party via the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organization (Interpol). c Where a request has been made pursuant to subparagraph a. of this Article and the Authority is not competent to deal with it, it shall forward the request to the competent national authority and inform the requesting Party directly. d Requests or communications made pursuant to this paragraph which do not involve coercive measures may be transmitted directly by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may inform the Secretary General of the Council of Europe, at the time of signing or depositing its instrument of accession, ratification, acceptance, approval or accession, that, for reasons of efficiency, requests made under this paragraph should be addressed to its central authority.	
Article 28 - Confidentiality and restrictions on use 1 In the absence of a mutual assistance treaty or arrangement based on uniform or reciprocal legislation in force between the requesting Party and the requested Party, the provisions of this article shall apply. They shall not apply where	**Tunisia is not currently a party to the BCC on cybercrime – no legal framework is identified for MLAT regarding to confidentiality and limitation on use in international requests.**

such a treaty, arrangement or legislation exists, unless the Parties concerned decide to apply all or part of this article instead. 2 The requested Party may make the provision of information or material in response to a request conditional: a on condition that they remain confidential where the request for mutual assistance could not be complied with in the absence of this condition; or b provided that they are not used for the purposes of investigations or proceedings other than those indicated in the request. 3 If the requesting Party cannot meet one of the conditions set out in paragraph 2, it shall promptly inform the requested Party, which shall then determine whether the information should nevertheless be provided. If the requesting Party accepts the condition, it shall be bound by it. 4 Any Party providing information or material subject to a condition set out in paragraph 2 may require the other Party to provide details, in relation to that condition, of the use made of this information or material.	
Section 2- Specific provisions	
Title 1 - Mutual assistance in respect of interim measures	
Article 29 - Rapid preservation of stored computer data 1 A Party may request another Party to order or otherwise require the expeditious preservation of data stored by means of a computer system in the territory of that other Party, in respect of which the requesting Party intends to submit a request for mutual assistance to search or similarly access, seize or similarly obtain, or disclose such data. 2 A request for conservation made pursuant to paragraph 1 must specify: a the authority requesting conservation; b the offence under investigation or the subject of criminal proceedings and a brief statement of the facts	**Tunisia is not currently a party to the BCC on cybercrime – no legal framework is identified for expedited preservation or stored computer data.**

relating thereto; c the stored computer data to be retained and the nature of its link with the offence; d all available information enabling the custodian of the stored computer data or the location of the computer system to be identified; e the need for the conservation measure; and f the fact that the Party intends to submit a request for mutual assistance with a view to searching or accessing by similar means, seizing or obtaining by similar means, or disclosing stored computer data. 3 After receiving a request from another Party, the requested Party shall take all appropriate measures to preserve the specified data without delay, in accordance with its domestic law. In order to comply with such a request, dual criminality is not required as a precondition for preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance in searching or similarly accessing, seizing or similarly obtaining or disclosing stored data may, for offences other than those established in accordance with Articles 2 to 11 of this Convention, reserve the right to refuse the request for preservation under this article where it has reason to believe that, at the time of disclosure, the dual criminality requirement cannot be met. 5 In addition, a conservation request can only be refused: a if the request concerns an offence which the requested Party considers to be of a political nature or related to an offence of a political nature; or b if the requested Party considers that compliance with the request would be likely to prejudice its sovereignty, security, public policy or other essential interests. 6 Where the requested Party considers that simple preservation will not be sufficient to ensure the future availability of the data, or will compromise the confidentiality of, or otherwise adversely affect, the requesting Party's investigation, it shall promptly inform the requesting Party, which shall decide to c whether the request should nevertheless be carried	

out. 7 Any preservation made in response to a request referred to in paragraph 1 shall be for a period of at least sixty days to allow the requesting Party to submit a request for search or similar access, seizure or similar obtaining, or disclosure of the data. Following receipt of such a request, the data shall continue to be retained pending a decision on the request.	
Article 30 – Prompt disclosure of retained data 1 Where, in executing a request for preservation of traffic data relating to a specific communication made pursuant to Article 29, the requested Party discovers that a service provider in another State was involved in the transmission of that communication, the requested Party shall promptly disclose to the requesting Party a sufficient amount of traffic data for the purpose of identifying that service provider and the channel through which the communication was transmitted. 2 Disclosure of traffic data pursuant to paragraph 1 may be refused only: a if the request concerns an offence which the requested Party considers to be of a political nature or related to an offence of a political nature; or if it considers that granting the request would be likely to prejudice its sovereignty, security, public order or other essential interests.	**Tunisia is not currently a party to the BCC on cybercrime – no legal framework is identified for expedited disclosure of preserved traffic data.**
Title 2 - Mutual assistance regarding investigative powers	
Article 31 – Mutual assistance concerning access to stored data 1 A Party may request another Party to search or similarly access, seize or similarly obtain, disclose data stored by means of a computer system in the territory of that other Party, including data retained in accordance with Article 29. 2 The requested Party shall comply with the request by applying the international instruments, arrangements and legislation referred to in Article 23 and by complying with the relevant provisions of this chapter. a The request must be satisfied as quickly as possible within the following cases: there is reason to believe that the	**Tunisia is not currently a party to the BCC on cybercrime – no legal framework is identified for mutual assistance**

relevant data are particularly sensitive to the risk of loss or modification; or b the instruments, arrangements and legislation referred to at paragraph 2 provide for rapid cooperation.	
Article 32 – Cross-border access to stored data with consent or when publicly accessible A Party may, without the authorisation of another Party : a access publicly available (open source) stored computer data, regardless of the geographical location of that data; or b access or receive, by means of a computer system located in its territory, computer data stored in another State, if the Party obtains the lawful and voluntary consent of the person lawfully entitled to disclose such data to it by means of that system. computer system.	**Tunisia is not currently a party to the BCC on cybercrime – no legal framework is identified for mutual assistance**
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall afford each other mutual assistance in the real-time collection of traffic data associated with specified communications in their territory, transmitted by means of a computer system. Subject to the provisions of paragraph 2, such mutual assistance shall be governed by the conditions and procedures laid down in national law. 2 Each Party shall afford such assistance at least in respect of criminal offences for which real-time collection of traffic data would be available in a similar case at the level of in-house.	**Tunisia is not currently a party to the BCC on cybercrime – no legal framework is identified for mutual assistance**
Article 34 – Mutual assistance regarding the interception of content data The Parties shall afford each other mutual assistance, to the extent permitted by their applicable domestic laws and treaties, in the collection or recording in real time of data relating to the content of specific communications. transmitted via a computer system.	**Tunisia is not currently a party to the BCC on cybercrime – no legal framework is identified for mutual assistance**

Title 3 - 24/7 Network	
Article 35 - 24/7 Network 1 Each Party shall designate a point of contact which may be contacted 24 hours a day, seven days a week, in order to provide immediate assistance for investigations concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include the facilitation, or, where domestic law and practice permit, the direct application of the following measures: has provided technical advice; b data retention, in accordance with Articles 29 and 30; c gathering evidence, providing legal information and locating suspects. 2 a The point of contact of a Party shall have the means to correspond with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not under the authority or authorities of that Party responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that it has trained and equipped staff to facilitate the operation of the network.	**Tunisia Decree Law 54 – 13 of 2022 relating to Cybercrime states in article 35;** The specialized authorities ensure to facilitate cooperation with their counterparts in foreign countries within the framework of ratified international, regional and bilateral conventions, and according to the principle of reciprocity through the exchange of information and data with precision and speed. required, with a view to ensuring early warning of offenses relating to information and communication systems, preventing them, avoiding their commission, helping to investigate them and prosecuting their perpetrators. The cooperation provided for in the first paragraph of this article is dependent on the extent of the commitment of the foreign State concerned to preserve the confidentiality of the information transmitted therein and on its commitment not to transmit it to a third party or exploit them for purposes other than the fight against offenses governed by this decree-law and their repression. NOTE - Tunisia is not a party to the Budapest Convention on Cybercrime but does have a dedicated 24/7 point of contact in the Ministry of Interior for the G7 Network and interactions with national and multi-national service providers. As of November 2023, further legislation was being drafted to compliment this position.
Article 42 - Reservations By written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation or reservations provided for in Article 4, (2), Article 6 (3), Article 9 (4), Article 10 (3), Article 11 (3), Article 14 (3), Article 22 (2), Article 29 (4) and Article 41 (1). No other reservations may be made.	