



www.coe.int/cybercrime

Last updated on 26th November 2023

Cybercrime legislation - legislative profile

Lebanon

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

| | |
|---|---|
| Chapter I – Terminology | |
| <p>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;</p> <p>"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;</p> <p>"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.</p> <p>"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.</p> | <p>ART 1 of law no 81/2018 : In order to apply the provisions of this law, each of items listed below will be defined: Authentication services provider: any public or private entity that issues authentication certificates after putting in place security measures that provides the functions specified in article 15 of this law.</p> <p>Service provider: the entity that allows users of its service the access to electronic communications network and provides direct information transfer services. These services can include the temporary "transitional storage information transmitted provided, in condition that it does not lead to any modification of the data stored, and the requirement to use this for good implementation of the service and must not exceed the time necessary for completion.</p> <p>Host data: Is the entity that stores Information of whatever nature, in benefit of others, for or without remuneration, and makes it accessible to the public through Direct Contact.</p> <p>Traffic data: Is any computer data relating to a communication system linked to the network, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.</p> |
| Chapter II - Measures to be taken at national level | |
| Section 1 - Substantive criminal law | |
| <i>Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems</i> | |

| | |
|---|--|
| <p>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.</p> | <p>Article 110 law no 81/2018 : Shall be punished with imprisonment from three months to two years and a fine of 1 million to 20 million LP or either the access to-or stay in- the whole or any part of a computer system without right, with the intention of fraud. The penalty is imprisonment for a term from six months to three years and fine from 2 million to 40 million Lebanese pounds, if the access leads to cancel digital data or software or modifying or jeopardizing the work of the information system.</p> |
| <p>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.</p> | <p>Article 17 of Law No 140 - released on 27/10/1999 incriminates illegal interception for unwires and wireless communications like phones and e-mails.</p> |
| <p>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.</p> | <p>Article 112 law no 81/2018 Shall be punished with imprisonment from six months to three years and a fine from three million to 60 million Lebanese pounds, or both, who enters numerical data in a system in intent of cheating and who damages, deletes, deteriorates, alters or suppresses a computer data contained in an information system.</p> |
| <p>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.</p> | <p>Article 112 law no 81/2018 Shall be punished with imprisonment from six months to three years and a fine from three million to 60 million Lebanese pounds, or both, who enters numerical data in a system in intent of cheating and who damages, deletes, deteriorates, alters or suppresses a computer data contained in an information system.</p> |
| <p>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 :</p> | <p>Article 114 law no 81/2018 Shall be punished with imprisonment from six months to three years and a fine from three million to 60 million Lebanese pounds or either both who</p> |

production, sale, obtaining for use, import, distribution or other forms of making available:
 a device, including a computer programme, primarily designed or adapted to enable the commission of one of the offences established in accordance with articles 2 to 5 above;
 a password, access code or similar computer data enabling access to all or part of a computer system,
 with the intention that they should be used to commit any of the offences referred to in Articles 2 to 5; and
 possession of an item referred to in paragraph a.i or ii above, with the intent that it be used to commit any of the offences referred to in Articles 2 to 5. A Party may require under its domestic law that a certain number of such items be possessed in order to incur criminal liability.

2 This Article shall not be construed as imposing criminal liability where the production, sale, procurement for use, import, dissemination or other making available referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with Articles 2 to 5 of this 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.

imports or produces or acquires or introduces or put at the disposal, without a legitimate reason, of hardware or software designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles of this chapter.

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.

Article 119 law no 81/2018 amended the text of article (453) of the Penal Code provides as follows:

Forgery is a deliberate misrepresentation of the truth, facts, or data which is proven by an instrument or manuscript or paper or electronic medium, or any medium that forms a document, with a view to cause physical, moral or social damage.

Article 8 - Computer fraud

Each Party shall adopt such legislative and other measures as may be

Article 655 Penal Code (amended pursuant to 239/1993)

| | |
|--|--|
| <p>necessary to establish as a criminal offence under its domestic law the intentional and wrongful causing of economic damage to another person:</p> <ul style="list-style-type: none"> a by any introduction, alteration, deletion or suppression of computer data; b by any form of interference with the functioning of a computer system, <p>with the intention, fraudulent or criminal, to obtain without right an economic benefit for oneself or for others.</p> | <p>Whoever induces others, through fraudulent maneuvers, to hand over to him movable or immovable property, or documents containing a pledge, release, or benefit, and seizes them, shall be punished by imprisonment from six months to three years and a fine from one hundred thousand to one million liras.</p> <p>These are considered fraudulent maneuvers:</p> <ul style="list-style-type: none"> 1- Actions that may make the victim believe that there is a fictitious project or that create in his mind the hope of profit or fear of harm. 2- Fabricating a lie that the victim believes as a result of the support of a third person, even in good faith, or as a result of a circumstance that the criminal prepared for, or a circumstance from which he benefited. 3- Disposing of movable or immovable property by someone who has no right or capacity to dispose of it, or by someone who has the right or capacity to dispose of it and misuses his right in order to extort money. 4- Using an alias or false description to deceive and influence. The same punishment applies to attempting to commit this crime. |
|--|--|

Title 3 - Content-related offences

| | |
|---|--|
| <p>Article 9 - Offences concerning child pornography</p> <p>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:</p> <ul style="list-style-type: none"> 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; | <p>Exploitation of Minors in Pornographic Materials Article 120 law no 81/2018</p> <p>Subsection (3) of Chapter II of Part VII titled: "Offences against Public Morality" of the Law issued by Legislative Decree no. 340 dated 01/03/1943 (Penal Code), shall be repealed and replaced by the following provisions:</p> <p>"Subsection (3) – Crimes of Minors' Exploitation for purposes of Pornography Article 535 penal code– Minors' exploitation for purposes of pornography means photographing, showing or physically depicting any minor through whatever means, such as drawings, photos, writings, films or signs showcasing the minor's sex organs or the minor himself/herself while engaging or acting as though engaging in explicit sexual activities. The Penal Code provisions shall apply to offences relating to minors' exploitation</p> |
|---|--|

| | |
|--|--|
| <p>e the possession of pornography child pornography in a computer system or computer data storage medium.</p> <p>2 For the purposes of paragraph 1 above, the term "child pornography" includes any pornographic material depicting a visual image:</p> <p>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.</p> <p>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.</p> <p>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.</p> | <p>for purposes of pornography (if validated), without prejudice to the provisions of the following Article.</p> <p>Article 536 penal code – The development or production of pornographic materials effectively involving minors is considered as a form of human trafficking, and the perpetrator of such crime shall be punished in accordance with Articles 586 (1) onwards on human trafficking of the Penal Code.</p> <p>If minors are not effectively involved in such pornographic material, the perpetrator shall be punished by imprisonment for one to three years and by a fine of five hundred thousand to two million Lebanese pounds.</p> <p>Any person who delivers, communicates, reproduces, displays, disposes of, distributes, exports, imports, posts, transmits or promotes minors' pornography by whatever means, shall be punished by imprisonment for one to three years and by a fine of five hundred thousand to two million Lebanese pounds.</p> <p>Penalties set forth in this article are increased in accordance with Article 257 (Penalties) in case of the use of an electronic communication network such as the Internet, radio or TV broadcasting to publish or distribute minors' pornography to an unspecified audience.</p> <p>The same penalties shall apply to attempts to commit the crimes set forth in the preceding subsections.</p> <p>Notwithstanding anything to the contrary herein, any person who regularly takes or displays pornographic materials involving minors, via radio/TV broadcast, a communication service targeting the general public, or any other means, or deliberately holds any such materials, shall be punished by imprisonment for no more than one year and/or a fine not exceeding two million Lebanese pounds.</p> <p>The provisions of this article shall be applied to pornographic images of any person looking like a minor.</p> <p>In case the criminal offence set forth in this article are committed by a legal entity, it shall be suspended from work for one month at least and two years at most.</p> |
|--|--|

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.

Offences related to infringements of copyright and related rights are subject to law number 75 dated 3-4-1999

Article 128 law n 81/2018 :

The following subsection shall be added to Article (51) of the Consumer Protection Law no. 659 dated 04/02/2005:

Electronic contracts shall be concluded pursuant to the provisions of Articles (33), (34), (35) and (38) of the Electronic Transactions and Personal Data Law.

Article 129 law no 81/2018 :

Notwithstanding anything to the contrary herein, any consumer who enters into a contract in accordance with this Chapter may reverse their decision to buy/hire goods or benefit from a service within a period of ten days starting from the date of concluding the contract for services or delivery date for goods, unless the parties agree to longer periods under the contract.

However, the consumer may not exercise the right set forth in the preceding subsection in the following events:

- 1 If they benefit from the service or use the goods before the elapsing of the ten- day period.
- 2 If the contract includes goods made to order or according to specifications defined by the consumer.
- 3 If the contract involves video tapes, discs or CDs: In case their covers have been removed.

| | |
|--|--|
| | <p>4 If the contract involves the purchase of newspapers, magazines and other publications.</p> <p>5 In case the goods become defective due to bad maintenance by the consumer.</p> <p>6 If the contract involves accommodation, transport, food or entertainment services delivered on a specific date or periodically at agreed-upon intervals.</p> <p>7 If the contract involves the purchase of software services online, except when the software is not downloaded or functional.</p> <p>Article 130 law no 81/2018 :</p> <p>Article (59) of the Consumer Protection Law no. 659 dated 04/02/2005 shall be repealed and replaced by the following:</p> <p>Any professional who uses indirect or electronic means for sale or lease shall abide by the provisions of this Law, particularly in relation to deceptive advertising, promotion and public safety.</p> |
|--|--|

Title 5 - Other forms of liability and sanctions

| | |
|---|--|
| Article 11 - Attempt and complicity | <p>Art 3 law no 81/2018 - The provisions in order with the law are applicable, unless stipulated in this law or contradict its provisions. (which allows the application of the measures stipulated in the Lebanese penal code for corporate liabilities, extradition and other national and international measures).</p> <p>Article 115 law no 81/2018 - The attempt is also punishable for the crimes set in this chapter.</p> |
| <p>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.</p> <p>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</p> | |

| | |
|--|---|
| <p>offences established in accordance with Articles 3 to 5, 7, 8, 9.1.a and c of this Convention.</p> <p>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.</p> | |
| <p>Article 12 - Liability of legal entities</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p> | <p>Art 3 law no 81/2018 - The provisions in order with the law are applicable, unless stipulated in this law or contradict its provisions.(which allows the application of the measures stipulated in the Lebanese penal code for corporate liabilities, extradition and other national and international measures).</p> |
| <p>Article 13 - Penalties and measures</p> <p>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</p> | |

| | |
|--|--|
| <p>punishable by effective, proportionate and dissuasive sanctions, including custodial sentences.</p> <p>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.</p> | |
| <p>Section 2 - Procedural law</p> | |
| <p>Title 1 - Common provisions</p> | |
| <p>Article 14 - Scope of application of procedural law measures</p> <p>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.</p> <p>2 Except as otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this Article:</p> <ul style="list-style-type: none"> 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. <p>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</p> | |

| | |
|---|--|
| <p>measure referred to in article 20.</p> <p>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:</p> <ul style="list-style-type: none"> 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, <p>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.</p> | |
| <p>Article 15 - Conditions and safeguards</p> <p>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.</p> <p>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.</p> <p>3 Each Party shall, to the extent consistent with the</p> | <p>Article 2 law no 81/2018:</p> <p>Information technology is at the service of every person provided that it did not affect the individual identity, rights or privacy or individual freedoms or the public.</p> <p>Article 66 law no 81/2018:</p> <p>The communication to the public by digital means is free within the respect of the requirement of the Constitution and national security and fundamental human rights and freedoms, or by special legal provisions.</p> |

| | |
|---|--|
| <p>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.</p> | |
| <p>Title 2 - Rapid preservation of stored computer data</p> | |
| <p>Article 16 - Rapid preservation of stored computer data</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>4 The powers and procedures referred to in this Article must be subject to articles 14 and 15.</p> | <p>Art 72 law no 81/2018 - An IT service provider shall save the traffic data of all the persons using their services, the data that help identify such persons and other technical data of communications, for three years as of the service delivery date.</p> <p>After notifying the competent judicial authority, the judicial police may request the IT service providers, as part of its criminal investigations, to store additional technical data on a given incidence or specific individuals, other than the data prescribed in subsection (1) of this Article, for no more than thirty days considering the urgent nature of this data and the potential loss or modification thereof. Furthermore, such data may only be submitted to the Judicial Police upon a decision by the competent judicial authority.</p> <p>The IT service provider may not invoke any technical failure causing the technical data not to be saved and shall take the appropriate technical measures as defined in a decision by the Minister of Telecommunications.</p> <p>The IT service provider shall be bound by professional secrecy to preserve the confidentiality of the technical data. However, the IT service provider may not invoke such secrecy before the competent judicial authority to the extent that the investigations and trials require the disclosure of such confidential data.</p> <p>The data storage obligation set forth in subsection (1) does not include any stored or transferred content that expresses the views of its author, such as exchanged correspondences or content of stored/transferred information or websites.</p> <p>The mechanism for saving/deleting traffic data and the nature of such data shall be defined by a decree issued by the Council of Ministers upon a proposal by the Minister of Justice.</p> |
| <p>Article 17 - Rapid retention and disclosure of traffic data</p> | <p>Art 72 law no 81/2018 - An IT service provider shall save the traffic data of all the persons using their services, the data that help identify such</p> |

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.

persons and other technical data of communications, for three years as of the service delivery date.

After notifying the competent judicial authority, the judicial police may request the IT service providers, as part of its criminal investigations, to store additional technical data on a given incidence or specific individuals, other than the data prescribed in subsection (1) of this Article, for no more than thirty days considering the urgent nature of this data and the potential loss or modification thereof. Furthermore, such data may only be submitted to the Judicial Police upon a decision by the competent judicial authority.

The IT service provider may not invoke any technical failure causing the technical data not to be saved and shall take the appropriate technical measures as defined in a decision by the Minister of Telecommunications.

The IT service provider shall be bound by professional secrecy to preserve the confidentiality of the technical data. However, the IT service provider may not invoke such secrecy before the competent judicial authority to the extent that the investigations and trials require the disclosure of such confidential data.

The data storage obligation set forth in subsection (1) does not include any stored or transferred content that expresses the views of its author, such as exchanged correspondences or content of stored/transferred information or websites.

The mechanism for saving/deleting traffic data and the nature of such data shall be defined by a decree issued by the Council of Ministers upon a proposal by the Minister of Justice.

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

Art 76 law no 81/2018 - IT service providers shall collaborate with the competent court and authorities stated in Law no.99/140 to the extent needed to uncover the truth in investigations and pending lawsuits.

The competent court and authorities identified in Law no. 99/140 and to the extent permitted by said law, require the IT service provider to submit any data they store or control in case it is deemed helpful in any investigation or pending lawsuit, in accordance with the obligations stipulated in Articles (72) and (74) above.

| | |
|--|--|
| <p>control relating to subscribers and concerning such services.</p> <p>2 The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.</p> <p>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:</p> <ul style="list-style-type: none"> 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. | <p>The IT service provider, upon a decision by the competent court or judicial authorities stated in Law no. 99/140 and to the extent permitted by said law, shall immediately provide such authority with traffic data and other technical data as set forth in Articles (72) and (74) herein and grant them real-time access to any communication performed through the provider's network.</p> |
|--|--|

Title 4 - Search and seizure of stored computer data

| | |
|--|---|
| <p>Article 19 - Search and seizure of stored computer data</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that, where its authorities search</p> | <p>Article 124 law no 81/2018:</p> <p>Seizure of data and software shall be conducted in a manner not compromising the rights of goodfaith persons and the person directly involved, by copying the seized data and software only. In other terms, the hardware containing the seized data and software shall not be seized, especially when such hardware is used for other legitimate purposes.</p> <p>At the time of seizure, in case of downloading or transferring data/IT evidence from a website or a computer, the source thereof shall be specified.</p> <p>Any data or digital evidence stored in an IT system located in the Lebanese territories may be seized if access thereto is possible from the IT system falling with the search warrant scope.</p> <p>Any data stored in an IT system may be accessed and seized, whether they</p> |
|--|---|

| | |
|--|---|
| <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>5 The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.</p> | <p>are in Lebanon or abroad, if they are made available to the public or in case the legally authorized person approves of disclosing such data through an IT system in the Lebanese territories.</p> <p>When the IT evidence is seized, the Public Prosecution or the judicial authority examining the case may decide that the process of downloading, transferring or copying data/software shall be done in the presence of the relevant person or any specialized technician appointed by the relevant person under a written authorization.</p> <p>Where appropriate, the scene where the search operations are conducted or the location of the electronic medium containing the data/software shall be closed and sealed pending the arrival of the technician within the specified time limit. Otherwise, the search operations may take place in the presence of two relatives of the concerned person, their lawyer or two witnesses. Nevertheless, the competent judicial authority may decide that their presence is not necessary.</p> <p>A copy of the seized data/software may be given to the concerned person at the time of seizure, by decision of the judicial authority taking such action.</p> <p>The judicial authority may request any person who knows how to operate the IT system or protection measures thereof, to provide the investigator in charge with the required information to access the requested data and software.</p> <p>It may also request any person having data or software that could serve as IT evidence, to make and hold a copy thereof until seizure is decided.</p> |
| <p><i>Title 5 - Real-time collection of computer data</i></p> | |
| <p>Article 20 - Real-time collection of traffic data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent</p> | <p>Art 76 law no 81/2018 -IT service providers shall collaborate with the competent court and authorities stated in Law no.99/140 to the extent needed to uncover the truth in investigations and pending lawsuits.</p> <p>The competent court and authorities identified in Law no. 99/140 and to the</p> |

| | |
|--|--|
| <p>authorities:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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, <p>in real time, traffic data associated with specific communications transmitted on its territory by means of a computer system.</p> <p>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.</p> <p>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.</p> <p>4 The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.</p> | <p>extent permitted by said law, require the IT service provider to submit any data they store or control in case it is deemed helpful in any investigation or pending lawsuit, in accordance with the obligations stipulated in Articles (72) and (74) above.</p> <p>The IT service provider, upon a decision by the competent court or judicial authorities stated in Law no. 99/140 and to the extent permitted by said law, shall immediately provide such authority with traffic data and other technical data as set forth in Articles (72) and (74) herein and grant them real-time access to any communication performed through the provider's network.</p> |
| <p>Article 21 - Interception of content data</p> <p>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:</p> <ul style="list-style-type: none"> 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: | <p>Law No 140-released on 27/10/1999.</p> |

| | |
|--|--|
| <p>i to be collected or recorded using technical means available on its territory, or</p> <p>ii to assist the competent authorities in collecting or recording data,</p> <p>in real time, data relating to the content of specific communications on its territory, transmitted by means of a computer system.</p> <p>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.</p> <p>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.</p> <p>The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.</p> | |
|--|--|

Section 3 - Competence

| | |
|--|---|
| <p>Article 22 - Jurisdiction</p> <p>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:</p> <p>a on its territory; or</p> <p>b on board a vessel flying the flag of that Party; or</p> <p>c on board an aircraft registered under the laws of that Party; or</p> <p>d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence</p> | <p>The entire matters relating to Jurisdiction are legislated in Art 15-26 penal code.</p> <p>Specific parts of these articles state;</p> <p>Article 15</p> <p>Lebanese Sharia law shall be applied to all crimes committed on Lebanese territory. The crime is considered to have been committed on Lebanese territory.</p> |
|--|---|

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.

- 1- If one of the elements that constitute the crime, or an act of an indivisible crime, or an act of primary or secondary association, is committed on this land.
- 2- If the result occurred on this land or was expected to occur there.

Article 16

The Lebanese territory includes the layer of air that covers it, i.e. the air region.

Article 19

Amended in accordance with Legislative Decree No. 112 dated 9/16/1983 Law No. 513 dated 6/6/1996 Lebanese laws apply to every Lebanese, foreigner, or stateless person, whether actor, partner, instigator, or intervener.

Article 20

Lebanese Sharia law applies to every Lebanese person, whether perpetrator, instigator or accomplice, who commits a misdemeanor or felony punishable by Lebanese Sharia law outside Lebanese territory. This remains the case even if the defendant loses or acquires Lebanese citizenship after committing the felony or misdemeanor.

Article 23

Amended in accordance with Law No. 513 dated 6/6/1996 Lebanese laws also apply to every foreigner or stateless person residing or found in Lebanon, who abroad, as a perpetrator, accomplice, instigator or accomplice, commits a felony or misdemeanor not stipulated in Articles 19 (Clause 1), 20 and 21, if his recovery has not been made. Requested or accepted. Likewise, if the felony or misdemeanor is committed by anyone against or on board a foreign aircraft rented without a crew, to a lessee who has a main place of business or a permanent residence in Lebanon, if the perpetrator's recovery has not been requested or accepted.

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 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

The full legal framework for Lebanon is detailed in Articles 30-36 of the Penal Code.

Relevant legislation includes;

Article 30 states, No one shall be extradited to a foreign country, except in cases stipulated in the provisions of this law, unless this is in implementation of a treaty that has the force of law.

Article 31 states, allows extradition for:

- 1- Crimes committed on the territory of the state requesting extradition.
- 2- Crimes that undermine its security or financial standing.
- 3- Crimes committed by one of its nationals.

| | |
|---|--|
| <p>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.</p> <p>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.</p> <p>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.</p> | |
| <p>Article 25 - General principles relating to mutual assistance</p> <p>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.</p> <p>2 Each Party shall also adopt such legislative and other measures as may be necessary to fulfil the obligations set out in Articles</p> <p>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</p> | <p>Bilateral cooperation: Lebanon signed several bilateral agreements aimed at strengthening cooperation in the field of cybercrime, cyber security and transnational organized crimes, especially with France and with the Arab countries.</p> <p>Multilateral cooperation: Lebanon signed the United Nations Convention against Transnational Organized Crime on 18 December 2001 and ratified it on 5 October 2005.</p> <p>Lebanon has not signed any international conventions against Cybercrime such as the Budapest Convention and the Arab Convention on Combatting Information Technology Offences.</p> <p>Lebanon is a member of Interpol.</p> |

| | |
|--|---|
| <p>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.</p> <p>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.</p> <p>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.</p> | |
| <p>Article 26 - Spontaneous information</p> <p>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.</p> <p>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</p> | <p>No legal framework has been identified for this article.</p> |

| | |
|---|---|
| <p>with such a request, it shall inform the other P a r t y , 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.</p> | |
| <p><i>Title 4 - Procedures relating to requests for mutual assistance in the absence of applicable international agreements</i></p> | |
| <p>Article 27 - Procedures for requests for mutual assistance in the absence of applicable international agreements</p> <p>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.</p> <p>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;</p> <p>b The central authorities communicate directly with each other;</p> <p>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;</p> <p>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.</p> <p>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.</p> <p>4 In addition to the conditions or grounds for refusal laid down in Article 25(4), mutual assistance may be refused by the</p> | <p>No legal framework has been identified for this article.</p> |

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

| | |
|---|---|
| <p>may be made through the International Criminal Police Organization (Interpol).</p> <p>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.</p> <p>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.</p> <p>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.</p> | |
| <p>Article 28 - Confidentiality and restrictions on use</p> <p>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.</p> <p>2 The requested Party may make the provision of information or material in response to a request conditional:</p> <p>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</p> <p>b provided that they are not used for the purposes of investigations or proceedings other than those indicated in the request.</p> <p>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</p> | <p>No legal framework has been identified for this article.</p> |

| | |
|---|---|
| <p>should nevertheless be provided. If the requesting Party accepts the condition, it shall be bound by it.</p> <p>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.</p> | |
| <p>Section 2- Specific provisions</p> | |
| <p><i>Title 1 - Mutual assistance in respect of interim measures</i></p> | |
| <p>Article 29 - Rapid preservation of stored computer data</p> <p>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.</p> <p>2 A request for conservation made pursuant to paragraph 1 must specify:</p> <ul style="list-style-type: none"> 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. <p>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</p> | <p>No legal framework has been identified for this article.</p> |

| | |
|--|---|
| <p>law. In order to comply with such a request, dual criminality is not required as a precondition for preservation.</p> <p>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.</p> <p>5 In addition, a conservation request can only be refused:</p> <ul style="list-style-type: none"> 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. <p>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</p> <ul style="list-style-type: none"> c whether the request should nevertheless be carried out. <p>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.</p> | |
| <p>Article 30 - Prompt disclosure of retained data</p> <p>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</p> | <p>No legal framework has been identified for this article.</p> |

| | |
|--|---|
| <p>purpose of identifying that service provider and the channel through which the communication was transmitted.</p> <p>2 Disclosure of traffic data pursuant to paragraph 1 may be refused only:</p> <p>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</p> <p>if it considers that granting the request would be likely to prejudice its sovereignty, security, public order or other essential interests.</p> | |
| <p><i>Title 2 - Mutual assistance regarding investigative powers</i></p> | |
| <p>Article 31 - Mutual assistance concerning access to stored data</p> <p>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.</p> <p>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.</p> <p>a The request must be satisfied as quickly as possible within the following cases: there is reason to believe that the relevant data are particularly sensitive to the risk of loss or modification; or</p> <p>b the instruments, arrangements and legislation referred to at paragraph 2 provide for rapid cooperation.</p> | <p>No legal framework has been identified for this article.</p> |
| <p>Article 32 - Cross-border access to stored data with consent or when publicly accessible</p> <p>A Party may, without the authorisation of another Party :</p> <p>a access publicly available (open source) stored computer data, regardless of the geographical location of that data; or</p> <p>b access or receive, by means of a computer system located in its territory, computer data stored in another State,</p> | <p>No legal framework has been identified for this article.</p> |

| | |
|---|--|
| <p>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.</p> | |
| <p>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.</p> | <p>No legal framework has been identified for this article.</p> |
| <p>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.</p> | <p>No legal framework has been identified for this article.</p> |
| <p>Title 3 - 24/7 Network</p> | |
| <p>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.</p> | <p>No legal framework has been identified for this article. Lebanon is not a party to the Budapest Convention on Cybercrime.</p> |

| | |
|--|--|
| <p>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.</p> <p>3 Each Party shall ensure that it has trained and equipped staff to facilitate the operation of the network.</p> | |
| <p>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.</p> | |