Last updated on 14th November 2023

Cybercrime legislation - legislative profile

HASHEMITE KINGDOM OF JORDAN

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	*Tel: +33-3-9021-4506*
Directorate General for Human Rights and Legal Affairs	*Fax: +33-3-9021-5650*
Council of Europe, Strasbourg France	*Email: alexander.seger@coe.int*
	www.coe.int/cybercrime

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

Chapter I – Terminology	
Article 1 – "Computer system", "computer data", "service provider", "traffic data" : For the purposes of this Convention : computer system" means any device or set of interconnected or related devices, one or more of which, when executing a program, performs automatic data processing; computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme for causing a computer system to perform a function; service provider" means: any public or private entity that offers users of its services the possibility of communicating by means of a computer system, and any other entity processing or storing computer data for this communication service or its users. "traffic data" means any data relating to a communication passing through a computer system, generated by the computer system as part of the communication chain, indicating the origin, destination, route, time, date, size and duration of the communication or the type of underlying service.	On 12th September 2023 the Hashemite Kingdom of Jordan enacted the **Electronic Crimes Law number 17 of 2023** **Article 2** of the Electronic Crimes Law states provides the following definitions which are similar to the one described in Article one of the Budapest Convention. Information network - A link between more than one information system or any information technology means to make available and obtain the data and information. Data - Everything that can be processed, stored, supplied, or transmitted using information technology, including writing, images, numbers, videos, letters, symbols, signs, and others. Service provider - Any natural or legal person, public or private, who provides subscribers with electronic services by means of information technology, or who processes or stores information on behalf of the telecommunications service or its users. Traffic data path - Any data movement related to a communication through an information system or any means of information technology that arises therefrom and forms part of the communication chain and indicates the source, destination, path, timing, and date of the communication.
Chapter II - Measures to be taken at national level	
Section 1 - Substantive criminal law	
Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems	

Article 2 - Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the intentional and unauthorised access to all or part of a computer system. A Party may require that the offence be committed in breach of security measures, with intent to obtain computer data or with other criminal intent, or in connection with a computer system connected to another computer system.	**Electronic Crimes Law number 17 of 2023 Article 3a states** Whoever intentionally accesses a website, information network, information system or information technology means or any part thereof by any means without authorization or in violation or excess of an authorization, shall be punished by imprisonment for a period not less than one week and no more than three months, or by a fine of not less than (300) three hundred Dinars and no more than (600) six hundred Dinars, or both penalties.
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.	**Electronic Crimes Law number 17 of 2023 Article 7 states** Whoever intentionally and unjustly intercepts the data flow, captures its content, obstructs, alters, deletes, or records that content, whether it is sent through the information network, information technology, information system, or data exchanged within the system or the network itself, shall be punished by imprisonment for a period of not less than six months and a fine of not less than (1500) one thousand five hundred Dinars and not more than (6000) six thousand Dinars.
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.	**Electronic Crimes Law number 17 of 2023 Article 3b states** Where the access stipulated in paragraph (a) of this Article is for the purpose of canceling, deleting, destroying, disclosing, posting, re-posting, damaging, blocking, altering, changing, transferring or copying data or information, or breach the confidentiality of data, or encoding, stopping or disabling the operation of the information network, information system or information technology or any part thereof, the perpetrator shall be punished by imprisonment for a period not less than three months and no more than one year and a fine of not less than (600) six hundred Dinars and no more than (3000) three thousand Dinars. The penalty shall be imprisonment for a period not less than one year and no more than three years and a fine of not less than (3000) three thousand Dinars and no more than (15000) fifteen thousand Dinars if he achieves the result. **Electronic Crimes Law number 17 of 2023 Article 6** states Whoever intentionally inserts, publishes, or uses a program or program command through the information network or information technology means, or by using an information system to cancel, delete, add, destroy, disclose, damage, block, encrypt, modify, change, transmit, copy, or capture or enabling others to access

	data or information, obstructing, disrupting, stopping or disabling the functioning of the information system or accessing it, changing, canceling, destroying or modifying its contents or occupying it without authorization or in violation of that authorization or impersonating its identity or the identity of its owner shall be imprisoned for a period of no less than six months and a fine of no less than (2500) two thousand five hundred Dinars and no more than (10000) ten thousand Dinars.
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.	**Electronic Crimes Law number 17 of 2023 Article 3c states** Whoever intentionally accesses a website to change, cancel, destroy or alter its contents, or occupy, encrypt, stop or enable it, or assumes its identity or the identity of its owner, the perpetrator shall be punished by imprisonment for a period not less than three months and a fine of not less than (600) six hundred Dinars and no more than (3000) three thousand Dinars.
Article 6 – Abuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right : production, sale, obtaining for use, import, distribution or other forms of making available: a device, including a computer programme, primarily designed or adapted to enable the commission of one of the offences established in accordance with articles 2 to 5 above; a password, access code or similar computer data enabling access to all or part of a computer system, with the intention that they should be used to commit any of the offences referred to in Articles 2 to 5; and possession o f 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	**Electronic Crimes Law number 17 of 2023 Article 8 states** He shall be punished by imprisonment for a period of no less than three years and a fine of no less than (2500) two thousand five hundred Dinars and no more than (10000) ten thousand Dinars, whoever: 1. Obtains intentionally and without authorization, or in excess of authorization, through the information network, information technology, or information system, data or information related to electronic payment means, or the implementation of electronic financial or banking transactions, or uses or publishes any of these data. 2. Fabricates, creates, develops, or designs any information technology means, information program, or program command with the intent of facilitating access to the data stipulated in Clause (1) of this Paragraph. 3. Accepted dealing with forged, counterfeit or copied cards or other means of electronic payment or data of electronic payment means that were illegally seized, knowing that they are illegal. **Electronic Crimes Law number 17 of 2023 Article 11 states** Whoever possesses, without authorization, a device, program, or any prepared electronic data, password, or access codes, or submits, produces, distributes,

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, issues, or promotes them, with the aim of committing any of the crimes stipulated in this Law shall be punished with imprisonment for a period of no less than three months or a fine of no less than (2500) two thousand five hundred Dinars and no more than (25000) twenty five thousand Dinars, or both penalties.

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.	**Electronic Crimes Law number 17 of 2023 Article 5a** states Whoever creates an account, page, group, channel, or similar on social media platforms and falsely attributes the same to a natural or legal person shall be punished by imprisonment for a period of no less than three months or a fine of no less than (1500) one thousand five hundred Dinars and no more than (15000) fifteen thousand Dinars, or both penalties. **Electronic Crimes Law number 17 of 2023 Article 5c** creates a more serious offence when the violation relates to official bodies or public servants.

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.
	Electronic Crimes Law number 17 of 2023 Article 8 states
	
	He shall be punished by imprisonment for a period of no less than three years and a fine of no less than (2500) two thousand five hundred Dinars and no more than (10000) ten thousand Dinars, whoever:
	
	1. Obtains intentionally and without authorization, or in excess of authorization, through the information network, information technology, or information system, data or information related to electronic payment means, or the implementation of electronic financial or banking transactions, or uses or publishes any of these data.
	
	2. Fabricates, creates, develops, or designs any information technology means, information program, or program command with the intent of facilitating access to the data stipulated in Clause (1) of this Paragraph.
	
	3. Accepted dealing with forged, counterfeit or copied cards or other means of electronic payment or data of electronic payment means that were illegally seized, knowing that they are illegal.

Title 3 - Content-related offences

Article 9 - Offences concerning child pornography	Electronic Crimes Law number 17 of 2023 Article 13c states
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 v i a a computer system; c the distribution or transmission of child pornography via a computer system; d procuring child pornography for oneself or others by means of a computer system; e the possession of pornography child pornography in a computer system or computer data storage medium. **2** For the purposes of paragraph 1 above, the term "child pornography" includes any pornographic material depicting a visual image: a a minor engaging in sexually explicit conduct; b a person who appears to be a minor engaging in sexually explicit behaviour; c realistic images depicting a minor engaged in sexually explicit behaviour. **3** For the purposes of paragraph 2 above, the term "minor" means any person under the a g e 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.	Whoever possesses images, recordings, drawings or other data within an information system or data storage support, or sexually suggestive of real, virtual, or simulated sexual organs or sexual acts of a juvenile under eighteen years of age, or if the content relates to a person with a mental illness or mental disability, shall be punished by imprisonment for a period of no less than six months or a fine of no less than (3000) three thousand Dinars and no more than (6000) six thousand Dinars.

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.	No legal framework identified

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	**Electronic Crimes Law number 17 of 2023 Article 4c states** attempts to commit crimes stipulated in this Article shall be punished by the penalty prescribed for the same crimes. This attempt to commit illegal access is restricted to offences against information network, information technology, information system, or any part

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.	thereof belonging to ministries, government departments, public official institutions, public, security, financial, or banking institutions, or companies owned or contributed by any of these entities or critical infrastructure and has access to data or information not available to the public and affects the national security, foreign relations of the Kingdom, public safety or the national economy shall be punished by imprisonment for a period not less than six months and no more than three years and a fine of no less than (2500) two thousand five hundred Dinars and no more than (25000) twenty-five thousand Dinars. No other legislation relating to attempt and aiding or abetting is in place for cybercrime offences.
Article 12 – Liability of legal entities 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for offences established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, founded: a on a power of representation of the legal entity; b on an authority to take decisions on behalf of the person moral; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall adopt such measures as may be necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of the offences established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. Depending on the legal principles of the Party, the liability of a legal entity may be criminal, civil or administrative. This liability is established without prejudice to the criminal liability of the natural persons who committed the offence.	No legal framework identified

Article 13 – Penalties and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 to 11 are punishable by effective, proportionate and dissuasive sanctions, including custodial sentences. 2 Each Party shall ensure that legal persons held liable pursuant to Article 12 are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	**Each article of the Electronic Crimes Law number 17 of 2023** has stipulated offences against each stipultated offence. In addition, the following articles are relevant. **Article 25** Whoever commits any crime not provided for in this Law and is punishable under any legislation using the information network, information technology, information system or website, or participates, interferes or incites to commit it shall be punished with the penalty stipulated in that legislation. **Article 26** Whoever intentionally participates in, interferes or incites the committal of any of the crimes stipulated in this Law shall be punished with in the same manner specified for its perpetrators. **Article 27** The penalties stipulated in this Law shall be doubled in the following cases: 1. If the perpetrator committed his crime by taking advantage of his position, work, or powers granted to him. 2. If the victims are multiple. 3. If any of the crimes stipulated in this Law were repeatedly committed. 4. If the perpetrator committed his crime for the benefit of a foreign country or an illegal organization. **Article 28** The court may reduce the penalties stipulated in this Law by half if the perpetrator provided information about any of the crimes stipulated in this Law before referring it to the public prosecutor and that would have resulted in the detection of the crime or its perpetrators or arresting them. **Article 29**

	The application of the penalties stipulated in this Law does not preclude the imposition of any harsher penalty stipulated in any other law.

Section 2 - Procedural law

Title 1 - Common provisions

Article 14 – Scope of application of procedural law measures 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings. 2 Except as otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this Article: a criminal offences established in accordance with Articles 2 to 11 of this Convention; b all other criminal offences committed u s i n g a computer system; and c the collection of electronic evidence of any criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to the offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not narrower than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider limiting such a reservation so as to enable the widest possible application of the measure referred to i n article 20.	

b   Where a Party, because of restrictions imposed by its legislation in force at the time of adoption of this Convention, is unable to apply the measures referred to in Articles 20 and 21 to communications transmitted on a computer system of a service provider:
 	
   i   is implemented for the benefit of a closed user group, and
   ii which does not use public telecommunications networks and which is not connected to another computer system, whether public or private,
 	
that Party may reserve the right not to apply such measures to such communications. Each Party shall consider limiting any such reservation so as to permit the widest possible application of the measure referred to in articles 20 and 21.	

Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, 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 E u r o p e Convention for the Protection of Human Rights and Fundamental Freedoms (1950) and the United Nations International Covenant on Civil and Political Rights (1966), or other applicable international human rights instruments, and which must incorporate the principle of proportionality. 2 Where appropriate, having regard to the nature of the procedure or power concerned, such conditions and safeguards shall include, inter alia, judicial or other independent supervision, reasons for application and limitations on the scope and duration of the power or procedure in question. 3 Each Party shall, to the extent consistent with th e public interest, in particular the proper administration of justice,	

consider the effect of the powers and procedures in this Section on the rights, responsibilities and duties of the judiciary and legitimate interests of third parties.	

Title 2 - Rapid preservation of stored computer data	

Article 16 – Rapid preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or otherwise require the expeditious preservation of specified electronic data, including traffic data, stored by means of a computer system, in particular where there is reason to believe that such data are particularly susceptible to loss or alteration. 2 Where a Party applies paragraph 1 above, by means of an order requiring a person to preserve specified stored data in its possession or control, that Party shall adopt such legislative and other measures as may be necessary to require that person to preserve and protect the integrity of that data for as long as necessary, but not longer than ninety days, to enable the competent authorities to obtain disclosure. A Party may provide for such an injunction to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the data custodian or other person responsible for storing the data to maintain the secrecy of the implementation of such procedures for the period provided for by its domestic law. 4 The powers and procedures referred to in this Article must be subject to articles 14 and 15.	**Electronic Crimes Law number 17 of 2023 Article 4c states** the competent public prosecutor or the competent court, when the information system, website, service provider inside or outside the Kingdom, social media platforms, or the person responsible for any account, public page, public group, channel, or the like publishes any materials that violate the provisions of this Law or the legislation in force in the Kingdom shall have the right to issue an order to those in charge of it to take the following: 1. Remove, block, stop, disable, register or intercept the data path or any publication or content, or prevent access to it, or temporarily ban the user or publisher within the period specified in the decision. 2. Provide them with all the necessary data or information that helps reveal the truth, including the data of the owner or user of the website or the information system that helps in determining his identity and conducting legal prosecution. 3. Urgent preservation of data and information necessary to reveal the truth, store it and maintain its integrity. 4. Maintain confidentiality.
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	**Electronic Crimes Law number 17 of 2023 Article 32 states** the competent public prosecutor or the competent court, when the information system, website, service provider inside or outside the Kingdom, social media platforms, or the person responsible for any account, public page, public group, channel, or the like publishes any materials that violate the provisions of this Law or the legislation in force in the Kingdom shall have the right to issue an order to those in charge of it to take the following:

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, o f 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.	1. Remove, block, stop, disable, register or intercept the data path or any publication or content, or prevent access to it, or temporarily ban the user or publisher within the period specified in the decision. 2. Provide them with all the necessary data or information that helps reveal the truth, including the data of the owner or user of the website or the information system that helps in determining his identity and conducting legal prosecution. 3. Urgent preservation of data and information necessary to reveal the truth, store it and maintain its integrity. 4. Maintain confidentiality.

Title 3 - Production order

Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue orders: a a person present in its territory to disclose specified computer data in its possession or control that is stored in a computer system or computer storage medium; and b a service provider offering services in the territory of the Party, to communicate data in its possession or under its control relating to subscribers and concerning such services. 2 The powers and procedures referred to in this Article shall be subject to Articles 14 and 15. 3 For the purposes of this Article, "subscriber data" means any information, whether in the form of computer data or in any other form, held by a service provider relating to subscribers to its services, other than traffic or content data, from which it can be established: a the type of communication service used, the technical arrangements made for it and the period of service; b t h e identity, postal or geographical address and telephone	**Electronic Crimes Law number 17 of 2023 Article 32 states** the competent public prosecutor or the competent court, when the information system, website, service provider inside or outside the Kingdom, social media platforms, or the person responsible for any account, public page, public group, channel, or the like publishes any materials that violate the provisions of this Law or the legislation in force in the Kingdom shall have the right to issue an order to those in charge of it to take the following: 1. Remove, block, stop, disable, register or intercept the data path or any publication or content, or prevent access to it, or temporarily ban the user or publisher within the period specified in the decision. 2. Provide them with all the necessary data or information that helps reveal the truth, including the data of the owner or user of the website or the information system that helps in determining his identity and conducting legal prosecution. 3. Urgent preservation of data and information necessary to reveal the truth, store it and maintain its integrity. 4. Maintain confidentiality.

number of the company. 　　the subscriber's telephone number, and any other access 　　number, data concerning invoicing and payment, available 　　o n 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.	

Title 4 - Search and seizure of stored computer data	
Article 19 – Search and seizure of stored computer data Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to carry out searches or similar accesses: a 　a computer system or part thereof or computer data stored therein; and b 　a computer storage medium for storing computer data on its territory. 2 　Each Party shall adopt such legislative and other measures as may be necessary to ensure that, where its authorities search or similarly access a specific computer system or part thereof pursuant to paragraph 1.a, and have reason to believe that the data sought is stored in another computer system or part thereof located in its territory, and t h a t 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	**Electronic Crimes Law number 17 of 2023 Article 32 states** Subject to the terms and conditions stipulated in the legislation in force and the personal rights of the defendant, the employees of the judicial police, a14er obtaining permission from the competent public prosecutor or the competent court may: 1. Enter and inspect any place where evidence indicates that it was used to commit any of the crimes stipulated in this Law. 2. Inspect and examine the devices, tools, programs, operating systems, the information network, and the means that evidence indicates that they were used to commit any of these crimes. The employee who conducted the inspection or examination shall organize a report of that and submit it to the public prosecutor or the competent court. **Electronic Crimes Law number 17 of 2023 Article 32 states** the competent public prosecutor or the competent court, when the information system, website, service provider inside or outside the Kingdom, social media platforms, or the person responsible for any account, public page, public group, channel, or the like publishes any materials that violate the provisions of this Law or the legislation in force in the Kingdom shall have the right to issue an order to those in charge of it to take the following: 1. Remove, block, stop, disable, register or intercept the data path or any publication or content, or prevent access to it, or temporarily ban the user or publisher within the period specified in the decision.

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.	2. Provide them with all the necessary data or information that helps reveal the truth, including the data of the owner or user of the website or the information system that helps in determining his identity and conducting legal prosecution. 3. Urgent preservation of data and information necessary to reveal the truth, store it and maintain its integrity. 4. Maintain confidentiality.

Title 5 - Real-time collection of computer data

Article 20 – Real–time collection of traffic data
 	
1   Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities:
a   to collect or record using technical means available on its territory, and
b   to oblige a service provider, within the framework of its existing technical capabilities:
    i   to be collected or recorded using technical means available on its territory, or
    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
	The Telecommunications Law number 13 of 1995 Article 29 allows the monitoring of communication pursuant to a judicial or an administrative request. Article 29 of the law states: "that the licensee should commit to provide the necessary facilities to the competent authorities for the implementation of court and administrative orders that have to do with tracking communications specified in these orders.

legal order, cannot adopt the measures set out in paragraph 1.a, it may instead adopt such legislative and other measures as may be necessary to ensure the collection or recording in real time of traffic data associated with specific communications transmitted on its territory through the application of technical means existing on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to require a service provider to keep secret the fact that any of the powers provided for in this Article have been as well as any information on this subject. 4 The powers and procedures referred to in this Article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities with respect to a range of serious offences to be defined in domestic law: a to be collected or recorded using technical means available on its territory, and b to oblige a service provider, within the scope of its technical capabilities: i to be collected or recorded using technical means available on its territory, or ii to assist the competent authorities in collecting or recording data, in real time, data relating to the content of specific communications on its territory, transmitted b y 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 t h e	**The Telecommunications Law number 13 of 1995 Article 29 allows** the monitoring of communication pursuant to a judicial or an administrative request. Article 29 of the law states: "that the licensee should commit to provide the necessary facilities to the competent authorities for the implementation of court and administrative orders that have to do with tracking communications specified in these orders.

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.

Section 3 - Competence	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish its jurisdiction over any criminal offence established in accordance with Articles 2 to 11 of this Convention, when the offence is committed: a on its territory; or b on board a vessel flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence does not fall within the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply, or to apply only in specific cases or conditions, the jurisdictional rules set out in paragraphs 1.b to 1.d of this article or in any part of those paragraphs. 3 Each Party shall adopt such measures as may be necessary to establish its jurisdiction over any of the offences referred to in Article 24, paragraph 1, of this Convention, where the alleged offender is present in its territory and cannot be extradited to another Party solely on the basis of his or her nationality, following a request for extradition.	**Electronic Crimes Law number 17 of 2023 Article 37 states** public right and personal right lawsuits are filed against the defendant before the competent judicial authority if any of the crimes stipulated in this Law were committed using the information network, information technology, information system, social media platform, website, or any electronic publishing means inside the Kingdom, or committed outside Kingdom and caused damage to any of its interests, citizens or residents, or resulted in the effects of the crime in whole or in part.

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 o v e r an alleged offence referred to in this Convention, the Parties concerned shall, where appropriate, consult with a view to determining the Party best able to prosecute.	

Chapter III - International cooperation

Section 1 - General principles
Title 1 - General principles relating to international cooperation

Article 24 – Extradition 1 a This article shall apply to extradition between the Parties for the criminal offences defined in accordance with Articles 2 to 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period o f 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, t h e 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 m a k e s 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	Jordan adopts bilateral extradition agreements with individual governments and then adopts a supporting legal framework in the Parliament. A review of the current agreements in place is not available and should be considered as a requirement for the CyberSouth project.

in respect of any criminal offence mentioned in paragraph 1 of this article. 4 Parties which do not m a k e 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 I f extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality o f 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 t h e outcome of t h e 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 o f ratification, acceptance, approval or accession, the name and address o f 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 t h e accuracy of the data contained in the register.	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another the widest measure of	Jordan does not have specific legislation enabling international legal cooperation in general. It therefore does not have most of the specific powers required by the Budapest Convention. It reported in 2021 that it was working on a draft international cooperation law.

mutual assistance for the purposes of investigations or proceedings concerning criminal offences relating to computer systems and data, or for t h e 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, i n 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 m a k e 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 MOJ is the Central Authority in Jordan that deals with MLA between Jordan and other countries. (More information - https://rm.coe.int/3692-4-1-study-int-coop-jordan-lebanon-final/1680a1a5d9)
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 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.	

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 s h a l l 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 t o send or respond to requests f o r 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 o f Europe the names and addresses of the authorities
	Jordan does not have specific legislation enabling international legal cooperation in general. It therefore does not have most of the specific powers required by the Budapest Convention. It reported in 2021 that it was working on a draft international cooperation law.
	
	The MOJ is the Central Authority in Jordan that deals with MLA between Jordan and other countries.
	
	(More information - https://rm.coe.int/3692-4-1-study-int-coop-jordan-lebanon-final/1680a1a5d9)

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.	Jordan does not have specific legislation enabling international legal cooperation in general. It therefore does not have most of the specific powers required by the Budapest Convention. It reported in 2021 that it was working on a draft international cooperation law. The MOJ is the Central Authority in Jordan that deals with MLA between Jordan and other countries.

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.	(More information - https://rm.coe.int/3692-4-1-study-int-coop-jordan-lebanon-final/1680a1a5d9)

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;	**No relevant legislation in place**

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.	**No relevant legislation in place**
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 relevant data are particularly sensitive to the risk of loss or modification; or
    b   the instruments, arrangements and legislation
	No relevant legislation in place

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.
	No relevant legislation in place

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.	**No relevant legislation in place**
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.	**No relevant legislation in place**
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.	Jordan is not a party to the Budapest Convention on Cybercrime and does not have a dedicated 24/7 point of contact. The PSD CCU currently undertakes numerous requests of partners afforded through networks it has made through the CyberSouth project and other activities. But it is not receiving sufficient responses from US based MNSP such as Gmail, Facebook etc. Accession to the Cybercrime Convention could provide a good framework to improve 24/7 requests. Whilst Jordan has good international relationships with many partners, information sharing will be more meaningful if intelligence and evidence can be undertaken under the auspices of Article 25 of the Convention.
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.	