Last updated on 30th November 2023

Cybercrime legislation - legislative profile

ALGERIA

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.	**Law n°09-04 of August 5, 2009, article 2. Terminology** For the purposes of this law, we mean: a - Offenses related to information and communication technologies, offenses affecting automated data processing systems, data as defined by the penal code as well as any other offense committed or whose commission is facilitated by a computer system or a electronic communication system. b - Computer system: any isolated device or set of devices interconnected or related which ensures or of which one or more elements ensure, in execution of a program, automated data processing. c - Computer data: any representation of facts, information or concepts in a form which lends itself to computer processing including a program capable of causing a computer system to execute a function. d - Service providers: 1 - any public or private entity which offers users of its services the possibility of communicating by means of a computer system and/or a telecommunications system; 2 - and any other entity processing or storing computer data for this communication service or its users. e - Data relating to traffic: any data relating to a communication

	passing through a computer system, produced by the latter as as part of the communication chain, indicating the origin, destination, the route, time, date, size and duration of the communication as well as the type of service. f - Electronic communications: any transmission, emission or reception signs, signals, writings, images, sounds or information ofany nature, by any electronic means.
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.	**Penal Code, article 394 bis (new)** Is punishable by a prison sentence of three (3) months to one (1) year and one fine of fifty thousand (50,000) DA to one hundred thousand (100,000) DA, anyone accesses or maintains itself, fraudulently, in all or part of a security system automated data processing or attempts to do so. The penalty is brought to double, when this resulted in either the deletion or modification of data contained in the system. When this resulted in an alteration of the operation of this system, the penalty is six (6) months to two (2) years of imprisonment and a fine of fifty thousand (50,000) DA to one hundred fifty thousand (150,000) DA
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.	**Penal Code, article 303 bis (new)** Is punishable by imprisonment of six (6) months to three (3) years and a fine from fifty thousand (50,000) DA to three hundred thousand (300,000) DA, anyone, at by means of any process, intentionally infringes on the privacy of the private life of others: 1 - by capturing, recording, or transmitting without authorization or consent of their author, communications, words spoken to private or confidential title. 2 - taking, recording, or transmitting without authorization or consent of the latter, the image of a person found in a private place. Attempting the offense provided for in this article is punishable by the same penalties that the offense has been completed. The victim's pardon puts an end to criminal proceedings.

	Penal Code, article 303 bis 1 (new) Any person who keeps, brings, or lets it become known to the public or a third party or uses in any manner whatsoever, any recording, image or document obtained, using one of the acts provided for in Article 303 bis of this law. If the offense provided for in the preceding paragraph is committed through the press, the special provisions provided for by the relevant laws to determine the responsible persons are applicable. Attempting the offense provided for in this article is punishable by the same penalties that the offense has been completed. The victim's pardon puts an end to criminal proceedings.
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.	**Penal Code, article 394 bis (new)** Is punishable by a prison sentence of three (3) months to one (1) year and one fine of fifty thousand (50,000) DA to one hundred thousand (100,000) DA, anyone accesses or maintains itself, fraudulently, in all or part of a security system automated data processing or attempts to do so. The penalty is brought to double, when this resulted in either the deletion or modification of data contained in the system. When this resulted in an alteration of the operation of this system, the penalty is six (6) months to two (2) years of imprisonment and a fine of fifty thousand (50,000) DA to one hundred fifty thousand (150,000) DA
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.	**Penal Code, article 394 bis (new)** Is punishable by a prison sentence of three (3) months to one (1) year and one fine of fifty thousand (50,000) DA to one hundred thousand (100,000) DA, anyone accesses or maintains itself, fraudulently, in all or part of a security system automated data processing or attempts to do so. The penalty is brought to double, when this resulted in either the deletion or modification of data contained in the system. When this resulted in an alteration of the operation of this system, the penalty is six (6) months to two (2) years of imprisonment and a fine of fifty thousand (50,000) DA to one hundred fifty thousand (150,000) DA
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	No legal framework identified.

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 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.	Algeria has an offence that creates a legal framework for forgery related to physical artefacts under Penal Code - Chapter 7 – Forgeries (non-specific provisions)Article 216 (amended). But no law or legal framework is identified for computer related forgery.
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;	No specific offence is identified for computer fraud, but the following law provides culpability for this article. **Penal Code - Chapter 3, Section 2** Fraud and issuance of checks without provision and Section 3 - Breach of trust

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.	(provisions not specific) Article 376. Whoever in bad faith misappropriates or dissipates to the detriment of owners, possessors or holders of effects, money, goods, notes, receipts, or any other writings containing or operating obligation or discharge, which were only given to him as rental, deposit, mandate, collateral, loan for use, or for salaried or self-employed work, at the responsible for returning or representing them, or making use of them determined, is guilty of breach of trust and punished with imprisonment of three (3) months to three (3) years and a fine of five hundred (500) to twenty thousand (20,000) DA. The culprit may, in addition, be punished for at least one (1) year and five (5) years at most the prohibition of one or more of the rights mentioned in article 14 and of the stay ban.
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; 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;	**Penal Code, article 333 bis** Is punishable by imprisonment of two (2) months to two (2) years and one fine of five hundred (500) to two thousand (2000) DA anyone who has manufactured, held, imported or caused to be imported with a view to trade, distribution, rental, display or exhibition, exhibits or attempts to expose to the eyes of the public, sold or attempted to sell, distributed or attempted to distribute, all printed matter, writings, drawings, posters, engravings, paintings, photographs, photographs, matrices, or reproductions, all objects contrary to decency. **Penal Code, article 333 bis 1 (new)** Is punishable by imprisonment of five (5) years to ten (10) years and a fine from 500,000 DA to 1,000,000 DA whoever represents, by whatever means that is, a minor under eighteen (18) years of age engaging in activities explicit sexual acts, real or simulated, or depicts the sexual organs of a minor, for primarily sexual purposes, or produces, distributes, the dissemination, propagation, import, export, offer, sale or possession of pornographic materials depicting minors.

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.	In the event of conviction, the court orders the confiscation of the means which were used in the commission of the offense as well as the property obtained in a manner illicit, subject to the rights of third parties in good faith. **Penal Code, article 334. (amended)** Is punishable by imprisonment of five (5) to ten (10) years, any attack on modesty consumed or attempted without violence, on the person of a minor aged 16 years of either sex. Indecent assault is punishable by imprisonment for a period of five (5) to ten (10) years when committed by any ascendant, on the person of a minor, even over the age of 16 years old, but not emancipated by marriage.
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, 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.	**Ordinance No. 03-05 of July 19, 2003 relating to copyright and neighbouring rights, chapter II,** Section 151 Anyone who: — illicitly discloses a work or undermines the integrity of a work or a performance by a performer; — reproduces a work or service by any process whatsoever under form of counterfeit copies; — imports or exports counterfeit copies of a work or service; — sells counterfeit copies of a work or service; — rents or puts into circulation counterfeit copies of a work or service. Article 152 Anyone who violates protected rights is guilty of the offense of counterfeiting under this order, communicates the work or performance, by public representation or performance, sound or audiovisual broadcasting, cable television or any other means of transmitting signs carrying sounds or images or sounds or by any computer processing system. Section 153

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.	The person guilty of the offense of counterfeiting a work or a service, such as provided for in articles 151 and 152 above is punishable by imprisonment of six (6)months to three (3) years and a fine of five hundred thousand (500,000 DA) to one million (1,000,000 DA) of dinars whether the publication takes place in Algeria orthe foreigner. Article 154 Is guilty of the offense provided for in article 151 of this ordinance and is liable the penalty provided for in article 153 above whoever contributes, by his action or the means in its possession, to infringe copyright or any holder of neighboring rights. Article 155 Is guilty of the offense of counterfeiting and punished with the same penalty provided for in article 153 above, anyone, in violation of recognized rights, deliberately refuses to pay to the author or any other holder of related rights the remuneration due under the rights provided for by this order. Article 156 In the event of a repeat offense, the penalty provided for in article 153 of this order is increased to double. The competent court may, in addition, order the temporary closure, for a period not exceeding six (6) months, of the establishment operated by the counterfeiter or his accomplice, or where applicable, permanent closure.
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	**Penal Code, article 394 (new)** Attempting the offenses provided for in this section is punishable by the same penalties.provided for the offense itself **Law No. 08-01 of January 23, 2008** supplementing Law No. 83-11 of July 2, 1983 relating to social insurance: Article 4 (article 93 quinquiès of the law of July 2, 1983) [...] Attempted offences cited in paragraphs 1 and 2 are punishable by the same penalty above ".

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 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.	**Penal Code, articles 42-46** Article 42 (amended) Are considered as accomplices to an offense those who, without participation directly to this offense, have, with knowledge, assisted by any means or assisted the author or authors of the action in the facts which prepared it or facilitated, or who have consumed it. Section 43 An accomplice is considered to be someone who, knowing their criminal conduct, usually provided housing, place of retreat or meetings for one or more criminals carrying out robbery or violence against the security of the State, public peace, people or property. Article 44 The accomplice of a crime or misdemeanor is punishable by the penalty punishing this crime or offense. Personal circumstances resulting in aggravation, attenuation or exemption from penalty only have effect with regard to the single participant to whom they apply. The objective circumstances, inherent to the offense, which aggravate or reduce the punishment of those who participated in this offense, have effect on their charge or in their favor, depending on whether they were aware of it or not. Complicity is never punishable in criminal matters. Article 45 The one who determined a person, not punishable due to a condition or of a personal capacity, to commit an offence, is liable to the penalties repressing the offense. Article 46

	When the proposed offense will not have been committed by the sole act of the voluntary abstention of the person who was to commit it, the instigator will incur nevertheless the penalties provided for this offence.
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.	**Penal Code, article 51 bis (new)** The legal entity, excluding the State, local authorities and legal entities under public law, is criminally liable, when the law so provides, for offences committed, on its behalf, by its organsation or legal representatives. The criminal liability of the legal person does not exclude that of the natural person author or accomplice of the same acts. **Penal Code, article 394 sixth (new)** The legal person who has committed an offense provided for in this section is punishable by a fine equivalent to five (5) times the maximum fine intended for the natural person
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	**Article 394 septiès (new)** Anyone who participates in a group formed or in an agreement established with a view to the preparation, characterized by one or more material facts, of one or more several of the offenses provided for in this section are punishable by penalties provided for the offense itself. **Penal Code, article 394 octiès (new)**

pursuant to Article 12 are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	Without prejudice to the rights of third parties in good faith, confiscation will be carried out instruments, programs and means used in the commission of the offense as well as the closure of the sites, the subject of one of the offences provided for in this section, and premises and places of operation in the case where the owner is informed. **Penal Code, article 18 bis (amended)** The penalties incurred by the legal entity in criminal and other matters are : 1- The fine whose rate is one (1) to five (5) times the maximum fine provided for natural persons, by the law which punishes the offense. 2 - One or more of the following additional penalties: - the dissolution of the legal entity; - the closure of the establishment or one of its annexes for a period which cannot exceed five (5) years; **-** exclusion from public contracts for a period which cannot exceed five (5) years; - the ban, permanently or for a period which cannot exceed five (5) years, to exercise directly or indirectly, one or more activities professional or social; - confiscation of the thing which was used to commit the offense or of the thing which is the product; - the display and dissemination of the judgment of conviction; - placement, for a period which cannot exceed five (5) years, under judicial supervision for the exercise of the activity
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 u s i n g 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 i n 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,	In the Algerian legal framework there are many guarantees that have been implemented, even if weaknesses can still be observed. In addition to a clearer definition, indicated above, of the guiding principles of

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.	investigation and criminal trial, three main texts reaffirm certain fundamental rights by specifying their scope: **Organic law No. 12-05 of January 12, 2012** relating to information, having for the purpose of establishing the principles and rules for the exercise of the right to information and freedom of the press. **Law No. 17-07 of March 27, 2017** modifying and supplementing Ordinance No. 66-155 of June 8, 1966 relating to the Code of Criminal Procedure. This law reaffirms the principles of legality, fair trial and respect for dignity and human rights, consequently specifies the principles of criminal procedure, provides details on public action, police missions, judicial actions, and the controls to which it is subject, the release of defendants, the judgment of the failings of the judicial police officers in the exercise of their functions, the skills and composition of courts of first and second instance in matters of judgment crimes and other related offenses, the procedure before these jurisdictions. **Organic law No. 17-06 of March 27, 2017** amending organic law No. 05-11 of July 17, 2005 relating to the judicial organization, mainly to clarify the existence of a double degree of jurisdiction (following opinion no. 01/A.L.O/CC/17 of March 16, 2017 relating to the control of compliance with the law organic law amending organic law No. 05-11 of July 17, 2005 relating to judicial organization to the Constitution). Furthermore, the Constitution revised in March 2016 expressly guarantees different rights and freedoms including the following: • Equality before the law "without distinction of race, sex, opinion or any other personal or social condition or circumstance" (article 32). • "Fundamental freedoms and human and citizen rights" (article 38). • Freedom of conscience and freedom of opinion, the exercise of religion being guaranteed in compliance with the law (article 39). • Freedom of investment and trade (article 43). • Freedom of intellectual, artistic, and scientific creation, including copyright, academic freedom and freedom of research scientific (article 44). • The right to education (article 65) and culture (article 45).

	• The private life and honor of the citizen, including "the secret of private correspondence and communication, in all their forms", it being specified that "no infringement of these rights is tolerated without reasoned requisition of the judicial authority", the law punishing "any violation of this provision" (article 46). • The protection of individuals in the processing of data personal character, which is "a fundamental right" (article 46). • The inviolability of the home, the search being able to "take place only on written order emanating from the competent judicial authority" (article 47). • Freedoms of expression, association and assembly (article 48). • "Freedom of the written, audiovisual and network press information", which cannot be "restricted by any form of censorship prior ". The "dissemination of information, ideas, images and opinions in complete freedom are guaranteed within the framework of the law and respect for constants and religious, moral and cultural values of the Nation", but the "press offense cannot be punished by a privative sentence of freedom" (article 50). The presumption of innocence and the right to a fair trial (article 56). • The legality of offenses and penalties (article 58). • Physical freedom (article 59), the Constitution determining the limits of custody and the fundamental rights of those in custody (article 60). • The State's right to compensation in the event of a judicial error (article 61). • The rights of children, protected by "the family, society and the State", the violence against children being punished by law (article 72). • The right to defense (article 169) and protection of the lawyer against any form of pressure (article 170). As in the framework of the previous Constitution, the legislative power legislates in matters of fundamental rights and the judiciary is guarantor of safeguarding these rights. The 2016 Constitution also strengthens the rights of Parliament, in particular of the parliamentary opposition which enjoys notably "effective participation" in legislative work and the control of government action and the right to refer the matter to the Council constitutional in accordance with the

	Constitution (article 114). The Constitution of 2016 also strengthens the independence of the judiciary, particularly in affirming the irremovability of the judges of the seat under the conditions established by the status of the judiciary (article 166). However, the Superior Council of the judiciary (which decides on the appointment and development of the careers of magistrates - article 174) remains chaired by the President of the Republic (article 173). It should be noted that Order No. 15-02 of July 23, 2015 modifying and supplementing the penal code deprives of double degree of jurisdiction the correctional and contraventional judgments which did not impose a sentence imprisonment and, for misdemeanors, having imposed a fine not exceeding certain amounts (new article 416 of the procedural code criminal, p. 36 of the law1). Furthermore, if the powers and limits of investigative services are regulated, they can still seem disproportionate in certain respects. Notably : • In matters of interception of correspondence according to the Code of Procedure criminal law (see below, in relation to Article 21 of the Convention of Budapest), the authorization must "include all the elements allowing to identify the connections to be intercepted, the places of residence or others targeted and the offense which motivates the use of these measures as well as the duration of these here" and is given for 4 months renewable "according to the needs of the investigation or information under the same conditions of form and duration" (article 65 bis 7) by the public prosecutor or (in the event judicial information) by the investigating judge (article 65 bis 5: guarantees therefore exist but the supervision of an independent magistrate default). • These operations must not prejudice confidentiality professional, but "the revelation of offenses other than those mentioned in the magistrate's authorization does not constitute a cause of nullity of incidental proceedings" (article 65 bis 6, such a possibility seeming to exceed the principle of strict necessity of the interference). The articles 65 bis 9 and 10 provide guarantees in terms of transparency of interception

	(transcription in a report of operations interception and implementation of the necessary devices, mentioning start and end dates and times; description of conversations "useful for the manifestation of the truth"), but the shelf life of these elements as well as the way in which they are protected from access and illegitimate uses do not appear to be regulated. • Under the terms of law n°09-04 of August 5, 2004, surveillance operations electronic can be put in place "for the purposes of investigations and judicial information when it is difficult to achieve results interesting for current research without resorting to surveillance electronic" (article 4 c), allowing an extremely wide scope of application broad without limiting it to serious offenses.
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	**Article 12 - Obligations of internet service providers** In addition to the obligations provided for in article 11 above, access providers to the internet are required: a) to intervene, without delay, to remove the content to which they authorize access in the event of a violation of laws, store them or make them inaccessible as soon as they have become aware of it directly or indirectly; b) to put in place technical devices to limit accessibility to distributors containing information contrary to public order or good morals and inform subscribers thereof. **Penal Code, article 394 bis 8 (created by Law No. 16-02 of June 19, 2016)** Without prejudice to the administrative sanctions provided for by legislation and regulations in force, is punishable by imprisonment of one year to three (3) years and a fine of 2,000,000 DA to 10,000,000 DA, or one of these two penalties only, the internet service provider within the meaning of article 2 of Law No. 09-04 of 14 Chaâbane 1430 corresponding to August 5, 2009 relating to special rules relating to the prevention and fight against offenses linked to information and communication technologies, which despite its formal notice by the national body

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.	provided for by the law in question or the intervention of a court decision obliging him to do so: a) does not intervene, without delay, to remove, store or make inaccessible the data to which he authorizes access, when their content constitutes an infringement of criminal legislation, b) does not put in place technical devices allowing the removal, storage or make inaccessible the data containing the offenses provided for in paragraph (a) of this article."
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 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.	**Law No. 09-04 of August 5, 2009** CHAPTER IV Obligations of service providers Article 10 - Assistance to the authorities As part of the application of the provisions of this law, suppliers services are required to make available to the authorities responsible for judicial investigations the data that they are required to keep in under article 11 below. Under penalty of the sanctions provided for in the matter of violation of the secrecy of the investigation and instruction, service providers are required to keep the confidentiality of the operations they carry out at the request of investigators and the information relating to it. **Article 11 - Conservation of traffic data** Depending on the nature and types of services, service providers undertake to conserve : a) data allowing the identification of users of the service; b) data relating to communications terminal equipment used; c) the technical characteristics as well as the date, time and duration of every communication; d) data relating to additional services required or used and their suppliers; e) data enabling the identification of the recipient(s) of the communication as well as the addresses of the sites visited. For telephony activities, the operator keeps the data cited in paragraph (a) of this article and those allowing the identification and location and the origin of the communication. The retention period of the data cited in this article is set at one (1) year from the day of registration. Without prejudice to administrative sanctions arising from non-compliance with obligations provided for by this article, the criminal liability

	of persons physical and moral is committed when this has resulted in to obstruct the proper conduct of judicial investigations. The penalty incurred by the natural person is imprisonment of six (6) months to five (5) years and the fine of 50,000 DA to 500,000 DA. The legal entity is liable to a fine according to the terms provided by the penal code. The terms of application of paragraphs 1, 2 and 3 of this article are, as as necessary, specified by regulation.
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, 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;	**Law No. 09-04 of August 5, 2009** CHAPTER IV Obligations of service providers Article 10 - Assistance to the authorities As part of the application of the provisions of this law, suppliers services are required to make available to the authorities responsible for judicial investigations the data that they are required to keep in under article 11 below. Under penalty of the sanctions provided for in the matter of violation of the secrecy of the investigation and instruction, service providers are required to keep the confidentiality of the operations they carry out at the request of investigators and the information relating to it. **Law No. 09-04 of August 5, 2009** CHAPTER IV Obligations of service providers Article 10 - Assistance to the authorities As part of the application of the provisions of this law, suppliers services are required to provide assistance to the authorities responsible for judicial investigations for the collection or recording, in real time, of data relating to the content of communications and to put at their disposal

c any other information relating to the location of the communication equipment, available on the basis of a contract or service arrangement.	
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 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	**Law No. 09-04 of August 5, 2009** CHAPTER III - Rules of procedure Article 5 - Search of computer systems The competent judicial authorities as well as judicial police officers, acting within the framework of the code of criminal procedure and in the cases provided for by Article 4 above, may, for the purposes of search, access, including to distance : (a) to a computer system or part thereof and to the data computers stored there; (b) a computer storage system. When, in the case provided for by the paragraph (a) of this article, the authority carrying out the search has reasons to believe that the data sought is stored in another computer system and that this data is accessible from the system initial, it can quickly extend the search to the system in question or to part of it after prior information to the judicial authority competent. If it is previously proven that the data sought, accessible to means of the first system, are stored in another computer system located outside the national territory, they are obtained with the assistance of competent foreign authorities in accordance with relevant international agreements and following the principle of reciprocity. The authorities in charge of the search are empowered to requisition any person familiar with the operation of the computer system in question or the measures applied to protect the computer data that it contains, in order to assist them and provide them with all the information necessary to the accomplishment of their mission. **Article 6 - Computer data entry** When the authority carrying out the search discovers, in a system computer, stored data that is useful in researching violations or their perpetrators, and that the seizure of the entire system is not necessary, the data in question as well as those which are necessary to their understanding, are copied onto computer storage media capable of being seized and placed under seal under the conditions provided for by the code of criminal procedure.

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.	The authority carrying out the search and seizure must, in any event, ensure the integrity of the data of the computer system in question. However, it may use the technical means required to implement form or reconstitute this data with a view to making it usable for needs of the investigation, on the condition that this reconstruction or formatting data does not alter its content. **Article 7 - Seizure by prohibiting access to data** If, for technical reasons, the authority carrying out the search is found unable to carry out the seizure in accordance with article 6 above, it must use appropriate techniques to prevent access to data contained in the computer system or to copies of this data which are available to persons authorized to use this system. **Article 8 - Data seized with incriminated content** The authority having carried out the search may order the necessary measures to make data whose content constitutes an offense inaccessible, in particular by designating any qualified person to use the means techniques appropriate for this purpose. **Article 9 - Limits on the use of collected data** Under penalty of sanctions decreed by the legislation in force, the data obtained by means of the surveillance operations provided for in this law may be used for purposes other than surveys and judicial information.
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: 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	**Law No. 09-04 of August 5, 2009** CHAPTER IV Obligations of service providers Article 10 - Assistance to the authorities As part of the application of the provisions of this law, suppliers services are required to make available to the authorities responsible for judicial investigations the data that they are required to keep in under article 11 below. Under penalty of the sanctions provided for in the matter of violation of the secrecy of the investigation and instruction, service providers are required to keep the confidentiality of the operations they carry out at the request of investigators and the information relating to it.

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.	**Article 11 - Conservation of traffic data** Depending on the nature and types of services, service providers undertake to conserve : a) data allowing the identification of users of the service; b) data relating to communications terminal equipment used; c) the technical characteristics as well as the date, time and duration of every communication; d) data relating to additional services required or used and their suppliers; e) data enabling the identification of the recipient(s) of the communication as well as the addresses of the sites visited. For telephony activities, the operator keeps the data cited in paragraph (a) of this article and those allowing the identification and location and the origin of the communication. The retention period of the data cited in this article is set at one (1) year from the day of registration. Without prejudice to administrative sanctions arising from non-compliance with obligations provided for by this article, the criminal liability of persons physical and moral is committed when this has resulted in to obstruct the proper conduct of judicial investigations. The penalty incurred by the natural person is imprisonment of six (6) months to five (5) years and the fine of 50,000 DA to 500,000 DA. The legal entity is liable to a fine according to the terms provided by the penal code. The terms of application of paragraphs 1, 2 and 3 of this article are, as as necessary, specified by regulation.
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	**Code of Criminal Procedure, articles 65 (5) to 65 (10)** inserted by law No. 06-22 of December 20, 2006. Article 65a 5 If the needs of the flagrant investigation or the relative preliminary investigation offenses relating to drug trafficking, transnational organized crime, breach of automated data processing systems, money laundering money, terrorism and offenses relating to foreign exchange legislation as well as corruption offenses require it, the public prosecutor competent authority may authorize: • the interception of correspondence sent via telecommunications;

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.	• the establishment of a technical device aimed, without consent of the interested parties, the capture, fixation, transmission and the recording of words spoken by one or more people as private or confidential in private or public places, or the image of one or more several people in a private place. The authorization allows, for the implementation of the technical device, entry into any residential or other place, including outside hours provided for in article 47 of this law, without the knowledge or consent of the persons holding a right to these goods. The operations thus authorized must be carried out under the direct control of the competent public prosecutor. In the event that a judicial investigation is opened, this authorization is given by the investigating judge. The operations thus authorized take place under his direct control. **Law No. 09-04 of August 5, 2009** Article 3 - Scope of application In accordance with the rules provided for by the code of criminal procedure and by this law and subject to legal provisions guaranteeing the secrecy of correspondence and communications, it can be done, for imperatives of protection of public order or for the purposes of investigations or ongoing judicial investigations, the establishment of systems techniques for performing communications surveillance operations electronic, collection and real-time recording of their content as well as searches and seizures in a computer system. Article 65 bis 6 The operations referred to in article 65 bis 5 above are carried out without carrying prejudice to professional secrecy provided for in Article 45 of this law. The disclosure of offenses other than those mentioned in the authorization of the magistrate does not constitute a cause for nullity of the incidental proceedings". Article 65a 7 The authorizations provided for in article 65 bis 5 above must include all the elements making it possible to identify the connections to be intercepted, the

	places of residence or other targeted and the offense which motivates the use of these measures as well as their duration. These authorizations are given in writing for a maximum period of four (4) month, renewable according to the needs of the investigation or information in the same conditions of form and duration. Article 65a 8 The public prosecutor or the judicial police officer authorized by him, the investigating judge or the judicial police officer appointed by him, may require any qualified agent from a service, unit or public body or private sector responsible for telecommunications, with a view to taking charge of technical aspects of the operations mentioned in article 65 bis 5 above. **CHAPTER II Surveillance of electronic communications** Article 4 - Cases authorizing the use of electronic surveillance The surveillance operations provided for in Article 3 above may be carried out in the following cases: a) to prevent offenses classified as terrorist or subversive acts and offenses against state security. b) when there is information about a probable breach of a system IT representing a threat to public order, national defense, state institutions or the national economy; c) for the purposes of investigations and judicial information when it is difficult to achieve results of interest to current research without use electronic surveillance; d) in the context of the execution of requests for mutual legal assistance international. The surveillance operations mentioned above cannot be carried out only with written authorization from the competent judicial authority. When it comes to the case provided for in paragraph (a) of this article, the authorization is issued to judicial police officers reporting to the body referred to in article 13 below, by the Attorney General at the Court of Algiers, for a period of six (6) months renewable, on the basis of a report indicating the nature of the technical process used and the objectives it aims to achieve. Under penalty of the sanctions provided for by the penal code in matters of violation of privacy of others, the technical devices put in place for the purposes

	designated in paragraph of this article must be oriented, exclusively, towards the collection and recording of data relating to prevention and control against terrorist acts and attacks on state security. **CHAPTER IV Obligations of service providers** Article 10 - Assistance to the authorities As part of the application of the provisions of this law, suppliers services are required to provide assistance to the authorities responsible for judicial investigations for the collection or recording, in real time, of data relating to the content of communications and to put at their disposal provision of the data that they are required to keep under Article 11 below below. Under penalty of the sanctions provided for in violation of the secrecy of the investigation and instruction, service providers are required to keep the confidentiality of the operations they carry out at the request of investigators and the information relating to it.
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 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	Algeria has a robust legal framework that deals with extradition, which are detailed in Articles 614 to 713 of the Code of Criminal Procedure, which are applicable unless otherwise provided as a result of bi-lateral treaties or diplomatic/international conventions that have been ratified by Algeria. According to the Code of Criminal Procedure from 2021, Algerians cannot be extradited from Algeria. Extraditable offences are those punishable with at least two years of imprisonment. Reciprocity of legal frameworks are also expected from countries making the request for extradition.

offences in any extradition treaty that may be concluded between or among them. Where a Party makes extradition conditional on the existence 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.	

Article 25 – General principles relating to mutual assistance	**Law No. 09-04 of August 5, 2009**
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.	Section 15 As part of investigations or judicial information carried out for the observation of offenses included in the scope of application of the this law and the search for their authors, the competent authorities may resort to international mutual legal assistance to collect evidence under electronic form. In case of emergency, and subject to international conventions and the principle of reciprocity, requests for mutual legal assistance referred to in the preceding paragraph are admissible if they are formulated by rapid means of communication, such as fax or e-mail provided that these means offer sufficient security and authentication conditions. Article 17 - Exchange of information and precautionary measures. Requests for mutual assistance aimed at exchanging information or taking any precautionary measure are satisfied in accordance with the conventions relevant international agreements, bilateral agreements and in application of the principle of reciprocity. Article 18 - Restrictions on requests for international assistance Execution of the request for mutual assistance is refused if it is likely to risk an attack on national sovereignty or public order. The satisfaction of requests for mutual assistance may be subject to the condition of maintain the confidentiality of the information communicated or on the condition of do not use them for purposes other than those indicated in the application.

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.	**Algeria is not currently a party to the BCC on cybercrime – no legal framework is identified for sharing spontaneous information.** However, cooperation under mutual legal assistance is available under Law No. 09-04 of August 5, 2009 and Section 15 and Section 17
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	**Law No. 09-04 of August 5, 2009** Section 15 As part of investigations or judicial information carried out for the observation of offenses included in the scope of application of the this law and the search for their authors, the competent authorities may resort to international mutual legal assistance to collect evidence under electronic form. In case of emergency, and subject to international conventions and the principle of reciprocity, requests for mutual legal assistance referred to in the preceding paragraph are admissible if they are formulated by rapid means of communication, such as fax or e-mail provided that these means offer sufficient security and authentication conditions. Article 18 - Restrictions on requests for international assistance Execution of the request for mutual assistance is refused if it is likely to risk an attack on national sovereignty or public order. The satisfaction of requests for

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.	mutual assistance may be subject to the condition of maintain the confidentiality of the information communicated.

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	**Law No. 09-04 of August 5, 2009** Article 18 - Restrictions on requests for international assistance. Execution of the request for mutual assistance is refused if it is likely to risk an attack on national sovereignty or public order. The satisfaction of requests for

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.	mutual assistance may be subject to the condition of maintain the confidentiality of the information communicated.
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	**Algeria 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.	**Algeria 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	**Algeria 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.	**Algeria 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.	**Algeria 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.	**Law No. 09-04 of August 5, 2009** **CHAPTER II Surveillance of electronic communications** **Article 4 - Cases authorizing the use of electronic surveillance** The surveillance operations provided for in Article 3 above may be carried out in cases that include ICT crime and undertaken by the Algerian authorities under the context of the execution of requests for mutual legal assistance from

	international counterparts.
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.	Algeria is not party to the Budapest Convention on Cybercrime and does not have access to the 24/7 Network provided by countries that have signed and/or acceded to the convention. However, Algeria has legislation that allows for the participation in 24/7 Networks. **Law No. 09-04 of August 5, 2009** CHAPTER V National body for the prevention and fight against offenses related to information and communication technologies Article 13 - Creation of the body A national body for the prevention and fight against crime linked to information and communication technologies. The composition, organization and operating methods of the body are set by regulation. Article 14 - Missions of the body The body referred to in Article 13 above is responsible in particular for: a) the revitalization and coordination of prevention and control operations against crime linked to information and communication technologies communication; b) assistance from judicial authorities and judicial police services in in the fight against crime linked to information technology and communication, including through the collection of information and legal expertise; c) the exchange of information with its interfaces abroad for the purpose of bringing together all data useful for locating and identifying the authors of the offenses related to information and communication technologies.
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.	