# ZIMBABWE

## Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

## Table of contents

*Version 22 April 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.*

**www.coe.int/cybercrime**

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 | **Cyber & Data Protection Act**<br>**PART XI CONSEQUENTIAL AMENDMENTS**<br>**35 Amendment of Chapter VIII of Cap. 9:23**<br>(1) The Criminal Law (Codification and Reform) Act [Chapter 9:23] (hereinafter called the "principal Act") is amended in section 162 by the repeal of the definitions of "computer virus", "data", "essential service" and "owner" and the substitution of the following definitions—<br>(…)<br>**"computer system"** means interconnected or related computer devices, one or more of which uses a programme to perform the automatic processing of data, exchange data with each other or any other computer system or connect to an electronic communications network;<br>(…)<br>**"data"** means any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data;<br>"**service provider**" means—<br>(a) any person that provides to users of its service the ability to communicate by means of information communication technology systems, and<br>(b) any person that processes or stores information and communications data on behalf of such communications service or users of such service; and includes— (c) access, caching and hosting provider;<br><br>"**traffic data**" means data relating to a communication by means of an information communications system or generated by an information communications system that forms a part of the chain of communications |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | indicating the communication's origin, destination, route, format, time, date, size, duration or type of the underlying service. |
| **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 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. | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments**<br>**35 Amendment of Chapter VIII of Cap. 9:23**<br>(1) The Criminal Law (Codification and Reform) Act [Chapter 9:23] (hereinafter called the "principal Act") is amended in section 162 by the repeal of the definitions of "computer virus", "data", "essential service" and "owner" and the substitution of the following definitions—<br>(…)<br>(2) The principal Act is amended by the repeal of sections 163 to 166 and the substitution of the following—<br><br>"**PART I Offences Relating to Computer Systems, Computer Data, Data Storage Mediums, Data Codes and Devices**"<br>**163 Hacking**<br>(1) A person who—<br>(a) knowing or suspecting that he or she must obtain prior authority to access the data, computer programme, computer data storage medium, or the whole or any part of a computer system in question; and<br>(b) intentionally, unlawfully and without such authority, secures access to such data, programme, medium or system;<br>shall be guilty of hacking and liable—<br>(c) in any of the aggravating circumstances described in section 13 to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years or both such fine and such imprisonment;<br>(d) in any other case, to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.<br><br>(2) For the purposes of this section "secure access" includes—<br>(a) to obtain, to make use of, gain entry into, view, display, instruct or communicate with, or store data in or retrieve data from; |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | (b) to copy, move, add, change or remove data, critical data or a critical database, or otherwise to make use of, configure or reconfigure any resources of a computer device, a computer network, a database, a critical database, an electronic communications network, a critical information infrastructure, whether in whole or in part, including their logical, arithmetical, memory, access codes, transmission, data storage, processor or memory function, whether physical, virtual, by direct or indirect means or by electronic, magnetic, audio, optical or any other means.<br><br>**CHAPTER VIII COMPUTER-RELATED CRIMES**<br>**163 Unauthorised access to or use of computer or computer network**<br>(1) Any person who, without authority from the owner of the computer or computer network, intentionally—<br>(a) gains access to; or<br>(b) destroys or alters; or<br>(c) renders meaningless, useless or ineffective; or<br>(d) copies or transfers; or<br>(e) obstructs, intercepts, diverts, interrupts or interferes with the use of;<br>any data, programme or system which is held in a computer or computer network shall be guilty of unauthorised access to or use of a computer or computer network and liable—<br>(i) if the crime was committed in any of the aggravating circumstances described in section one hundred and sixty-six, to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both; or<br>(ii) in any other case, to a fine not exceeding level eight or imprisonment for a period not exceeding three years or both.<br><br>(2) It shall be a defence to a charge of unauthorised access to or use of a computer for the accused to prove that he or she was not motivated by malice when engaging in the conduct constituting the crime, and that the conduct did not materially affect the data, programme or system in question nor the interests of the owner of the computer or computer network. |
| **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 | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments**<br>**35 Amendment of Chapter VIII of Cap. 9:23** |

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| 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. | (1) The Criminal Law (Codification and Reform) Act [Chapter 9:23] (hereinafter called the "principal Act") is amended in section 162 by the repeal of the definitions of "computer virus", "data", "essential service" and "owner" and the substitution of the following definitions—<br>(…)<br>(2) The principal Act is amended by the repeal of sections 163 to 166 and the substitution of the following—<br><br>"**PART I Offences Relating to Computer Systems, Computer Data, Data Storage Mediums, Data Codes and Devices**"<br>(…)<br>**163A Unlawful acquisition of data**<br>(1) Any person who unlawfully and intentionally—<br>(a) intercepts by technical or any other means any private transmission of computer data to, from or within a computer network, computer device, database or information system or electromagnetic emissions from a computer or information system carrying such computer data;<br>(b) overcomes or circumvents any protective security measure intended to prevent access to data; and<br>(c) acquires data within a computer system or data which is transmitted to or from a computer system;<br>shall be guilty of unlawful acquisition of data and shall be liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.<br><br>(2) Any person who unlawfully and intentionally possesses data knowing that such data was acquired unlawfully shall be guilty of unlawful possession of data and liable to a fine not exceeding level 14 or to imprisonment not exceeding five years or to both such fine and such imprisonment.<br><br>(3) For the purposes of this section "acquire" includes to use, examine, capture, copy, move to a different location or divert data to a destination other than its intended location.<br><br>(4) Any person who contravenes this section in any of the aggravating circumstances described in section 13 shall be liable to a fine not exceeding level |

Back to the Table of Contents

| BUDAPEST CONVENTION | DOMESTIC LEGISLATION |
|---|---|
| | 14 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment. |
| **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. | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments**<br>**35 Amendment of Chapter VIII of Cap. 9:23**<br>(1) The Criminal Law (Codification and Reform) Act [Chapter 9:23] (hereinafter called the "principal Act") is amended in section 162 by the repeal of the definitions of "computer virus", "data", "essential service" and "owner" and the substitution of the following definitions—<br>(…)<br>(2) The principal Act is amended by the repeal of sections 163 to 166 and the substitution of the following—<br><br>"**PART I Offences Relating to Computer Systems, Computer Data, Data Storage Mediums, Data Codes and Devices**"<br>(…)<br>**163B Unlawful interference with data or data storage medium**<br>(1) Any person who unlawfully and intentionally interferes with computer data or a data storage medium by—<br>(a) damaging, corrupting, impairing or deteriorating computer data; or<br>(b) deleting computer data; or<br>(c) altering computer data; or<br>(d) rendering computer data meaningless, useless or ineffective; or<br>(e) obstructing, interrupting or interfering with the lawful use of computer data; or<br>(f) obstructing, interrupting or interfering with any person in the lawful use of computer data; or<br>(g) denying, hindering, blocking access to computer data to any person authorised to access it; or<br>(h) maliciously creating, altering or manipulating any data, programme or system in whole or in part which is intended for installation in a computer;<br>shall be guilty of an offence and liable to a fine not exceeding level 10 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment. |

Back to the Table of Contents

| | |
|---|---|
| | (2) Any person who contravenes subsection (1) in any of the aggravating circumstances described in section 13 is liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years or to both such fine and such imprisonment. |
| **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 | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments**<br>**35 Amendment of Chapter VIII of Cap. 9:23**<br>(1) The Criminal Law (Codification and Reform) Act [Chapter 9:23] (hereinafter called the "principal Act") is amended in section 162 by the repeal of the definitions of "computer virus", "data", "essential service" and "owner" and the substitution of the following definitions—<br>(…)<br>(2) The principal Act is amended by the repeal of sections 163 to 166 and the substitution of the following—<br><br>"**PART I Offences Relating to Computer Systems, Computer Data, Data Storage Mediums, Data Codes and Devices**"<br>(…)<br>**163C Unlawful interference with computer system**<br>(1) Any person who unlawfully and intentionally interferes with the use of a computer or information system, computer device, an electronic communications system or critical information infrastructure by blocking, hindering, impeding, interrupting, altering or impairing the functioning of, access to or the integrity of, a computer device, computer or information system, an electronic communications network or critical information infrastructure shall be guilty of unlawful interference with computer or information system and liable to a fine not exceeding level 14 or to imprisonment not exceeding ten years or to both such fine and such imprisonment.<br><br>(2) Any person who contravenes subsection (1) in any of the aggravating circumstances described in section 13 is liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding twenty years or to both such fine and such imprisonment. |
| **Article 6 – Misuse of devices** | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments**<br>**35 Amendment of Chapter VIII of Cap. 9:23** |

Back to the Table of Contents

| | |
|---|---|
| 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.<br><br>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. | (1) The Criminal Law (Codification and Reform) Act [Chapter 9:23] (hereinafter called the "principal Act") is amended in section 162 by the repeal of the definitions of "computer virus", "data", "essential service" and "owner" and the substitution of the following definitions—<br>(…)<br>(2) The principal Act is amended by the repeal of sections 163 to 166 and the substitution of the following—<br><br>"**PART I Offences Relating to Computer Systems, Computer Data, Data Storage Mediums, Data Codes and Devices**"<br>(…)<br>**163D Unlawful disclosure of data code**<br>(1) Any person who unlawfully and intentionally—<br>(a) communicates, discloses or transmits any computer data, programme, access code or command or any other means of gaining access to any programme or data held in a computer or information system to any person not authorised to access the computer data, programme, code or command for any purpose;<br>(b) activates or installs or downloads a programme that is designed to create, destroy, mutilate, remove or modify any data, programme or other form of information existing within or outside a computer or computer system; or<br>(c) creates, alters or destroys a password, personal identification number, code or any method used to access a computer or computer network;<br>shall be guilty of an offence and liable to a fine not exceeding level 12 or imprisonment for a period not exceeding ten years or both such fine and such imprisonment.<br><br>(2) A person shall not be liable under this section if the action is—<br>(a) pursuant to measures that can be taken in terms of section 39; or<br>(b) authorised under the law.<br><br>(3) Where an offence under this section is committed in relation to data that forms part of a database or that involves national security or the provision of an essential service, the penalty shall be imprisonment for a period not exceeding ten years.<br>(4) For the purposes of this section, it is immaterial whether the intended effect of the illegal interference is permanent or merely temporary.<br><br>**163E Unlawful use of data or devices** |

Back to the Table of Contents

| | |
|---|---|
| | (1) Any person who unlawfully and intentionally acquires, possesses, produces, sells, procures for use, imports, distributes, supplies, uses or makes available an access code, password, a computer programme designed or adapted for the purpose of committing an offence or similar data or device by which the whole or any part of a computer or information system is capable of being accessed, for purposes of the commission or attempted commission of an offence in terms of this Act, shall be guilty of an offence and liable to a fine not exceeding level 12 or imprisonment for a period not exceeding ten years or both such fine and such imprisonment.<br><br>(2) Any person who unlawfully and intentionally assembles, obtains, sells, purchases, possesses, makes available, advertises or uses malicious software, programmes or devices for purposes of causing damage to data, computer or information systems and networks, electronic communications networks, critical information infrastructure or computer devices shall be guilty of an offence and liable to a fine not exceeding level 10 or imprisonment for a period not exceeding five years or both such fine and such imprisonment.<br><br>(3) Any person who contravenes this section in any of the aggravating circumstances described in section 13 shall be liable to a fine not exceeding level 12 or imprisonment for a period not exceeding ten years or to both such fine and such imprisonment. |
| **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. | **Criminal Law (Codification and Reform) Act**<br>**CHAPTER VI PROPERTY CRIMES**<br>**PART IV FRAUD AND FORGERY**<br>**135 Interpretation in Part IV of Chapter VI**<br>In this Part<br>(…)<br>"**document or item**" means an embodiment of any information, design or other written or depicted matter in any material form whatsoever that is capable of being read or understood by persons or machines and, without limiting this definition in any way, includes :<br>(…)<br>(e) information stored by electronic means that is capable of being printed out or retrieved or displayed on a screen or terminal;<br>(…) |

Back to the Table of Contents

| | |
|---|---|
| | **137 Forgery**<br>(1) Any person who forges any document or item by<br>(a) making a document or signature which purports to be made by a person who did not make it or authorise it to be made or by a person who does not exist; or<br>(b) tampering with a document or item by making some material alteration, erasure or obliteration;<br>with the intention of defrauding another person or realising that there is a real risk or possibility of defrauding another person thereby, shall be guilty of forgery and liable to<br>(i) in a case of forgery of a public document or item, a fine not exceeding level fourteen or imprisonment for a period not exceeding twenty years or both; or<br>(ii) in a case of forgery of a document or item other than a public document or item, a fine not exceeding level thirteen or imprisonment for a period not exceeding fifteen years or both.<br><br>(2) In a case where<br>(a) a person delivers or causes to be delivered a forged document or item to another person with the intention of defrauding that person or realising that there is a real risk or possibility of defrauding that person<br>(i) the competent charges shall be fraud and forgery if the person delivering the forged document or item or causing it to be delivered also forged it;<br>(ii) the competent charge shall be fraud if the person delivering the forged document or item or causing it to be delivered did not forge it;<br>(b) a banknote issued by the Reserve Bank of Zimbabwe is forged, the competent charge shall be that specified in section 42 of the Reserve Bank of Zimbabwe Act [Chapter 22:15]. |
| **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 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; | **Criminal Law (Codification and Reform) Act**<br>**CHAPTER VI PROPERTY CRIMES**<br>**PART IV FRAUD AND FORGERY**<br>**135 Interpretation in Part IV of Chapter VI**<br>In this Part<br>(…)<br>"**document or item**" means an embodiment of any information, design or other written or depicted matter in any material form whatsoever that is capable of |

Back to the Table of Contents

| | |
|---|---|
| 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. | being read or understood by persons or machines and, without limiting this definition in any way, includes :<br>(…)<br>(e) information stored by electronic means that is capable of being printed out or retrieved or displayed on a screen or terminal;<br>(…)<br><br>**136 Fraud**<br>Any person who makes a misrepresentation<br>(a) intending to deceive another person or realising that there is a real risk or possibility of deceiving another person; and<br>(b) intending to cause another person to act upon the misrepresentation to his or her prejudice, or realising that there is a real risk or possibility that another person may act upon the misrepresentation to his or her prejudice;<br>shall be guilty of fraud if the misrepresentation causes prejudice to another person or creates a real risk or possibility that another person might be prejudiced, and be liable to<br>i) a fine not exceeding level fourteen or not exceeding twice the value of any property obtained by him or her as a result of the crime, whichever is the greater; or<br>(ii) imprisonment for a period not exceeding thirty-five years;<br>or both. |
| **Title 3 – Content-related offences** | |
| **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;<br>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. | **Cyber & Data Protection Act**<br>**PART III OFFENCES AGAINST CHILDREN AND PROCEDURAL LAW**<br>**165A Child sexual abuse material**<br>(1) In this Act—<br>"**Child sexual abuse material**" means any representation through publication, exhibition, cinematography, electronic means or any other means whatsoever, of a child, a person made to appear as a child or realistic material representing a child, engaged in real or simulated explicit sexual activity, or any representation of the sexual parts of a child for primarily sexual purposes.<br><br>(2) Any person who unlawfully and intentionally, through a computer or information system—<br>(a) produces child sexual abuse material;<br>(b) offers or makes available child sexual abuse material; |

Back to the Table of Contents

| | |
|---|---|
| 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 or transmits child sexual abuse material;<br>(d) procures or obtains child sexual abuse material for oneself or for another person;<br>(e) possesses child sexual abuse material on a computersystem or a computer-data storage medium;<br>(f) knowingly obtains, accesses or procures child sexual abuse material;<br>(g) baits a child into the production or distribution of child sexual abuse material;<br>shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years, or both such fine and such imprisonment.<br><br>(3) Any person of 18 years or above, who unlawfully and intentionally through information and communication technologies, proposes to meet a child who has not reached the age of consent to sexual activity asset by the Criminal Law (Codification and ReformAct) [Chapter 9:23] for the purpose of engaging in sexual activity with him or her, where this proposal has been followed by material acts leading to such a meeting, shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding ten years, or both such fine and such imprisonment.<br><br>**165B Exposing children to pornography**<br>Any person who unlawfully and intentionally through a computer or information system—<br>(a) makes pornographic material available to any child; or<br>(b) facilitates access by any child to pornography or displays pornographic material to any child;<br>with or without the intention of lowering the child's inhibitions in relation to sexual activity or inducing the child to have sexual relations with that person;<br>shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.<br><br>**PART XI CONSEQUENTIAL AMENDMENTS**<br>**35 Amendment of Chapter VIII of Cap. 9:23**<br>(1) The Criminal Law (Codification and Reform) Act [Chapter 9:23] (hereinafter called the "principal Act") is amended in section 162 by the repeal of the definitions of "computer virus", "data", "essential service" and "owner" and the substitution of the following definitions— |

Back to the Table of Contents

| | |
|---|---|
| | (…)<br>"**child**" means any person under the age of eighteen years;<br><br>"**child pornography**" means any representation through publication, exhibition, cinematography, electronic means or any other means whatsoever, of a child engaged in real or simulated explicit sexual activity, or any representation of the sexual parts of a child for primarily sexual purposes;<br>(…) |
| **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 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. | **Copyright and Neighbouring Rights Act**<br>**PART VII RIGHTS IN PERFORMANCES**<br>**78 Criminal liability for infringement of rights of performers and holders of recording rights**<br>(I) Any person who<br>(a) makes an illicit recording of a performance; or<br>(b) imports an illicit recording of a performance into Zimbabwe or exports it from Zimbabwe, otherwise than for his personal and private use; or<br>(b) in the course of business. possesses an illicit recording of a performance or exhibits it in public or distributes it; or<br>(c) sells an illicit recording of a performance or lets it for hire or offers or exposes it for sale or hire;<br>knowing or having reasonable grounds for believing that it is an illicit recording, shall be guilty of an offence and liable to • fine not exceeding level ten or 10 imprisonment for a period not exceeding two years or to both such fine and such imprisonment.<br><br>(2) Any person who causes an illicit recording to be performed in public, knowing or having reasonable grounds for believing that it is an illicit recording, shall be guilty of an offence and liable to a fine not exceeding level ten or to imprisonment for a period not exceeding Iwo years or to both such line and such imprisonment.<br><br>(3) Any person who causes an illicit recording to be broadcast or transmitted in a cable programme service, knowing or having reasonable grounds for believing that il is an illicit recording, shall be guilty of an offence and liable a fine not exceeding level ten or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment. |

Back to the Table of Contents

| | |
|---|---|
| | (4) Any person who falsely represents that he is authorised to give consent for the purposes of this Part in relation to a performance, not having reasonable grounds for believing that he is so authorised. shall be guilty of an offence end liable to a fine not exceeding level ten or to imprisonment for a period not exceeding six months or to both such fine and such imprisonment. |
| **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. | Criminal Law (Codification and Reform) Act<br>**CHAPTER XII UNFINALISED CRIMES: THREATS, INCITEMENT, CONSPIRACY AND ATTEMPT**<br>**189 Attempt**<br>(1) Subject to subsection (1), any person who<br>(a) intending to commit a crime, whether in terms of this Code or any other enactment; or<br>(b) realising that there is a real risk or possibility that a crime, whether in terms of this Code or any other enactment, may be committed;<br>does or omits to do anything that has reached at least the commencement of the execution of the intended crime, shall be guilty of attempting to commit the crime concerned:<br><br>(2) A person shall not be guilty of attempting to commit a crime if, before the commencement of the execution of the intended crime, he or she changes his or her mind and voluntarily desists from proceeding further with the crime. |
| **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;<br>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 | Criminal Law (Codification and Reform) Act<br>**CHAPTER XVI GENERAL**<br>**277 Criminal liability of corporations and associations and their members, employees and agents**<br>(…)<br>(2) For the purposes of imposing criminal liability upon a corporate body, any conduct on the part of<br>(a) a director or employee of the corporate body; or<br>(b) any person acting on instructions or with permission, express or implied, given by a director or employee of the corporate body;<br>in the exercise of his or her power or in the performance of his or her duties as such a director, employee or authorised person, or in furthering or endeavouring to further the interests of the corporate body, shall be deemed to have been the conduct of the corporate body, and if the conduct was accompanied by any |

Back to the Table of Contents

| | |
|---|---|
| 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. | intention on the part of the director, employee or authorised person, that intention shall be deemed to have been the intention of the corporate body.<br><br>(3) Where there has been any conduct which constitutes a crime for which a corporate body is or was liable to prosecution, that conduct shall be deemed to have been the conduct of every person who at the time was a director or employee of the corporate body, and if the conduct was accompanied by any intention on the part of the person responsible for it, that intention shall be deemed to have been the intention of every other person who at the time was a director or employee of the corporate body: Provided that, if it is proved that a director or employee of the corporate body took no part in the conduct, this subsection shall not apply to him or her.<br><br>(4) For the purposes of imposing criminal liability upon members and employees of an association of persons which is not a corporate body, any conduct on the part of<br>(a) a member or employee of the association; or<br>(b) any person acting on instructions or with permission, express or implied, given by a member or employee of the association; in the exercise of his or her power or in the performance of his or her duties as such a member, employee or authorised person, or in furthering or endeavouring to further the interests of the association, shall be deemed to have been the conduct of every other person who at the time was a member or employee of the association, and if the conduct was accompanied by any intention on the part of the member, employee or authorised person, that intention shall be deemed to have been the intention of every other person who at the time was a member or employee of the association:<br><br>Provided that<br>(i) if it is proved that a member or employee of the association took no part in the conduct, this subsection shall not apply to him or her;<br>(i) if the association is controlled or governed by a committee or other similar governing body, this subsection shall not apply so as to render criminally liable any person who was not at the time of the conduct a member of that committee or other body.<br><br>(5) A person who is criminally liable for any conduct in terms of subsection (3) or (4) shall be liable to be prosecuted and punished personally for the crime concerned. |

Back to the Table of Contents

| | |
|---|---|
| | (6) This section shall not limit any other law which imposes criminal liability upon corporate bodies and associations and their directors, employees and members. |
| **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. | **N/A** |
| ***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 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 | **36 Amendment of Cap. 9:07**<br>The Criminal Procedure and Evidence Act [Chapter 9:07] is amended by the insertion after Part XX of the following Part— |

Back to the Table of Contents

| | |
|---|---|
| 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 powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties. | |
| **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 | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments**<br>**36 Amendment of Cap. 9:07**<br>The Criminal Procedure and Evidence Act [Chapter 9:07] is amended by the insertion after Part XX of the following Part—<br>**"PART XXA Provisions Relating to Cyber Crime"**<br>(…)<br>**379B Expedited preservation**<br>(1) A magistrate may, on an application by a police officer in the prescribed form, that there are reasonable grounds to suspect or believe that traffic data associated |

| | |
|---|---|
| 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. | with a specified communication is required for the purposes of a criminal investigation—<br>(a) order any person in control of such data to—<br>(i) collect, record or preserve the traffic data associated with a specified communication during a specified period; or<br>(ii) permit and assist a specified police officer to collect or record that data.<br>(b) authorise the police officer to collect or record traffic data associated with a specified communication during a specified period through the use of any appropriate technological means.<br><br>(2) Section 33(3) of the Data Protection Act[Chapter 11:22] shall apply mutatis mutandis to an application in terms of this section. |
| **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. | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments**<br>**36 Amendment of Cap. 9:07**<br>The Criminal Procedure and Evidence Act [Chapter 9:07] is amended by the insertion after Part XX of the following Part—<br>**"PART XXA Provisions Relating to Cyber Crime"**<br>(…)<br><br>**379B Expedited preservation**<br>(1) A magistrate may, on an application by a police officer in the prescribed form, that there are reasonable grounds to suspect or believe that traffic data associated with a specified communication is required for the purposes of a criminal investigation—<br>(a) order any person in control of such data to—<br>(i) collect, record or preserve the traffic data associated with a specified communication during a specified period; or<br>(ii) permit and assist a specified police officer to collect or record that data.<br>(b) authorise the police officer to collect or record traffic data associated with a specified communication during a specified period through the use of any appropriate technological means.<br><br>(2) Section 33(3) of the Data Protection Act[Chapter 11:22] shall apply mutatis mutandis to an application in terms of this section. |
| **Article 18 – Production order** | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments** |

Back to the Table of Contents

| | |
|---|---|
| 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:<br>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. | **36 Amendment of Cap. 9:07**<br>The Criminal Procedure and Evidence Act [Chapter 9:07] is amended by the insertion after Part XX of the following Part—<br>**"PART XXA Provisions Relating to Cyber Crime"**<br>**379A Search and seizure**<br>(…)<br>(2) A magistrate may, on an application by a police officer in the prescribed form, that specified computer data or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, order that—<br>(a) a person in Zimbabwe in control of the relevant computer system produce from the system specified computer data or a printout or other intelligible output of that data; or<br>(b) an electronic communications service provider in Zimbabwe produce information about persons who subscribe to or otherwise use the service.<br>(…) |
| **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 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. | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments**<br>**36 Amendment of Cap. 9:07**<br>The Criminal Procedure and Evidence Act [Chapter 9:07] is amended by the insertion after Part XX of the following Part—<br>**"PART XXA Provisions Relating to Cyber Crime"**<br>**379A Search and seizure**<br>(1) In this section **"seize"** includes—<br>(a) taking possession of or securing a computer;<br>(b) securing a computer system or part there of or a computer-data storage medium;<br>(c) taking a printout or output of computer data;<br>(d) making and retaining a copy of computer data, including through the use of use of onsite equipment;<br>(e) activating any onsite computer system or computer data storage media; |

Back to the Table of Contents

| | |
|---|---|
| 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.<br>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. | (f) maintaining the integrity of any stored relevant computer data;<br>(g) rendering inaccessible or removing computer data in the accessed computer system.<br><br>(2) A magistrate may, on an application by a police officer in the prescribed form, that specified computer data or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, order that—<br>(a) a person in Zimbabwe in control of the relevant computer system produce from the system specified computer data or a printout or other intelligible output of that data; or<br>(b) an electronic communications service provider in Zimbabwe produce information about persons who subscribe to or otherwise use the service.<br><br>(3) An application referred to in subsection (1)shall be supported by an affidavit in which the police officer shall set out the offence being investigated, the computer system in which it is suspected to be stored, the reasonable grounds upon which the belief is based, the measures that will be taken in pursuance of the investigation and the period over which those measures will be taken.<br><br>(4) A police officer granted a warrant in terms of this section may—<br>(a) if there are reasonable grounds to believe that computer data concerned is susceptible to loss, alteration, deletion, impairment or modification, by written notice given to a person in control of the computer data, require the person in control of the data to ensure that the data specified in the notice is preserved for a period not exceeding seven days as may be specified in the notice which period may be extended, on an application to a magistrate, for such period as the magistrate may grant;<br>(b) by written notice to a person in control of the computer system or information system concerned, require the person in control there of to disclose relevant traffic data concerning specified communications in order to identify—<br>(i) the service providers; or<br>(ii) the path through which the communication was transmitted.<br><br>(5) Any person who does not comply with the order given in terms of this section shall be guilty of an offence and liable to a fine. |

Back to the Table of Contents

| | |
|---|---|
| **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 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. | **Cyber & Data Protection Act**<br>**PART XI Consequential Amendments**<br>**36 Amendment of Cap. 9:07**<br>The Criminal Procedure and Evidence Act [Chapter 9:07] is amended by the insertion after Part XX of the following Part—<br>**"PART XXA Provisions Relating to Cyber Crime"**<br>**379A Search and seizure**<br>(1) In this section **"seize"** includes—<br>(a) taking possession of or securing a computer;<br>(b) securing a computer system or part there of or a computer-data storage medium;<br>(c) taking a printout or output of computer data;<br>(d) making and retaining a copy of computer data, including through the use of use of onsite equipment;<br>(e) activating any onsite computer system or computer data storage media;<br>(f) maintaining the integrity of any stored relevant computer data;<br>(g) rendering inaccessible or removing computer data in the accessed computer system.<br><br>(2) A magistrate may, on an application by a police officer in the prescribed form, that specified computer data or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, order that—<br>(a) a person in Zimbabwe in control of the relevant computer system produce from the system specified computer data or a printout or other intelligible output of that data; or<br>(b) an electronic communications service provider in Zimbabwe produce information about persons who subscribe to or otherwise use the service.<br><br>(3)An application referred to in subsection (1)shall be supported by an affidavit in which the police officer shall set out the offence being investigated, the computer system in which it is suspected to be stored, the reasonable grounds upon which the belief is based, the measures that will be taken in pursuance of the investigation and the period over which those measures will be taken.<br><br>(4) A police officer granted a warrant in terms of this section may—<br>(a) if there are reasonable grounds to believe that computer data concerned is susceptible to loss, alteration, deletion, impairment or modification, by written notice given to a person in control of the computer data, require the |

Back to the Table of Contents

| | |
|---|---|
| | person in control of the data to ensure that the data specified in the notice is preserved for a period not exceeding seven days as may be specified in the notice which period may be extended, on an application to a magistrate, for such period as the magistrate may grant;<br>(b) by written notice to a person in control of the computer system or information system concerned, require the person in control there of to disclose relevant traffic data concerning specified communications in order to identify—<br>(i) the service providers; or<br>(ii) the path through which the communication was transmitted.<br><br>(5) Any person who does not comply with the order given in terms of this section shall be guilty of an offence and liable to a fine.<br><br>**379C Obligations and immunity of service providers**<br>(…)<br>(5) Where the hosting provider removes the content after receiving an order pursuant to sub-section (3), no liability shall arise from the contractual obligations with the user with regard to the availability of the service.<br><br>(6) A hosting provider who fails to remove or disable access to information in terms of subsection (3) shall be guilty of an offence and liable to a fine not exceeding level 8 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.<br><br>(7) A caching provider shall not be criminally liable for the automatic, intermediate, or temporary storage of information where the caching was performed for the sole purpose of making the onward transmission of the information to other users of the service upon their request more efficient if the caching provider—<br>(a) does not modify the information;<br>(b) complies with conditions of access to the information;<br>(c) complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;<br>(d) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and<br>(e) acts promptly to remove or to disable access to the information it has stored upon obtaining knowledge that the information has been removed from the network at the initial source of the transmission, or that access to |

Back to the Table of Contents

| | |
|---|---|
| | it has been disabled, or that a court or an appropriate public authority has ordered such removal or disablement.<br><br>(8) A caching provider who contravenes the conditions set out in subsection (7) shall be guilty of an offence and liable to a fine not exceeding level 8 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.<br><br>(9) An internet service provider who enables access to information provided by a third person by providing an electronic hyperlink shall not be criminally liable with respect to the information if the internet service provider—<br>(a) promptly removes or disables access to the information after receiving an order from an appropriate public authority or court to remove the link; or<br>(b) through other means, obtains knowledge or becomes aware of stored specific illegal information promptly informs the appropriate authority to enable it to evaluate the nature of the information and if necessary issue an order for its removal.<br><br>(10) An internet service provider who fails to promptly remove or disable access to information in terms of subsection (9) shall be guilty of an offence and liable to a fine not exceeding level 8 or to imprisonment for a period not exceeding two years or both such fine and such imprisonment.<br><br>(11) Any service provider who knowingly enables access to stores, transmits or provides an electronic hyperlink to, any information with knowledge of the unlawfulness of the content of any such information shall be guilty of an offence and liable to a fine not exceeding level 14 or to imprisonment not exceeding a period of ten years or to both such fine and such imprisonment. |
| **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 | |

| | |
|---|---|
| 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. | |
| ***Section 3 – Jurisdiction*** | |
| **Article 22 – Jurisdiction**<br>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. | Cyber & Data Protection Act<br>**PART XI Consequential Amendments**<br>**36 Amendment of Cap. 9:07**<br>The Criminal Procedure and Evidence Act [Chapter 9:07] is amended by the insertion after Part XX of the following Part—<br>**"PART XXA Provisions Relating to Cyber Crime"**<br>**379D Jurisdiction**<br>1)A court in Zimbabwe shall have jurisdiction to try any offence under this Act where the offence was committed wholly or in part—<br>(a) within Zimbabwe or by any person in or outside Zimbabwe using a computer or information system or device, software or data located in Zimbabwe; or<br>(b) on a ship or aircraft registered in Zimbabwe; or<br>(c) by a national or permanent resident of Zimbabwe or a person carrying on business in Zimbabwe, whether or not the offence is committed in Zimbabwe; or<br>(d) by a national or permanent resident of Zimbabwe or a person carrying on business in Zimbabwe and the offence is committed outside Zimbabwe, if the person's conduct also constitutes an offence under the law of the |

Back to the Table of Contents

| | |
|---|---|
| 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. | country where the offence was committed and harmful effects were caused in Zimbabwe; or<br>(e) by any person, regardless of the location, nationality or citizenship of the person—<br>(i) using a computer or information system or device, software, or data located within Zimbabwe; or directed against a computer or information system or<br>(ii) device, software or data located in Zimbabwe. |
| **Chapter III – International co-operation** | |
| **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.<br>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. | **Extradition Act** |

Back to the Table of Contents

| | |
|---|---|
| 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**<br>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 | **Criminal Matters (Mutual Assistance) Act**<br>**PART I PELIMINARY**<br>**3 Application of Act**<br>(1) Subject to subsections (2) and (3), whenever the Minister is satisfied that reciprocal provisions have been made by any foreign country to facilitate the provision to Zimbabwe of assistance in criminal matters, he may, by statutory instrument, declare that this Act shall apply in relation to any such foreign country.<br><br>(2) The Minister may, by statutory instrument, direct that the application of this Act in relation to a specified foreign country shall be subject to such conditions or modifications as may be specified in the statutory instrument, and thereupon this Act shall apply accordingly.<br><br>(3) This section shall not apply to Part II.<br><br>(4) The requirement of dual criminality upon which the principle of mutual assistance in criminal matters is based shall be deemed to be fulfilled in respect of any offence for which assistance is sought if the conduct underlying the offence is a criminal offence under the laws of Zimbabwe and the foreign country concerned, irrespective of whether the laws of the requesting foreign country |

| | |
|---|---|
| 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. | place the offence within the same class of offences as Zimbabwe or denominate the offence by the same terminology as in Zimbabwe.<br>**4 Aspects of mutual assistance**<br>For the purposes of this Act, mutual assistance in criminal matters shall include—<br>(a) the obtaining of evidence, documents or other articles;<br>(b) the provision of documents and other records;<br>(c) the location and identification of witnesses or suspects;<br>(d) the execution of requests for search and seizure;<br>(e) the making of arrangements for persons to give evidence or assist in investigations;<br>(f) the forfeiture or confiscation of property in respect of offences;<br>(g) the recovery of pecuniary penalties in respect of offences;<br>(h) the interdicting of dealings in property, or the freezing of assets, that may be forfeited or confiscated, or that may be needed to satisfy pecuniary penalties imposed, in respect of offences;<br>(i) the location of property that may be forfeited, or that may be needed to satisfy pecuniary penalties imposed, in respect of offences; and<br>(j) the service of documents.<br>(k) Identifying or tracing the proceeds of crime, funds or property or instrumentalities or other things for evidentiary or confiscation purposes;<br>(l) the examination of objects and sites;<br>(m) any other form of mutual legal assistance not contrary to the law of Zimbabwe.<br><br>**6 Refusal of assistance**<br>(1) A request by a foreign country for assistance under this Act shall be refused if, in the opinion of the Prosecutor-General—<br>(a) the request relates to the prosecution or punishment of a person for an offence that is, by reason of the circumstances in which it is alleged to have been committed or was committed, an offence of a political character; or<br>(b) there are reasonable grounds for believing that the request has been made with a view to prosecuting or punishing a person for an offence of a political character; or<br>(c) there are reasonable grounds for believing that the request was made for the purpose of prosecuting, punishing or otherwise causing prejudice to a person on account of the person's race, sex, religion, nationality or political opinions; or<br>(d) the request relates to prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Zimbabwe, would have constituted an offence under the military law of Zimbabwe but not under the ordinary criminal law of Zimbabwe; or<br>(e) the granting of the request would prejudice public safety, public order, defence or the economic interests of Zimbabwe; or |

Back to the Table of Contents

(f) the request relates to the prosecution of a person for an offence in a case where the person has been acquitted or pardoned by a competent court or authority in the foreign country, or has undergone the punishment provided by the law of that country, in respect of that offence or of another offence constituted by the same act or omission as that offence; or
(g) except in the case of a request under section eleven, the foreign country is not a country to which this Act applies.

(2) A request by a foreign country for assistance under this Act may be refused if in the opinion of the Prosecutor-General—
(a) the request relates to the prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Zimbabwe, would not have constituted an offence against the law of Zimbabwe; or
(b) the request relates to the prosecution or punishment of a person in respect of an act or omission that occurred, or is alleged to have occurred, outside the foreign country and a similar act or omission occurring outside Zimbabwe in similar circumstances would not have constituted an offence against the law of Zimbabwe; or
(c) the request relates to the prosecution or punishment in respect of an act or omission where, if it had occurred in Zimbabwe at the same time and had constituted an offence against the law of Zimbabwe, the person responsible could no longer be prosecuted by reason of lapse of time or any other reason; or
(d) the provision of the assistance could prejudice an investigation or proceedings in relation to a criminal matter in Zimbabwe; or
(e) the provision of the assistance would, or would be likely to, prejudice the safety of any person, whether in or outside Zimbabwe; or
(f) the provision of the assistance would impose an excessive burden on the resources of Zimbabwe.

**7 Assistance may be conditional**
Assistance in terms of this Act may be provided to a foreign country subject to such conditions as the Prosecutor-General may determine.

**8 Request by Zimbabwe**
Any request by Zimbabwe for assistance in any criminal matter in terms of this Act shall be made by the Prosecutor-General.

**9 Request for assistance by foreign country**
(1) A request by the appropriate authority of a foreign country for assistance in a criminal matter shall be made to the Prosecutor-General.

Back to the Table of Contents

| | |
|---|---|
| | (2) A request made in terms of subsection (1) shall contain or be accompanied by a document giving the following information—<br>(a) the name of the authority concerned with the criminal matter to which the request relates; and<br>(b) a description of the nature of the criminal matter and a summary of the relevant facts and laws; and<br>(c) a description of the purpose of the request and of the nature of the assistance being sought; and<br>(d) details of the procedure that the foreign country wishes to be followed by Zimbabwe in giving effect to the request, including details of the manner and form in which any information, document or thing is to be supplied to the foreign country pursuant to the request; and<br>(e) the wishes of the foreign country concerning the confidentiality of the request and the reasons for those wishes; and<br>(f) details of the period within which the foreign country wishes that the request be complied with; and<br>(g) if the request involves a person travelling from Zimbabwe to the foreign country, details of allowances to which the person will be entitled and of the arrangements for accommodation for the person, while the person is in the foreign country pursuant to the request; and<br>(h) any other information required to be included with the request under a treaty or other arrangement between Zimbabwe and the foreign country; and<br>(i) any other information that may assist in giving effect to the request;<br>but failure to comply with this subsection shall not be a ground for refusing the request. |
| **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. | N/A |

Back to the Table of Contents

| | |
|---|---|
| **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. 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 | N/A |

Back to the Table of Contents

| | |
|---|---|
| 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.<br>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: | |

Back to the Table of Contents

| | |
|---|---|
| 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. | |
| **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 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 | N/A |

| | |
|---|---|
| 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. | N/A |
| **Article 31 – Mutual assistance regarding accessing of stored computer data** | N/A |

Back to the Table of Contents

| | |
|---|---|
| 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. | N/A |
| **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. | N/A |
| **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. | N/A |

Back to the Table of Contents

| | |
|---|---|
| **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. | N/A |
| **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, 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