# Jamaica

## Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

## Table of contents

*Version 11 February 2022*

[reference to the provisions of the Budapest Convention]



*This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.*



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

| State: | |
|---|---|
| **Signature of the Budapest Convention:** | N/A |
| **Ratification/accession:** | N/A |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Chapter I – Use of terms** | |
| **Article 1 – "Computer system", "computer data", "service provider", "traffic data":**<br>For the purposes of this Convention:<br>a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;<br><br>b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;<br>c "service provider" means:<br><br>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and<br>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;<br>d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service | **Cybercrimes Act (2015)**<br><br>**Part I. Preliminary**<br>**Section 2 (Interpretation)**<br>¨computer¨means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data and –<br>(a) includes any data storage facility or electronic communications system directly connected to or operating in conjunction with such device or group of such interconnected or related devices;<br>(b) does not include such devices as the Minister may prescribe by order published in the Gazette.<br>"computer service" includes provision of access to any computer or to any function of a computer, computer output, data processing and the storage or retrieval of any program or data;<br>"data" includes –<br>(a) Material in whatever form stored electronically;<br>(b) The whole or part of a computer program; and<br>(c) Any representation of information or of concepts in a form suitable for use in a computer, including a program suitable to cause a computer to perform a function; |
| **Chapter II – Measures to be taken at the 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**<br>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when | **Cybercrimes Act (2015)**<br><br>**Part II. Offences** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. | **Section 3 (Unauthorised access to computer program or data)**<br>(1) A person who knowingly obtains, for himself or another person, any unauthorised access to any program or data held in a computer commits an offence.<br>(2) The intent required for the commission of an offence under subsection (1) need to be directed at-<br>(a) any specifically identifiable program or data;<br>(b) a program or data of any specifically identifiable kind; or<br>(c) a program or data held in any specifically identifiable computer.<br>(3) A person who commits an offence under subsection(1) is liable upon –<br>(a) summary conviction before a Resident Magistrate to-<br>(i) in the case of a first offence, a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;<br>(b) Conviction on indictment before a Circuit Court to –<br>(i) in the case of a first offence, a fine or imprisonment for a term not exceeding sever years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years.<br><br>**Section 4 (Access with intent to commit or facilitate commission of offence)**<br>(1) A person commits an offence if that person accesses any program or data held in a computer with the intent to –<br>(a) commit any offence punishable by imprisonment for a term that exceeds one year; or<br>(b) facilitate the commission of an offence reffered to in paragraph (a),whether by himself or by any other person.<br>(2) A person may commit an offence under subsection (1) even if the facts are such that the commission of the offence reffered to in subsection (1) (a) is impossible. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (3) For the purpose of this section, it is immaterial whether-<br>(a) the access referred to in subsection (1) is with or without authorisation;<br>(b) the offence reffered to in subsection (1)(a) is committed at the same time when the access is secured or to any other time.<br>(4) A person who commits an offence under subsection (1) is liable upon<br>(a) summary conviction before a Resident Magistrate to-<br>(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years.<br>(b) conviction on indictment before a Circuit Court to-<br>(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;<br>(ii) if any damae is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years. |
| **Article 3 – Illegal interception**<br>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, the interception without right, made by technical means, of non-public transmissions of computer data 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 dishonest intent, or in relation to a computer system that is connected to another computer system. | **Cybercrimes Act (2015)**<br><br>**Part II. Offences**<br><br>**Section 6 (Unauthorised interception of computer function or service)**<br>(1) A person commits an offence if that person knowingly –<br>(a) secures unauthorised access to any computer for the purpose of obtaining, directly or indirectly, any computer service; or<br>(b) without authorisation, directly or indirectly intercepts or causes to be intercepted any function of a computer.<br>(2) For the purposes of subsection (1), the access or interception referred to need not to be directed at –<br>(a) any specifically identifiable program or data or type of program or data; or<br>(b) any program or data held in a specifically identifiable computer. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (3) Subsection (1) shall not apply to any interception permitted under the provisions of the Interception of Communications Act.<br>(4) For the purposes of this section, intercepting includes listening to or viewing, by use of technical means, or recording, a function of a computer or acquiring the substance, meaning or purport of any such function.<br>(5) A person who commits an offence under subsection (1) is liable upon –<br>(a) summary conviction before a Resident Magistrate to-<br>(i) in the case of a first offence, a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;<br>(b) convication on indictment before a Circuit Court, to –<br>(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years. |
| **Article 4 – Data interference**<br>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, the damaging, deletion, deterioration, alteration or suppression of computer data without right.<br>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. | **Cybercrimes Act (2015)**<br><br>**Part II. Offences**<br>**Section 5 (Unauthorised modification of computer program or data)**<br>(1) A person who does any act which that person knows is likely to cause any authorised modification of the contents of any computer, commits an offence.<br>(2) For the purpose of subsection (1) –<br>(a) the act in question need to be directed at –<br>(i) any specifically identifiable program or data or type of program or data;<br>(ii) any program or data held in a specifically identifiable computer; and<br>(b) it is immaterial whether the modification is, or is intended to be, permanent or temporary. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (3) A person who commits an offence under subsection (1) is liable upon –<br>(a) summary conviction before a Resident Magistrate to –<br>(i) in the case of a first offence, a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not excedeeing four years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;<br>(b) conviction on indictment before a Circuit Court to-<br>(i) in the case of a first offence, a fine or imprisonment for a term not exceeding seven years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonmenet for a term not exceeding ten years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonmenet for a term not exceeding fifteen years. |
| **Article 5 – System interference**<br>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, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data | **Cybercrimes Act (2015)**<br><br>**Part II. Offences**<br>**Section 7 (Unauthorised obstruction of operation of computer)**<br>(1) A person commits an offence if that person, without authorization or without lawful justification or excuse, wilfully causes, directly or indirectly -<br>(a) a degradation, failure, interruption or obstruction of the operation of a computer; or<br>(b) a denial of access to, or impairment of, anu program or data stored in a computer.<br>(2) A person who commits an offence under subsection (1) is liable upon –<br>(a) summary conviction before a Resident Magistrate, to –<br>(i) in the case of a first offence, a fine not exceeding three million dollars or to imprisonment for a term not exceeding three years; or<br>(ii) if any daumage is caused as a result of the commission of the offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years; or |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;<br>(b) conviction on indictment before a Circuit Court, to –<br>(i) in the case of a first offence, a fine or imprisonement for a term not exceeding seven years; or<br>(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding ten years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding fifteen years. |
| **Article 6 – Misuse of devices**<br>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:<br>a the production, sale, procurement for use, import, distribution or otherwise making available of:<br>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;<br>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,<br>with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and<br><br>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.<br><br>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. | **Cybercrimes Act (2015)**<br><br>**Part II. Offences**<br>**Section 8 (Computer related fraud or forgery)**<br>(1) A person commits an offence if that person fraudulently, with intent to procure an advantage for himself or another person -<br>(a) causes loss of property to another person by any –<br>(i) input, alteration, deletion or suppression of data; or<br>(ii) interference with any function of a computer; or<br>(b) accesses any computer and inputs, alters, deletes or suppresses any data ("the original data") with the intention that the data, after such input, alteration, deletion or suppression (whether or not that data is readable or intelligible), be considered or acted upon as if that data were the original data.<br>(2) A person who commits an offence under subsection (1) shall be liable upon –<br>(a) summary conviction before a Resident Magistrate, to –<br>(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;<br>(b) conviction on indictement before a Circuit Court to –<br>(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article. | (ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years.<br><br>**Section 10 (Unlawfully making available devices or data for commission of offence)**<br>(1) A person commits an offence who, for the purpose of committing, or facilitating the commission of, an offence under any of sections 3 to 9, possesses, receives, manufactures, sells, imports, distributes, discloses or otherwise makes available-<br>(a) a computer;<br>(b) any key; or<br>(c) any other data or device,<br>designed or adapted primarly for the purpose of committing an offence under any of sections 3 to 9.<br>(2) A person who comits an offence under subsection (1) is liable upon –<br>(a) summary conviction before a Resident Magistrate, to –<br>(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;<br>(b) conviction before a Circuit Court to –<br>(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Title 2 – Computer-related offences** | |
| **Article 7 – Computer-related forgery**<br>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 input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches. | **Cybercrimes Act (2015)**<br><br>**Part II. Offences**<br>**Section 8 (Computer related fraud or forgery)**<br>(1) A person commits an offence if that person fraudulently, with intent to procure an advantage for himself or another person -<br>(a) causes loss of property to another person by any –<br>(i) input, alteration, deletion or suppression of data; or<br>(ii) interference with any function of a computer; or<br>(b) accesses any computer and inputs, alters, deletes or suppresses any data ("the original data") with the intention that the data, after such input, alteration, deletion or suppression (whether or not that data is readable or intelligible), be considered or acted upon as if that data were the original data.<br>(2) A person who commits an offence under subsection (1) shall be liable upon –<br>(a) summary conviction before a Resident Magistrate, to –<br>(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;<br>(b) conviction on indictement before a Circuit Court to –<br>(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years. |
| **Article 8 – Computer-related fraud**<br>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when | **Cybercrimes Act (2015)**<br><br>**Part II. Offences**<br>**Section 8 (Computer related fraud or forgery)** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| committed intentionally and without right, the causing of a loss of property to another person by:<br><br>a any input, alteration, deletion or suppression of computer data;<br><br>b any interference with the functioning of a computer system,<br><br>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. | (1) A person commits an offence if that person fraudulently, with intent to procure an advantage for himself or another person -<br>(a) causes loss of property to another person by any –<br>(i) input, alteration, deletion or suppression of data; or<br>(ii) interference with any function of a computer; or<br>(b) accesses any computer and inputs, alters, deletes or suppresses any data ("the original data") with the intention that the data, after such input, alteration, deletion or suppression (whether or not that data is readable or intelligible), be considered or acted upon as if that data were the original data.<br>(2) A person who commits an offence under subsection (1) shall be liable upon –<br>(a) summary conviction before a Resident Magistrate, to –<br>(i) in the case of a first offence, a fine not exceeding four million dollars or imprisonment for a term not exceeding four years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine not exceeding five million dollars or imprisonment for a term not exceeding five years;<br>(b) conviction on indictement before a Circuit Court to –<br>(i) in the case of a first offence, a fine or imprisonment for a term not exceeding ten years;<br>(ii) if any damage is caused as a result of the commission of the offence, a fine or imprisonment for a term not exceeding fifteen years; or<br>(iii) in the case of a second or subsequent offence, regardless of whether or not any damage is caused, a fine or imprisonment for a term not exceeding twenty years. |
| | |
| **Article 9 – Offences related to child pornography**<br>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, the following conduct:<br>a producing child pornography for the purpose of its distribution through a computer system;<br>b offering or making available child pornography through a computer system; | **Child Pornography (Prevention) Act (2009)**<br><br>**Section 4 (Producing, distributing, etd., child pornography)**<br>(1) A person commits an offence who knowingly -<br>(a) produces child pornography;<br>(b) distributes, imports or exports child pornography; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| c distributing or transmitting child pornography through a computer system;<br>d procuring child pornography through a computer system for oneself or for another person;<br>e possessing child pornography in a computer system or on a computer-data storage medium.<br><br>2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:<br>a a minor engaged in sexually explicit conduct;<br>b a person appearing to be a minor engaged in sexually explicit conduct;<br>c realistic images representing a minor engaged in sexually explicit conduct<br><br>3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.<br><br>4 Each 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. | (c) distributes any advertisement likely to be'understood as conveying that the advertiser or any other person proouces, distributes, imports, or exports, any child pornography; or<br>(d) possesses any child pornography for the purpose of distributing, importing, or exporting, it.<br>(2) In this Act, distributing child pornography includes selling it or publishing it in any form, and parting with possession ofchild pornography by exposing or offering it for acquisition by another person.<br>(3) A person who commits an offence under –<br>(a) subsection (l)(a) is liable, on conviction on indictment before a Circuit Court, to a tine or to imprisonment for a term not exceeding twenty years, or to both such fine and imprisonment;<br>(b) subsection (l)(b), (c) or (d) is liable, on conviction on indictment before a Circuit Court, to a fine or to imprisonment for a term not exceeding fifteen years, or to both such fine and imprisonment. |
| **Title 4 – Offences related to infringements of copyright and related rights** | |
| **Article 10 – Offences related to infringements of copyright and related rights**<br>1 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 copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.<br>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the | **Copyright Act (1993) and Copyright (Amendment) Act (2015)**<br><br>**Section 114 (Infringement of recording rights by importing, proceedings, etc. ilicit recording.**<br>(1) A person infringes the rights of a person having recording rights in relation to a performance who, without his consent -<br>(a) imports into Jamaica otherwise than for his private and domestic use; or<br>(b) in the course of a business, possesses, sells or lets for hire, offers or exposes for sale or hire, or distributes,<br>A recording of the performance which is, and which that person knows or has reason to believe is, an illicit recording. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (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 such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.<br>3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article. | **Section 25 (Amendment of section 114 of principal Act)**<br>Section 114 of the Principal Act is amended in subsection (1) by –<br>(c) inserting next after paragraphe (b) as amended, the following as paragraphs (c), (d) –<br>(c) rents of distributes n unauthorized recording of the whole or a substantial part of the performance;<br>(d) makes the whole or a substantial part of the performance available to the public by means of a recording made accessible, or communicated to the public by means of any form of technology that allows a member of the public to access the performance from a place and at a time chosen by the member of the public |
| **Title 5 – Ancillary liability and sanctions** | |
| **Article 11 – Attempt and aiding or abetting**<br>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 through 10 of the present Convention with intent that such offence be committed.<br>2 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, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.<br>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article. | **Cybercrimes Act (2015)**<br><br>**Part II. Offences**<br>**Section 12 (Inciting, etc.)**<br>A person who intentionallu incites, attempts, aids or abets the commission of any offence under any of sections 3 to 10 ("the substantive offence"), or conspires with another person to commit the substantive offence, commits an offense and shall be liable to the same penalty as applies to the substantive offence, and to be proceeded against and punished accordingly. |
| **Article 12 – Corporate liability**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence 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 it, based on:<br>a a power of representation of the legal person; | **Cybercrimes Act (2015)**<br><br>**Part II. Offences**<br>**Section 14 (Offences by bodies corporate)**<br>(1) For the avoidance of doubt, where a body corporate commits an offence under this Act, the body corporate shall be liable to the fine applicable in respect of the offence. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| b an authority to take decisions on behalf of the legal person;<br>c an authority to exercise control within the legal person.<br>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures 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 a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.<br>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.<br>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence. | (2) Where a body corporate commits an offence under this Act and the court is satisfied that a director, manager, secretary, or other similar officer, of that body corporate –<br>(a) connived in the commission of the offence, that director, manager, secretary, or other similar officer, shall also be liable to be proceeded against for the offence and punished accordingly;or<br>(b) failed to exercise due diligence to prevent the commission of the offence, that director, manager, secretary, or other similar officer, shalle be liable –<br>(i) on conviction before a Resident Magistrate, to a fine not exceeding two million dollars or imprisonment for a term not exceeding two years;<br>(ii) on conviction on indictment before a Circuit Court to a fine or imprisonment for a term not exceeding six years. |
| **Article 13 – Sanctions and measures**<br>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 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.<br>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions. | Each offence in the Act contains sanctions including deprivation of liberty and monetary sanctions. |
| ***Section 2 – Procedural law*** | |
| **Article 14 – Scope of procedural provisions**<br>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.<br>2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:<br>a the criminal offences established in accordance with Articles 2 through 11 of this Convention;<br>b other criminal offences committed by means of a computer system; and<br>c the collection of evidence in electronic form of a criminal offence.<br>3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.<br>b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:<br>i is being operated for the benefit of a closed group of users, and<br>ii does not employ public communications networks and is not connected with another computer system, whether public or private,<br>that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21 | |
| **Article 15 – Conditions and safeguards**<br>1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.<br>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.<br><br>3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the | **Charter of Fundamental Rights and Freedoms (Constitutional Amendment) Act (2011)**<br><br>**Chapter III. Chapter of Fundamental Rights and Freedoms**<br>**Section 13 (Fundamental rights and freedoms)**<br>(1) Whereas –<br>(a) the state has an obligation to promote universal respect for, and observance of, human rights and freedoms;<br>(b) all persons in Jamaica are entitled to preserve for themselves and future generations the fundamental rights and freedoms to which they are entitled by virtue of their inherent dignity as persons and as citizens of a free and democratic<br>society; and<br>(c) all persons are under a responsibility to respect and uphold the rights of others<br>recognized in this Chapter, the following provisions ofthis Chapter shall have effect for the purpose of affording protection to the rights and freedoms of persons as set out in those provisions, to the extent that those rights and freedoms do not prejudice the rights and freedoms of others. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties. | (3) The rights and freedoms referred to in subsection (2) are as follows –<br>(a) the right to life, liberty and security ofthe person and the right not to be deprived thereof except in the execution of the sentence of a court in respect of a criminal offence of which the person has been convicted;<br>(g) the right to equality before the law;<br>(h) the right to equitable and humane treatment by any public authority in the exercise of any function;<br>(j) the right of everyone to-<br>(i) protection from search of the person and property;<br>(ii) respect for and protection of private and family life, and privacy of the home; and<br>(ill) protection of privacy of other property and of communication;<br><br>**Section 15 (Protection of property rights)**<br>(1) No property of any description shall be compulsorily taken possession of and no interest in or right over property of any description shall be compulsorily acquired except by or under the provisions of a law that -<br>(a) prescribes the principles on which and the manner in which compensation therefor is to be determined and given; and<br>(b) secures to any person claiming an interest in or right over such property a right of access to a court for the purpose<br>(i) establishing such interest or right (if any);<br>(ii) determining the compensation (if any) to which he is entitled; and<br>(iii) enforcing his right to any such compensation.<br>(2) Nothing in this section shall be construed as affecting the making or operation of any law so far as it provides for the taking of possession or acquisition of property –<br>(b) by way of penalty for breach of the law, whether under civil process or after conviction of a criminal offence;<br>(c) upon the attempted removal of the property in question out of or into Jamaica in contravention of any law;<br>(d) by way of the taking of a sample for the purposes of any law;<br>(h) in the execution of judgments or orders of courts;<br>(g) in consequence of any law with respect to the limitation of actions;<br><br>**Section 16 (Protection of right due to process)**<br>(1) Whenever any person is charged with a criminal offence he shall, unless the charge is withdrawn, be afforded a fair hearing within a reasonable time by an independent and impartial court established by law. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | In 2020, Jamaica adopted the Data Protection Act of 2020, which sets out the rights of data subjects, requirements for data controllers, standards and exemptions for processing personal data and enforcement provisions. |
| **Article 16 – Expedited preservation of stored computer data**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.<br><br>2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.<br><br>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.<br><br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | **Cybercrimes Act (2015)**<br><br>**Part III. Investigations**<br>**Section 17 (Preservation of data)**<br>(1) Where a constable is satisfied that -<br>(a) data stored in a computer or any data storage medium is reasonably required for the purposes of a criminal investigation; and<br>(b) there are reasonable grounds for suspecting that the data may be destroyed or rendered inaccessible,<br>the constable may, by notice in accordance with subsection (2) given to the person in possession or control of the computer or data storage medium (as the case may be), require the person to ensure that the data be preserved.<br>(2) The notice referred to in subsection (1) shall be in writing and shall specify –<br>(a) the name of the person in possession or control of the computer or data storage medium (as the case may be) or the address where the computer or data storage medium (as the case may be) is located;<br>(b) the period for which the data is required to be preserved, being a period not exceeding sixty days; and<br>(c) the requirements to be complied with for the preservation of the data.<br>(3) For the purposes of subsection (2), "address" includes a location, e-mail address, telephone number or other number or designation used for the purpose of identifying a computer or electronic communications system.<br>(4) The period specified under subsection (2), or any previous order made under this subsection, may be extended, upon the order of a Resident Magistrate on an application without notice, for such further period as may be specified by the Resident Magistrate in the order.<br>(5) A person commits an offence if the person fails, without reasonable excuse, to comply with a requirement imposed on that person by a notice or under this section.<br>(6) A person commits an offence if, in purpoted compliance with a requirement imposed on that person under a notice or order made under this section, the person –<br>(a) makes a statement that the person knows to be false or misleading in a material particular; or<br>(b) recklessly makes a statement that is false or misleading in a material particular.<br>(7) A person who commits an offence under subsection (5) or (6) is liable – |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (a) upon conviction before a Resident Magistrate, to a fine not exceeding three million dollars or imprisonment for a term not exceeding three years;<br>(b) upon conviction on indictment before a Circuit Court, to a fine or imprisonement for a term not exceeding seven years. |
| **Article 17 – Expedited preservation and partial disclosure of traffic data**<br>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:<br>a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and<br>b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.<br><br>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 18 – Production order**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:<br>a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and<br>b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.<br><br>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.<br>3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: | **Cybercrimes Act (2015)**<br><br>**Part III. Investigations**<br>**Section 21 (Production orders)**<br>(1) A Resident Magistrate, if satisfied on the basis of an application made by a constable, that any data or other computer output specified in the application is reasonably required for the purpose of a criminal investigation or criminal proceedings, may make an order under subsection (2).<br>(2) An order under this subsection may require a person in possession or control of the data or other computer output to produce it in intelligible form to the constable.<br>(3) Where a production order requires the person to whom it is addressed to produce any data or other computer output in intelligible fomr that person –<br>(a) shall be entitled to use any key in his possession or control to obtain access to the data or output;<br>(b) shall be taken to have produced the data or output in intelligible form if –<br>(i) the person makes, instead, a disclosure of any key to the data or output; and |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| a the type of communication service used, the technical provisions taken thereto and the period of service;<br>b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;<br>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. | (ii) the data or output is produced in accordance with the order, with respect to the person to whom, and the time in which, the person was ordered to produce the data or output.<br>(4) Where a constable has reasonable grounds to believe that –<br>(a) a key to any data or other computer output is in the possession of any person; and<br>(b) the production of the key is necessary for the purposes of the investigation in relation to which –<br>(i) the constable makes, or intends to make, and application for a production order; or<br>(ii) a production order has been issued to the constable,<br>the constable may apply to the Resident Magistrate for such ancillary order, as may be required in the circumstances, to be included in the production order. |
| **Article 19 – Search and seizure of stored computer data**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:<br>a a computer system or part of it and computer data stored therein; and<br>b a computer-data storage medium in which computer data may be stored<br>in its territory.<br>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 of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.<br>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:<br>a seize or similarly secure a computer system or part of it or a computer-data storage medium;<br>b make and retain a copy of those computer data;<br>c maintain the integrity of the relevant stored computer data;<br>d render inaccessible or remove those computer data in the accessed computer system. | **Cybercrimes Act (2015)**<br><br>**Part III. Investigations**<br>**Section 18 (Search and seizure warrants)**<br>(1) A Resident Magistrate may issue a warrant under this subsection, if satisfied by information on oath that there are reasonable grounds to suspect that there may be in any place any computer material that -<br>(a) may be relevant as evidence in proving an offence;or<br>(b) has been acquired by a person for, or in, the commission of and offence or as a result of the commission of an offence.<br>(2) A warrant under subsection (1) shall authorize a constable, with such assistance as may be necessary, to enter the place specified in the warrant to search for and seize the computer material.<br><br>**Section 19 (Record of seized material)**<br>(1) If any computer material is seized or rendered inaccessible in the execution of a warrant under section 18(1), the person who executed the warrant shall, during the execution, or as soon as possible thereafter -<br>(a) make a list of what has been seized or rendered inaccessible; and<br>(b) give a copy of the list to the person to whom the warrant is addressed or the occupier of the premises on which the warrant is executed.<br>(2) A person who, immediately before the execution of a warrant, had possession or control of data seized in the execution, may request a copy of the data from the constable who executed the warrant, and the constable shall, as soon as is reasonable practicable, comply with the request if the conditions under subsection (3) are satisfied. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.<br>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | (3) The conditions referred to in subsection (2) are that providing the copy would not –<br>(a) constitute or facilitate the commission of a criminale offence; or<br>(b) prejudice –<br>(i) the investigation in relation to which the warrant was issued;<br>(ii) another ongoing investigation; or<br>(iii) any criminal proceedings that may be brought in relation to any investigation mentioned in sub-paragraph (i) or (ii).<br>(4) A person who executed a warrant under section 18(1) shall take all reasonable steps to preserve the computer material seized or rendered inaccessible.<br>(5) A person who contravenes subsection (4) commits an offence and is liable upon conviction before a Resident Magistrate, to a fine not exceeding three million dollars, or in default of payment thereof to a term of imprisonment not exceeding three years.<br>(6) Where computer material is seized or rendered inaccessible in the execution of a warrnt under section 18(1), a person commits an offence if that person –<br>(a) uses the date comprised in the computer material for any purpose otherwise than in accordance with this Act; or<br>(b) discloses such data other than for the purposes of this Act,<br>is liable upon conviction before a Resident Magistrate to a fine not exceeding three million dollars or, in default of payment thereof, to a term of imprisonment not exceeding three years. |
| **Article 20 – Real-time collection of traffic data**<br>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:<br>a collect or record through the application of technical means on the territory of that Party, and<br>b compel a service provider, within its existing technical capability:<br>i to collect or record through the application of technical means on the territory of that Party; or<br>ii to co-operate and assist the competent authorities in the collection or recording of,<br>traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.<br>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.<br>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.<br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | |
| **Article 21 – Interception of content data**<br>1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:<br>a collect or record through the application of technical means on the territory of that Party, and<br>b compel a service provider, within its existing technical capability:<br>i to collect or record through the application of technical means on the territory of that Party, or<br>ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.<br>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.<br>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.<br>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. | **Interception of Communications Act (2002)** |
| | |
| **Article 22 – Jurisdiction** | **Cybercrimes Act (2015)** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:<br>a in its territory; or<br>b on board a ship flying the flag of that Party; or<br>c on board an aircraft registered under the laws of that Party; or<br>d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.<br>2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.<br>3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.<br>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.<br>When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution. | **Part IV. General**<br>**Section 22 (Jurisdiction)**<br>(1) This Act applies in respect of conduct occurring -<br>(a) wholly or partly in Jamaica;<br>(b) wholly or partly on board a Jamaican ship or Jamaican aircraft;<br>(c) wholly outside of Jamaica and attributable to a Jamaican national; or<br>(d) wholly outside of Jamaica, if the conduct affects a computer or dat –<br>(i) wholly or partly in Jamaica; or<br>(ii) wholly or partly on borad a Jamaican ship or Jamaican aircraft. |
| | |
| **Article 24 – Extradition**<br>1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 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.<br><br>b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. | **Extradition Act (1991)** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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 to be concluded between or among them.<br>3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.<br>4 Parties that 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.<br>5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.<br>6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.<br>7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.<br><br>b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure | |
| **Article 25 – General principles relating to mutual assistance** | **Mutual Assistance in Criminal Matters Act (1995)**<br><br>**Part III. Requests by Foreign States** |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.<br><br>2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.<br><br>3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.<br><br>4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.<br><br>5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws. | **Section 15 (Provision of assistance under this Part)**<br>(1) Assistance may be provided to a foreign state, on request, in accordance with this Part.<br>(2) Assistance provided under this Part shall be in respect, of investigations and proceedings in relation to a criminal matter and such assistance may be provided as aforesaid-<br>(a) to the foreign state which makes a request for the purposes only of the criminal law enforcement authorities in that state; and<br>(b) only if criminal proceedings have been instituted in that state or if there is reasonable cause to believe that an offence in respect of which such proceedings<br>could be instituted, has been or is likely to be committed.<br>(3) Assistance under 'this Part may be provided in relation' to-<br>(a) the location and identification of persons and objects;<br>(b) the examination and taking of testimony of witnesses;<br>(c) the production of-<br>(i) documents and other records, including judicial or official records; and<br>(ii) other articles;<br>(d) the making of arrangements for persons to give evidence or assist investigations;<br>(e) the temporary transfer of persons in custody for the giving of testimony;<br>(f) the carrying out of search and seizure;<br>(g) the service of documents;<br>(h) the restraining of dealings in property, or the freezing of assets that may be forfeited or that may be needed to satisfy orders which are similar to pecuniary penalty orders imposed in respect of a prescribed offence;<br>(i) the tracing, seizure and forfeiture of property that may be subject to a forfeiture order in force for the time being in relation to a prescribed offence in the foreign state which makes a request;<br>(j) the interception of communications in accordance with the Interception of Communications Act;<br>(k) the disclosure of communications data in accordance with the provisions of the Interception of Communications Act;<br>(l) such other matters as may be included in an agreement or arrangement in force between Jamaica and a foreign state.<br>(4) Requests made by a foreign state shall be made in writing to the Central Authority and shall contain such of the particulars set out in the First Schedule as the Central Authority may require, but without prejudice to the requirement for |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | such additional information as may be considered necessary for the purpose of giving effect to the request.<br><br>**Section 23 (Requests by a relevant foreign state for search and seizure)**<br>(1) Where -<br>(a) a proceeding or investigation relating to a criminal search and matter has commenced in a relevant foreign state;<br>(b) there are reasonable grounds for believing that an article (not beiig tainted property) relevant to the proceeding or investigation is located in Jamaica;<br>and<br>(c) the relevant foreign state requests the Central Authority to arrange for the issue of a search warrant under this section in relation to that article,<br>the Central Authority may authorize a police officer to apply to a Resident Magistrate for the search warrant requested by the relevant foreign state. |
| **Article 26 – Spontaneous information**<br>1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.<br><br>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them. | |
| **Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements**<br>1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. | **Mutual Assistance in Criminal Matters Act (1995)**<br><br>**Part III. Requests by Foreign States**<br>**Section 15 (Provision of assistance under this Part)**<br>(1) Assistance may be provided to a foreign state, on request, in accordance with this Part. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.<br>2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.<br>b The central authorities shall communicate directly with each other;<br>c Each Party shall, at the time of signature or when depositing its instrument 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 pursuance of this paragraph;<br>d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.<br>3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.<br>4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:<br>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or<br>b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.<br>5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.<br>6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.<br>7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. | (2) Assistance provided under this Part shall be in respect, of investigations and proceedings in relation to a criminal matter and such assistance may be provided as aforesaid-<br>(a) to the foreign state which makes a request for the purposes only of the criminal law enforcement authorities in that state; and<br>(b) only if criminal proceedings have been instituted in that state or if there is reasonable cause to believe that an offence in respect of which such proceedings<br>could be instituted, has been or is likely to be committed.<br>(3) Assistance under 'this Part may be provided in relation' to-<br>(a) the location and identification of persons and objects;<br>(b) the examination and taking of testimony of witnesses;<br>(c) the production of-<br>(i) documents and other records, including judicial or official records; and<br>(ii) other articles;<br>(d) the making of arrangements for persons to give evidence or assist investigations;<br>(e) the temporary transfer of persons in custody for the giving of testimony;<br>(f) the carrying out of search and seizure;<br>(g) the service of documents;<br>(h) the restraining of dealings in property, or the freezing of assets that may be forfeited or that may be needed to satisfy orders which are similar to pecuniary penalty orders imposed in respect of a prescribed offence;<br>(i) the tracing, seizure and forfeiture of property that may be subject to a forfeiture order in force for the time being in relation to a prescribed offence in the foreign state which makes a request;<br>(j) the interception of communications in accordance with the Interception of Communications Act;<br>(k) the disclosure of communications data in accordance with the provisions of the Interception of Communications Act;<br>(l) such other matters as may be included in an agreement or arrangement in force between Jamaica and a foreign state.<br>(4) Requests made by a foreign state shall be made in writing to the Central Authority and shall contain such of the particulars set out in the First Schedule as the Central Authority may require, but without prejudice to the requirement for such additional information as may be considered necessary for the purpose of giving effect to the request. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.<br>9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.<br>b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).<br>c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.<br>d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.<br>e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority. | |
| **Article 28 – Confidentiality and limitation on use**<br>1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.<br>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: | **Mutual Assistance in Criminal Matters Act (1995)**<br><br>**Part III. Requests by Foreign States**<br>**Section 24 (Confidentiality of information or evidence, etc.)**<br>(1) Where assistance is provided to a foreign state in relation to the provision of information or evidence, the Central Authority may, subject to subsection (2), require that such information or evidence be kept confidential in accordance with such conditions as the Central Authority may specify. |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or<br>b not used for investigations or proceedings other than those stated in the request.<br>3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.<br>4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material. | (2) Subsection (1) shall not apply in any case where the information or evidence is required for the purpose of any criminal proceedings in the relevant foreign state. |
| **Article 29 – Expedited preservation of stored computer data**<br>1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.<br>2 A request for preservation made under paragraph 1 shall specify:<br>a the authority seeking the preservation;<br>b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;<br>c the stored computer data to be preserved and its relationship to the offence;<br>d any available information identifying the custodian of the stored computer data or the location of the computer system;<br>e the necessity of the preservation; and<br>f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.<br>3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.<br>4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.<br>5 In addition, a request for preservation may only be refused if:<br>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or<br>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.<br>6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.<br>4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request. | |
| **Article 30 – Expedited disclosure of preserved traffic data**<br>1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.<br>2 Disclosure of traffic data under paragraph 1 may only be withheld if:<br>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or<br>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | |
| **Article 31 – Mutual assistance regarding accessing of stored computer data**<br>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.<br>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.<br>3 The request shall be responded to on an expedited basis where:<br>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or<br>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation. | |
| **Article 32 – Trans-border access to stored computer data with consent or where publicly available**<br>A Party may, without the authorisation of another Party:<br>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or<br>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. | |
| **Article 33 – Mutual assistance in the real-time collection of traffic data**<br>1 The Parties shall provide mutual assistance to each other 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, this assistance shall be governed by the conditions and procedures provided for under domestic law.<br>2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case. | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| **Article 34 – Mutual assistance regarding the interception of content data**<br>The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws. | |
| **Article 35 – 24/7 Network**<br>1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings 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 facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:<br>a the provision of technical advice;<br>b the preservation of data pursuant to Articles 29 and 30;<br>c the collection of evidence, the provision of legal information, and locating of suspects.<br>2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.<br><br>b If the point of contact designated by a Party is not part of that Party's authority or authorities 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.<br><br>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network. | |
| **Article 42 – Reservations**<br>By a 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(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, | |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
| --- | --- |
| paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made. | |

Back to the Table of Contents