COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Last updated on 20 November 2023

Cybercrime legislation - legislative profile

KINGDOM OF MOROCCO

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

Country :	**Kingdom of Morocco**
Signature of the Convention :	No
Ratification/Accession	Ratification on 29th June 2018. It came into force on 1st October 2018.
Article of the Budapest Convention on Cybercrime	• Penal Code of **1962 as amended and supplemented.** • Law No. 22-01 on Criminal Procedure promulgated on 3 October 2002, available only in Arabic. Participating in the provisions of Article 15 : • Constitution of 2011

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.	Moroccan law does not define subscriber information, traffic data, or content data.
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	**Penal Code, Articles 607-3 and 607-4** **Article 607-3** Fraudulent access to all or part of an automated data processing system is punishable by one to three months' imprisonment and a fine of 2,000 to 10,000 dirhams, or by one of these two penalties only.

connection with a computer system connected to another computer system.	The same penalty shall apply to any person who remains in all or part of an automated data processing system to which he has gained access by mistake and when he does not have the right to do so. The penalty is doubled when the result is either the deletion or modification of data contained in the automated data processing system, or an alteration in the operation of this system. **Article 607-4** Without prejudice to more severe criminal provisions, anyone who commits the acts provided for in the previous article against all or part of an automated data processing system supposed to contain information relating to the internal or external security of the State or secrets concerning the national economy shall be punished by six months to two years imprisonment and a fine of between 10,000 and 100,000 dirhams. Without prejudice to more severe penal provisions, the penalty is increased from two years' to five years' imprisonment and a fine of 100,000 to 200,000 dirhams where the acts punishable under the first paragraph of this article result in either the modification or deletion of data contained in the automated data processing system, or an alteration in the operation of that system, or where the said acts are committed by a civil servant or an employee in the course of or in connection with the performance of his duties, or where he facilitates the performance of such acts by another person.
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.	Law no. 24-96 on post and telecommunications promulgated on 7 August 1997 (amended), article 92 Will be punished by imprisonment of 3 months to 5 years and a fine of 5,000 to 100,000 dirhams any person authorised to provide an international express mail service or any agent employed by them who, in the performance of their duties, opens, diverts or destroys mail, violates the secrecy of correspondence or assists in carrying out these acts. The same penalties will apply to any person authorised to provide a telecommunications service and any employee of telecommunications network operators or telecommunications service providers who, in the course of his or her duties and

	outside the cases provided for by law, violates in any way whatsoever the confidentiality of correspondence emitted, transmitted or received by telecommunications or who has ordered or assisted in the performance of such acts. Will be punished by imprisonment of one month to one year and a fine of 5,000 to 100,000 dirhams or by one of these two penalties only, any person other than those mentioned in the two preceding paragraphs who has committed one of the acts punishable by the said paragraphs. In addition to the penalties provided for in paragraphs 1, 2 and 3 above, the offender is banned from exercising any activity or profession in the telecommunications or postal sectors or in connection with these sectors for a period of one to five years. Articles 115 and 116 Code of Criminal Procedure Article 448 Any person who, except in the cases provided for in article 232, in bad faith, opens or deletes letters or correspondence addressed to third parties, shall be punished by imprisonment of between one month and one year and a fine of between 1,080 and 500 dirhams or by one of these two penalties only. Article 232 Any public official, government agent, employee or servant of the postal service who opens, misappropriates or deletes letters entrusted to the post office, or who facilitates the opening, misappropriation or deletion of letters entrusted to the post office, shall be liable to prosecution. deletion69, is punishable by three months to five years' imprisonment and a fine of between 2,700 and 1,000 dirhams.
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.	**Criminal Code, article 607-6** The act of fraudulently introducing data into an automated data processing system or of damaging, deleting or fraudulently modifying the data contained therein, or the way in which it is processed or transmitted, is punishable by one to three years' imprisonment and by a fine of 10,000 to 500,000 euros. 200,000 dirham fine or one of these two penalties only. **Article 607-3 of the Criminal Code, third paragraph:** The penalty is doubled when the result is either the deletion or modification of data contained in the automated data processing

	system, or an alteration in the operation of this system. **Article 607-4 of the Criminal Code, second paragraph:** "Without prejudice to more severe criminal provisions, the penalty is increased from two years' to five years' imprisonment and a fine of between MAD100,000 and MAD200,000 where the acts punishable under the first paragraph of this article result in either the modification or deletion of data contained in the automated data processing system, or an alteration in the operation of that system, or where the said acts are committed by a civil servant or an employee in the course of or in connection with the performance of his duties, or where he facilitates the performance of such acts by another person".
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.	**Criminal Code, article 607-5** Intentionally hindering or distorting the operation of an automated data processing system is punishable by one to three years' imprisonment and a fine of between 10,000 and 200,000 dirhams, or by one of these two penalties only. **Article 607-4 of the Criminal Code, second paragraph:** "Without prejudice to more severe criminal provisions, the penalty shall be increased from two years' to five years' imprisonment and a fine of between MAD100,000 and MAD200,000 where the acts punishable under the first paragraph of this article result in either the modification or deletion of data contained in the computer system, or the modification or deletion of data contained in the computer system, automated data processing system, or an alteration of the operation of this system or when the said acts are committed by a civil servant or an employee in the course of or in connection with the performance of his duties or if he facilitates the performance of such acts by others".
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	**Criminal Code, article 607-10** Shall be punishable by imprisonment for a term of two to five years and a fine of from 50,000 to 2,000,000 dirhams for any person to manufacture, acquire, hold, transfer, offer or make available equipment, instruments, computer programmes or any data designed or specially adapted to commit the offences provided for in this chapter. **Law No. 53-05 on the electronic exchange of legal data: Article 32:** Any person who imports, exports, supplies, operates or uses any

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.	cryptographic means or service without the declaration or authorisation required under Articles 13 and 14 above shall be liable to one year's imprisonment and a fine of MAD 100,000. The court may also order the confiscation of the cryptographic equipment concerned. **Article 33:** Where a means of cryptography, within the meaning of Article 14 above, has been used to prepare or commit a felony or misdemeanor or to facilitate the preparation or commission thereof, the maximum custodial sentence shall be increased as follows: - it is increased to life imprisonment when the offence is punishable by thirty years' imprisonment; - it is increased to thirty years of criminal imprisonment when the offence is punishable by twenty years of criminal imprisonment; - it is increased to twenty years' imprisonment, when the offence is punishable by fifteen years' imprisonment; - it is increased to fifteen years' imprisonment where the offence is punishable by ten years' imprisonment; - it is increased to ten years' imprisonment where the offence is punishable by five years' imprisonment; - doubled if the offence is punishable by up to three years' imprisonment. However, the provisions of this article shall not apply to the perpetrator or accomplice of the offence who, at the request of the judicial or administrative authorities, has provided them with the unencrypted version of the encrypted messages, as well as the secret conventions required for decryption.
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	**Criminal Code, article 607-7** Without prejudice to more severe criminal provisions, the forgery or falsification of computerised documents, in any form whatsoever, which is likely to cause harm to others, is punishable by imprisonment of between one and five years and a fine of between

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.	10,000 and 1,000,000 dirhams. Without prejudice to more severe criminal provisions, the same penalty shall apply to anyone who knowingly makes use of the computerised documents referred to in the previous paragraph.
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.	**Article 607-6 of the Criminal Code:** "The fact of fraudulently introducing data into an automated data processing system or of damaging, deleting or fraudulently modifying the data contained therein, or the way in which it is processed or transmitted, is punishable by one to three years' imprisonment and by fines of 10,000 to 500,000 dihram. 200,000 dirham fine or one of these two penalties only". **Articles 52, 54, 57, 59 and 61 of Law No. 09-08 on the protection of individuals with regard to the processing of personal data:** **Article 52:** "Without prejudice to civil liability in respect of persons who have suffered damage as a result of the offence, any person who implements a file of personal data without the declaration or authorisation required under article 12 above or has continued to process personal data despite the withdrawal of the receipt for the declaration or authorisation". **Article 54:** "Any person who, in breach of a), b) and c) of Article 3 of this Act, collects personal data by fraudulent, unfair or unlawful means, implements processing for purposes other than those declared or authorised, or subjects the aforementioned data to further processing incompatible with the declared or authorised purposes, shall be liable to imprisonment of between three months and one year and a fine of between 20,000 and 200,000 dihram, or to one of these two penalties only". Article 57: "Any person who, without the express consent of the persons concerned, processes personal data which, directly or indirectly, reveals the racial or ethnic origins, political, philosophical or religious opinions or trade union membership of persons, or which relates to the health of such persons, shall be liable to imprisonment for a term of three months to one year and a fine of 50,000 to 300,000 dihram, or to one of these two penalties only. The same penalties shall apply to anyone who processes personal data relating to offences, convictions or security measures". **Article 59:** "Any person who processes personal data concerning a natural person despite the opposition of that person, when this opposition is based on

	legitimate grounds or when this processing is for the purposes of canvassing, in particular commercial canvassing, as referred to in Article 9 or by electronic means as referred to in Article 10 of this law, shall be punished by imprisonment of between three months and one year and a fine of between 20,000 and 200,000 dihram or by one of these two penalties only". **Article 61:** "Any controller, subcontractor or person who, by virtue of his or her duties, is responsible for processing personal data and who, even through negligence, causes or facilitates the improper or fraudulent use of the data processed or received or communicates it to unauthorised third parties, shall be punished by imprisonment of between three months and one year and a fine of between 20,000 and 200,000 dihram or one of these two penalties only. The court may also order the seizure of any equipment used to to commit the offence as well as the deletion of all or part of the personal data forming the subject of the processing that gave rise to the offence".
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	**Criminal Code, article 503-2** Anyone who provokes, incites or facilitates the exploitation of children under the age of eighteen in pornography by any representation, by any means whatsoever, of a real, simulated or perceived sexual act or any representation of the sexual organs of a child for sexual purposes, shall be punished by imprisonment of between one and five years and a fine of between ten thousand and one million dirhams. The same penalty applies to anyone who produces, distributes, publishes, imports, exports, exhibits, sells or holds similar pornographic material. These acts are punishable even if committed outside the Kingdom. The penalty provided for in the first paragraph of this article shall be doubled if the perpetrator is one of the child's ascendants, a person responsible for the child's protection or a person having authority over the child. The same penalty applies to attempts to commit such acts. The conviction orders the confiscation and destruction of the

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.	pornographic material. The court may order the publication or posting of the judgment. The judgement may also order the withdrawal of any licence held by the convicted person. It may also order the temporary or permanent closure of the premises. **Article 73 of Law 88-13 on the press and publishing :** "It is forbidden to : - manufacture or hold with a view to trading, distribution, guarantee of distribution, rental, display or exhibition; - knowingly import or cause to be imported, export or cause to be exported, transport or cause to be transported, for the same purposes as set out above ; - offer, even free of charge, publicly or non-publicly. in any form whatsoever to the public ; - distribute, cause to be distributed or deliver for distribution. any printed matter, writings, drawings, engravings, photographs or media content **disseminating erotic or pornographic content or likely to be exploited to incite pimping, prostitution or sexual abuse of minors**, subject to the legislation in force". **Article 74:** The acts referred to in article 73 above are punishable by a fine of between 50,000 and 100,000 dirhams. **Article 79 of Law 88-13 on the press and publishing :** "A fine of between 100,000 and 500,000 dirhams shall be imposed on anyone who : offered, given or sold to children under eighteen years of age publications of any kind, inciting **to** debauchery, **prostitution**, crime or the consumption or trafficking of drugs, psychotropic substances, alcoholic beverages or tobacco;

	exposes these publications electronically or on the public highway, outside or inside shops, or makes a propaganda for them in the same places, whatever the means used for publication or making available to the public".
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. 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.	**Act no. 34-05 amending Act no. 02-2000 on copyright and related rights** **Article 64** - Any person who, for the purposes of commercial exploitation, unlawfully and by any means whatsoever commits an infringement shall be liable to a term of imprisonment of between two and six months and a fine of between ten thousand (I 0,000) and one hundred thousand (100,000) dirhams or to one of these two penalties only: Deliberate infringement for the purposes of commercial exploitation means : -the copyright mentioned in articles 9 and 10 paragraph (a) (republishing and reproducing the work in any way and in any form, permanent or temporary, including temporary archiving in electronic form); - the rights of performers referred to in Article 50 ; - the rights of phonogram producers referred to in article 51 ; - the rights of the broadcasting organisations referred to in article 52. Deliberate infringement for the purposes of commercial exploitation means : -any deliberate infringement of copyright or related rights that is motivated neither directly nor indirectly by financial gain; -any deliberate infringement committed for the purpose of obtaining a commercial advantage or private financial gain. The same penalties as set out in the first paragraph above, as well as the ancillary measures and sanctions referred to in article 64.3 below, shall be imposed on the following persons - anyone who imports or exports copies made in breach of the

	provisions of this law; - anyone who unlawfully performs any of the acts referred to in article 7, paragraph 1 of this law; -anyone who commits any of the acts referred to in article 65 of this law; - anyone against whom the criminal liability referred to in article 65.4 of this law has been determined. **Article 64.1** In the event of a habitual offence, the penalties provided for in article 64 above shall be doubled. **Article 64.2** Where the perpetrator of one of the acts referred to in Article 64 commits a new act constituting an infringement of copyright and related rights less than five years after a first judgment which has become final, he shall be punished by a prison sentence of between one and four years and a fine of between sixty thousand (60,000) and six hundred thousand (600,000) dirhams or by one of these two penalties only. **Article 65** - Without prejudice to the provisions of Law No. 77-03 on audiovisual communication, the following acts shall be considered unlawful and, for the purposes of Articles 61 to 64 of this Law, shall be deemed to constitute a violation of the rights of the public authors, performers and producers of sound recordings. a) the manufacture, import, export, assembly, modification, sale, rental or hiring of a device, system or means specially designed or adapted to render inoperative any device, system or means used to prevent or restrict the reproduction of a work or to impair the quality of copies made; b) manufacturing, importing, exporting, assembling, modifying, selling, renting or leasing a device, system or means designed or adapted knowingly or with good reason to know that it would enable or facilitate the decoding of programme-carrying coded signals without the authorisation of the lawful distributor;

	c) the reception and redistribution of signals carrying programmes originally coded in the knowledge that they have been decoded without the authorisation of the legitimate distributor; d) the circumvention, removal or restriction of any effective technological measure ; e) the manufacture, import, sale, offer to the public or distribution of any device, element, service or means used, or advertised or promoted, or essentially designed or produced for the purpose of enabling or assisting in the circumvention of, or rendering ineffective or restricting, any effective technological measure; f) deleting or modifying, without being authorised to do so, any information relating to the rights plan ; g) the distribution or importation for distribution of rights management information in the knowledge that the rights management information has been removed or altered without authorisation; h) the distribution or importation for distribution, broadcasting, communication to the public or making available to the public, without authorisation, of works, performances, phonograms or broadcasts, knowing that information in electronic form relating to the rights regime has been removed or modified without authorisation. For the purposes of this Article, "effective technological measure" means any technological measure, device or component which, in its normal use, controls access to a work, performance, phonogram or other subject-matter, or protects any copyright or related rights. For the purposes of this Article, "rights-management information" means information which makes it possible to identify the author, the work, the performer, the performance, the producer of the work and the copyright owner. **Article 575 of the Criminal Code:** "Anyone who publishes on Moroccan territory writings, musical compositions, drawings, paintings or any other production, printed

	or engraved in whole or in part, in disregard of the laws and regulations relating to authors' property, is guilty of counterfeiting and liable to a fine of between 200 and 10,000 dirhams, whether these works have been published in Morocco or abroad. The same penalties shall apply to the offering for sale, distribution, use or import of counterfeit works.
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 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 114-117, 607-8, and 129** **Article 114** Any attempt to commit a crime that has been manifested by the beginning of its execution or by unequivocal acts aimed directly at committing it, if it has not been suspended or if it has only failed to have an effect due to circumstances beyond the control of its perpetrator, shall be treated in the same way as a completed crime and punished as such. **Article 115** Attempted offences are only punishable by virtue of a special provision of the law. **Article 116** Attempted contraventions are never punishable. **Article 117** An attempt to commit an offence is punishable even if the intended aim could not be achieved due to a factual circumstance unknown to the perpetrator. **Article 607-8** Attempts to commit the offences provided for in articles 607-3 to 607-7 above and in article 607-10 below are punishable by the same penalties as the offence itself. **Article 129** The following shall be considered accomplices to an offence

	classified as a felony or misdemeanour: those who, without directly participating in the offence, have : 1° By means of gifts, promises, threats, abuse of authority or power, machinations or culpable artifices, provoked this action or gave instructions to commit it; 2° Procured weapons, instruments or any other means used in the action, knowing that they were intended for that purpose; 3° With knowledge of, aiding or assisting the perpetrator or perpetrators of the act, in the acts that prepared or facilitated it; 4° With knowledge of their criminal conduct, have habitually provided lodgings, places of retreat or meeting places for one or more criminals carrying out robberies or acts of violence against State security, public peace, persons or property. **Article 607-8 of the Criminal Code:** "Attempted offences under articles 607-3 to 607-7 above and article 607-10 below are punishable by the same penalties as the offence itself.
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	**Penal Code, article 127** Legal entities may only be sentenced to pecuniary penalties and the ancillary penalties provided for under numbers 5, 6 and 7 of article 36. They may also be subject to the real security measures of article 62. **Article 64 of Act No. 09-08 on the protection of individuals with regard to the processing of personal data:** "When the perpetrator of one of the offences provided for and punishable under this chapter is a legal entity, and without prejudice to the penalties that may be imposed on the perpetrator, the penalties provided for in this chapter shall not apply. may be applied to its directors who commit one of the following offences If the offender fails to comply with the above provisions, the fine will be doubled. In addition, the legal entity may be punished by one of the following penalties : - partial confiscation of his property; - confiscation under article 89 of the Criminal Code;

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.	- closure of the establishment or establishments of the legal entity where the offence was committed". **Article 40 of Act no. 53-05 on the electronic exchange of legal data:** "Where the offender is a legal entity, and without prejudice to the penalties that may be imposed on its directors who commit any of the offences provided for above, the fines provided for in this chapter shall be doubled. In addition, the legal person may be punished by one of the following penalties : - Partial confiscation of property; - Confiscation under article 89 of the Criminal Code ; - Closure of the establishment(s) of the legal entity used to commit the offences. **Article 104 of Law 88-13 on the press and publishing:** In the event of a penalty being imposed on the perpetrator of one of the acts listed in article 71 of this law, the periodical publication may be suspended or the electronic newspaper or electronic medium blocked by court order for a period of one month in the case of daily, weekly or fortnightly publication, or for two consecutive editions in the case of monthly, quarterly, half-yearly or annual publication. If a penalty is imposed for one of the acts referred to in articles 72 and 73 of this law, the suspension of the periodical publication or the blocking of the electronic newspaper or electronic medium may be ordered by the same judicial decision, for a period not exceeding one month, in the case of a daily, weekly or fortnightly publication, or for two consecutive editions if the publication is monthly, quarterly, half-yearly or annual. The court may order the publication of the conviction or its distribution at the offender's expense. This suspension will have no effect on the employment contracts entered into by the operator, who will continue to be bound by all the contractual obligations relating thereto as well as all other legal

	obligations arising from other contracts concluded in connection with the management of the periodical or electronic newspaper.
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 pursuant to Article 12 are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	**Penal Code, Article 607-9** Anyone who participates in an association formed or an agreement established for the purpose of preparing, as evidenced by one or more material facts, one or more of the offences provided for in this chapter shall be punished by the penalties provided for the offence itself or for the most severely punished offence. **Penal Code, Article 607-11** Subject to the rights of a third party acting in good faith, the court may order the confiscation of the material used to commit the offences provided for in this Chapter and of the thing which is the product thereof. The guilty party may, in addition, be prohibited from exercising one or more of the rights mentioned in Article 40 of this Code for a period of two to ten years. Incapacity to hold any public office or employment for a period of between two and ten years and the publication or posting of the conviction decision may also be pronounced. **Penal Code, Article 127** Legal persons may only be sentenced to pecuniary penalties and to the accessory penalties provided for under numbers 5, 6 and 7 of Article 36. They may also be subject to the real security measures provided for in Article 62. **Penal Code, Article 36** Ancillary penalties are : 1° Legal prohibition; 2° Civic degradation; 3° The suspension of the exercise of certain civic, civil or family rights; 4° The loss or suspension of the right to pensions provided by the State and public institutions. However, this loss may not apply to persons responsible for the maintenance of one or more children, subject to the provisions laid down in this respect by the pension schemes13. 5° The partial confiscation of property belonging to the convicted person, independently of the confiscation provided for as a security measure by Article 89; 6° The dissolution of a legal person; 7° The publication of the conviction decision. **Penal Code, Article 62**

	The actual security measures are : 1° The confiscation of objects related to the offence or harmful or dangerous objects, or whose possession is illegal; 2° The closure of the establishment that was used to commit an offence. **Penal Code, Article 218-1** The following offences constitute acts of terrorism, when they are intentionally committed in connection with an individual or collective undertaking with the aim of seriously undermining public order through intimidation, terror or violence: 7) infringements relating to automated data processing systems ;
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 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	Guarantees exist in **the 2011 Constitution** and in the **Code of Criminal Procedure**. In its preamble, the 2011 Constitution reaffirms the Kingdom of Morocco's commitment "*to the principles, rights and obligations*" set out in the international charters and conventions by which it is bound, as well as its attachment "*to human rights as universally recognised*". The Constitution also expressly guarantees various rights and freedoms, including the following: • the free exercise of religious worship (article 3), • freedom of association (articles 12 and 29), as well as freedom of assembly, peaceful demonstration and trade union and political membership, the conditions for exercising these freedoms being laid down by law (article 29), • a right of petition (article 15) and to present motions on

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.	legislative matters (article 14), • equal rights for men and women (article 19), • the right to life (article 20), • the right to physical security for oneself, one's family and property (article 21), • the right to physical and moral integrity, excluding torture and cruel, degrading treatment or treatment violating human dignity (article 22), • physical freedom (article 23), • the presumption of innocence (articles 23 and 119), • the right to a fair trial and the rights of the defence (articles 23 and 120), • the prohibition of incitement to racism, hatred and violence (article 23), • the right to privacy, including the principle that "*private communications, in whatever form, shall be secret*", with only "*the courts* [...] being able to *authorise, under the conditions and in the manner laid down by law, access to their content, their total or partial disclosure or their invocation against any person*" (article 24), • freedom of movement (article 24), • *freedom of thought, opinion and expression in all their forms*", as well as "*freedom of creation, publication and exhibition in literary and artistic matters and of scientific and technical research*" (article 25), • the right of access to information held by the authorities (article 27), • freedom of the press (article 28), • the right to strike (article 29), • the right of ownership (article 35), • the right to access to justice and to appeal against administrative acts (article 118), • free, means-tested access to the courts (article 121), • the right to compensation in the event of a miscarriage of justice (article 122), • the right to reasoned judgments (article 125). The Constitution also establishes an independent national human

	rights council (art 161), an ombudsman (art 162) and an authority responsible for parity and combating all forms of discrimination (art 164). When it comes to checks and balances, the Constitution : provides for the election of members of parliament by direct universal suffrage for one of the chambers and by indirect universal suffrage for the other. The other (articles 62 and 63), • guarantees *the* parliamentary opposition "*rights enabling it to carry out its duties properly*", including freedom of opinion and "*airtime on the public media*", "*effective participation in legislative work*" (article 10) and "*effective participation in monitoring the work of government*". • enshrines the independence of the judiciary (article 107) and the security of tenure of judges (article 108). Fundamental rights and freedoms are also "*a matter for the law*" (article 71), and the courts are responsible for protecting them (article 117).
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	**Article 57 of the Code of Criminal Procedure :** "The judicial police officer ... shall ensure the preservation of any evidence that may disappear and of anything that may help to establish the truth". **Article 15 of the Code of Criminal Procedure :** "the procedure during the investigation and trial is secret. All persons involved in these proceedings are bound by professional secrecy under the conditions and penalties set out in the Criminal Code". **Article 10 of Law 24-96 on postal services and telecommunications, which requires operators of public communications networks (service providers)**

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.	**to comply with the requirements of national defence and public security and the prerogatives of the French Post Office and the French Telecommunications Regulatory Authority (Telecommunications Regulatory Authority) judicial authority.** The provisions contained in Articles 57 and 15 of the Code of Criminal Procedure meet the needs of computer data retention and the retention and disclosure of traffic data. However, the Moroccan legislator has not obliged the service provider to disclose the data, nor has it insisted on the procedure for rapid data retention.
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.	
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	**Article 114** of the Code of Criminal Procedure states that "the information and documents required to identify the communication to be intercepted with a view to carrying out interception operations on calls authorised by recording, transcription or seizure, may be obtained from any operator of a general network or telecommunications services provided for in law no. 24.96 relating to post and telecommunications". However, these provisions are linked to the procedure for intercepting telephone calls 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; c any other information relating to the location of the communication equipment, available on the basis of a contract or service arrangement.	communications made by remote means of communication, and concern a limited list of offences which do not include cybercrime. **Article 10 of Law 24-96 on postal services and telecommunications, which requires operators of public communications networks (service providers) to meet the requirements of national defence and public security and the prerogatives of the judicial authorities.**
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.	The search procedure is set out in **article 60** of the Code of Criminal Procedure, which defines a search as a general procedure that applies to all offences, regardless of their nature. The seizure procedure is set out in **article 59** of the Code of Criminal Procedure, which states: "If the nature of the crime or misdemeanour is such that proof can be obtained by seizing papers, **documents or other objects** in the possession of persons who may have participated in the offence or hold documents or objects relating to the incriminating facts, the criminal investigation officer shall immediately go to the home of

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 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.	these persons to carry out a search under the conditions set out in articles 60 and 62, and shall draw up a report".
Title 5 - Real-time collection of computer data	
Article 20 – Real-time collection of traffic data	**Article 108 of the Code of Criminal Procedure** allows the examining magistrate, the King's public prosecutor and the first

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 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.	president of the court to where the needs of the information or investigation so require, to order in writing the interception of telephone calls and any communication made by remote means of communication, to record them and to take copies or seize them. However, this procedure only concerns a limited list of offences set out in Article 108, which does not include cybercrime per se. **Article 108 of the Criminal Procedure** does allow the investigating judge, when the needs of the information require it, to order in writing the interception of telephone calls and any communication made by remote means of communication, to record them and to take copies or seize them for offences which may be the subject of the preparatory investigation, namely crimes and misdemeanors punishable by 5 years of imprisonment or more, and related offences including cybercrimes where the punishment is 5 years imprisonment or more, an related offences. This is limited to falsification of computer documents, manufacturing or possession of equipment or computer programs dedicated specifically to commit offenses linked to attacks on the automated data processing system, the offences relating to child pornography, sextortion, etc.
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	**Article 108 of the Code of Criminal Procedure** allows the examining magistrate, the King's public prosecutor and the first president of the court to where the needs of the information or investigation so require, to order in writing the interception of telephone calls and any communication made by remote means of communication, to record them and to take copies or seize them. However, this procedure only concerns a limited list of offences set out in Article 108, which does not include cybercrime per se.

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.	**Article 108 of the Criminal Procedure** does allow the investigating judge, when the needs of the information require it, to order in writing the interception of telephone calls and any communication made by remote means of communication, to record them and to take copies or seize them for offences which may be the subject of the preparatory investigation, namely crimes and misdemeanors punishable by 5 years of imprisonment or more, and related offences including cybercrimes where the punishment is 5 years imprisonment or more, an related offences. This is limited to falsification of computer documents, manufacturing or possession of equipment or computer programs dedicated specifically to commit offenses linked to attacks on the automated data processing system, the offences relating to child pornography, sextortion, etc.
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	**Penal Code, articles 10-12** **Article 10** Moroccan criminal law applies to all persons, whether nationals, foreigners or stateless persons, who are present in the territory of the Kingdom, subject to the exceptions established by domestic public law or international law. **Article 11** Moroccan ships and aircraft are considered to be part of the territory, wherever they may be, unless they are subject to

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.	foreign law under international law. **Article 12** Moroccan criminal law applies to offences committed outside the Kingdom when they fall within the jurisdiction of Moroccan criminal courts under the provisions of articles 751 to 756 of the Code of Criminal Procedure (Editor's note: referring to articles 707 to 712 of law no. 22.01 on criminal procedure). **Articles 704, 705, 706 and 707 of the Code of Criminal Procedure** : **Article 704:** "The courts of the Kingdom of Morocco have jurisdiction over any offence committed on Moroccan territory, regardless of the nationality of the perpetrator. Any offence, one of the acts of which is committed within Morocco and which constitutes one of its constituent elements, is considered as if it were committed on the territory of the Kingdom. The jurisdiction of Moroccan courts to try the principal offence extends to all acts of complicity or concealment, even if committed outside the Kingdom and by foreigners. **Article 705:** The courts of the Kingdom have jurisdiction over crimes or offences committed on the high seas on vessels flying the Moroccan flag, regardless of the nationality of the perpetrators. Moroccan courts also have jurisdiction over crimes or offences committed in a Moroccan seaport on board a foreign merchant vessel. The competent court is that of the first Moroccan port of anchorage, or that of the place of arrest of the perpetrator if he is subsequently arrested in Morocco. **Article 706:** The courts of the Kingdom have jurisdiction over crimes or offences committed on board Moroccan aircraft, regardless of the nationality of the offender. They are also responsible for dealing with crimes or offences committed on board foreign aircraft if the perpetrator or victim is of Moroccan nationality or if the aircraft lands in Morocco after the crime or offence has been committed. The competent courts are those of the place of landing if the offender is arrested at the time of landing, and those of the place

	of arrest if the offender is subsequently arrested in Morocco. **Article 707:** Any act classified as a crime under Moroccan law committed outside the Kingdom of Morocco by a Moroccan may be prosecuted and tried in Morocco. However, the prosecution or trial may only take place when the accused has returned to Morocco and does not prove that the conviction has acquired the force of res judicata abroad and, in the event of conviction, has served his or her sentence or obtained a pardon.
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	Paragraph 1(a) of article 24 of the Budapest Convention complies with **article 713 of the Code of Criminal Procedure**, which states that "international conventions take precedence over national laws concerning judicial cooperation with foreign States". The same article also states that the provisions relating to judicial relations with foreign authorities only apply in the absence of, or in the absence of any mention of, such provisions in the conventions. With regard to Article 24(1)(b) of the Budapest Convention, since Morocco ratified the said Convention, no bilateral convention on extradition has been concluded to take account of the provisions of Article 24(1)(b), and, generally speaking, there are no provisions in Moroccan law that prevent extradition for the offences contained in the Convention, since **Article 720 of the Code of Criminal Procedure** states that "the facts that may give rise to extradition, whether it is a question of requesting it or granting it, are as follows ...": 1. all acts punishable by criminal penalties under the law of the requesting State ; 2. offences punishable by custodial sentences under the law of the requesting State when the maximum sentence under that law is at least one year or, in the case of a convicted person, when the sentence handed down by one of the courts of the

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.	requesting State is equal to or greater than four months;".

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.	**The general principles governing requests for mutual legal assistance in Morocco are as follows**: **The primacy of international conventions over domestic law.** If there is a bilateral convention on mutual legal assistance in criminal matters, it will be applied, otherwise multilateral conventions will be applied. In the absence of bilateral and international conventions, domestic law will apply Bilateral conventions provide that in urgent cases, letters rogatory are sent from the competent judicial authority in the requesting State to the competent judicial authority in the requested State. However, execution documents are returned via the official channels in force (diplomatic channel or central authority). The same applies to domestic legislation (article 715 of the Code of Criminal Procedure).

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.	There is no legal framework in Morocco outside MLAT channels for the sharing of spontaneous informaton. **The primacy of international conventions over domestic law.** If there is a bilateral convention on mutual legal assistance in criminal matters, it will be applied, otherwise multilateral conventions will be applied. In the absence of bilateral and international conventions, domestic law will apply Bilateral conventions in this area provide that in urgent cases, letters rogatory are sent from the competent judicial authority in the requesting State to the competent judicial authority in the requested State. However, execution documents are returned via the official channels in force (diplomatic channel or central authority). The same applies to domestic legislation (article 715 of the Code of Criminal Procedure).
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	

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	

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	

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.	There is no legal framework in Morocco describing the prompt disclosure of retained data outside MLAT channels for the sharing of spontaneous informaton. Bilateral conventions in this area provide that in urgent cases, letters rogatory are sent from the competent judicial authority in the requesting State to the competent judicial authority in the requested State. However, execution documents are returned via the official channels in force (diplomatic channel or central authority). The same applies to domestic legislation (article 715 of the Code of Criminal Procedure).
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	There is no legal framework in Morocco describing the prompt disclosure of retained data outside MLAT channels for the sharing of spontaneous informaton. Bilateral conventions in this area provide that in urgent cases, letters rogatory are sent from the competent judicial authority in the requesting State to the competent judicial authority in the requested State. However, execution documents are returned via the official channels in force (diplomatic channel or central authority). The same applies to domestic legislation (article 715 of the Code of Criminal Procedure).

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.	There is no legal framework in Morocco describing the prompt disclosure of retained data outside MLAT channels for the sharing of spontaneous informaton. Bilateral conventions in this area provide that in urgent cases, letters rogatory are sent from the competent judicial authority in the requesting State to the competent judicial authority in the requested State. However, execution documents are returned via the official channels in force (diplomatic channel or central authority). The same applies to domestic legislation (article 715 of the Code of Criminal Procedure).
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.	There is no legal framework in Morocco describing the prompt disclosure of retained data outside MLAT channels for the sharing of spontaneous informaton. Bilateral conventions in this area provide that in urgent cases, letters rogatory are sent from the competent judicial authority in the requesting State to the competent judicial authority in the requested State. However, execution documents are returned via the official channels in force (diplomatic channel or central authority). The same applies to domestic legislation (article 715 of the Code of Criminal Procedure).
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.	There is no legal framework in Morocco describing the prompt disclosure of retained data outside MLAT channels for the sharing of spontaneous informaton. Bilateral conventions in this area provide that in urgent cases, letters rogatory are sent from the competent judicial authority in the requesting State to the competent judicial authority in the requested State. However, execution documents are returned via the official channels in force

	(diplomatic channel or central authority). The same applies to domestic legislation (article 715 of the Code of Criminal Procedure).
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.	Article 10 of Law 24-96 on Postal Services and Telecommunications requires operators of public telecommunications networks (service providers) to meet the requirements of national defence, public security and the prerogatives of the judicial authorities. Requests for rapid preservation of stored computer data can be sent by e-mail to the Budapest Convention 24/7 contact point.
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.	