Ethiopia

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 3 June 2020

[reference to the provisions of the Budapest Convention]

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

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

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: 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; 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; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; 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	Computer Crime Proclamation No. 958/2016 (7 July 2016) (henceforth CCP 958/2016) **Part I - GENERAL**: **2. Definitions** In this Proclamation unless the context otherwise requires: 1/ "Computer crime" means a) A crime committed against a computer, computer system, computer data or computer network; b) A conventional crime committed by means of a computer, computer system, computer data or computer network; or c) Illegal computer content data disseminated through a computer, computer system, or computer network; 2/ "data processing service" means the service of reception, storage, processing, emission, routing or transmission of data by means of computer system and includes networking services; 3/ "computer or computer system" means any software and the microchips technology based data processing, storage, analysis, dissemination and communication device or any device that is capable of performing logical, arithmetic or routing function and includes accessories of that device; 4/ "computer data" means any content data, traffic data, computer program, or any other subscriber information in a form suitable for processing by means of a computer system; 5/ "computer program" means a set of instructions or commands expressed in words, codes or schemes which are capable of causing a computer system to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	perform or achieve a particular task or result; 6/ "traffic data" means any computer generated data relating to a chain of communication by means of a computer system indicating the communication's origin, destination, route, time, date, duration, size or types of underlying service; 7/ "content data" means any computer data found in the form of audio, video, picture, arithmetic formula or any other form that conveys the essence, substance, meaning or purpose of a stored or transmitted computer data or computer communication; 8/ "network" means the interconnection of two or more computer systems by which data processing service can be provided or received; 9/ "computer data security" means the protection of a computer data from deleting, changing, and accessing by unauthorized person, compromising its confidentiality or any other damage; 10/ "access" means to communicate with, to enter in, store in, store data in, retrieve, or obtain data from, to view, to receive, move or copy data from a computer system, or otherwise make use of any data processing service thereof; 11/ "critical infrastructure" means a computer system, network or data where any of the crimes stipulated under article 3 to 6 of this proclamation, is committed against it, would have a considerable damage on public safety and the national interest; 12/ "interception" means real-time surveillance, recording, listening, acquisition, viewing, controlling or any other similar act of data processing service or computer data; 13/ "service provider" means a person who provides technical data processing or communication service or alternative infrastructure to users by means of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	computer system; 14/ "Attorney General" means head of the Federal Attorney General appointed by the House of Peoples Representatives; 15 "Public prosecutor" means lawyer appointed by the Attorney General and administered by public prosecutors administration regulation and included the Attorney General and the deputy attorney generals; 16/ "investigatory organ" mean a person legally invested with the power of investigation; 17/ "regional state" means any state referred to in Article 47(1) of the Constitution of the Federal Democratic Republic of Ethiopia and for the purpose this Proclamation it includes Addis Ababa and Dire Dawa city administrations; 18/ "police" mean Federal Police or Regional State Police to whom the power of the Federal Police is delegated; 19/ "Agency" mean Information Network Security Agency; 20/ "person" means a physical or juridical person; 21/ any expression in the masculine gender includes the feminine.
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 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	**CCP 958/2016 Part II - COMPUTER CRIMES** **Section I: CRIMES AGAINST COMPUTER SYSTEM AND COMPUTER DATA** **3. Illegal Access** 1/ Whosoever, without authorization or in excess of authorization, intentionally secures access to the whole or any part of computer system, computer data or network shall be punishable with simple imprisonment not exceeding three

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
other dishonest intent, or in relation to a computer system that is connected to another computer system.	years or fine from Birr 30,000 to 50,000 or both. 2/ Where the crime stipulated under sub-article (1) of this Article is committed against: a) a computer system, computer data or network that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from three years to five years and fine from Birr 30,000 to 50,000; b) a critical infrastructure, the punishment shall be rigorous imprisonment from five years to ten years and fine from Birr 50,000 to 100,000.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**CCP 958/2016: 4. Illegal Interception** 1/ Whosoever, without authorization or in excess of authorization, intentionally intercepts non-public computer data or data processing service shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000. 2/ Where the crime stipulated under sub-article (1) of this Article is committed against: a) a computer data or data processing service that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from five years to ten years and fine from Birr 50,000 to 100,000. b) a critical infrastructure, the punishment shall be rigorous imprisonment from ten years to fifteen years and fine from Birr 100,000 to 200,000.
Article 4 – Data interference 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. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**CCP 958/2016: 6. Causing Damage to Computer Data** 1/ Whosoever, without authorization or in excess of authorization, intentionally alters, deletes, suppresses a computer data, renders it meaningless, useless or inaccessible to authorized users shall be punishable with rigorous imprisonment not exceeding three years and fine not exceeding Birr 30,000. 2/ Where the crime stipulated under sub-article (1) of this Article is committed against: a) a computer data that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from three years to five years and fine from Birr 30,000 to 50,000; b) a critical infrastructure, the punishment shall be rigorous imprisonment from five to ten years and fine from Birr 50,000 to 100,000.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 5 – System interference 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	**CCP 958/2016: 5. Interference with Computer System** 1/ Whosoever, without authorization or in excess of authorization, intentionally hinders, impairs, interrupts or disrupts the proper functioning of the whole or any part of computer system by inputting, transmitting, deleting or altering computer data shall be punishable with rigorous imprisonment from three years to five years and fine not exceeding Birr 50,000. 2/ where the crime stipulated under sub-article (1) of this Article is committed against: a) a computer system that is exclusively destined for the use of a legal person, the punishment shall be rigorous imprisonment from five to ten years and fine from Birr 50,000 to 100,000; b) a critical infrastructure, the punishment shall be rigorous imprisonment from 10 years to 15 years and fine from Birr 100,000 to 200,000 or, in serious case, rigorous imprisonment from fifteen years to twenty years and fine from Birr 200,000 to 500,000.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: 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; 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, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and 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. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise	**CCP 958/2016: 7. Criminal Acts Related to Usage of Computer Devices and Data** 1/ Whosoever, knowing that it can cause damage to computer system, computer data or network, intentionally transmits any computer program exclusively designed or adapted for this purpose shall be punishable with simple imprisonment not exceeding five years or fine not exceeding Birr 30,000. 2/ Whosoever, knowing that it is to be used for the commission of unlawful act specified under Articles 3 to 6 of this Proclamation, intentionally imports, produces, offers for sale, distributes or makes available any computer device or computer program designed or adapted exclusively for the purpose of committing such crimes shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000. 3/ Whosoever possesses any computer devices or data specified under sub-article (1) or (2) of this Article with the intention to further the commission of any of the crimes specified under Articles 3 to 6 of this Proclamation shall be punishable with simple imprisonment not exceeding three years or fine from Birr 5,000 to 30, 000. 4/ Whosoever, without authorization or excess of authorization, intentionally discloses or transfers any computer program, secret code, key, password or any other similar data for gaining access to a computer system, computer data or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	network shall be punishable with simple imprisonment not exceeding five years or in serious cases with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000. 5/ Where the crime stipulated under sub-article (4) of this Article is committed negligently, the punishment shall be simple imprisonment not exceeding one year and fine not exceeding Birr 10,000.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery 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.	**CCP 958/2016: Part II - Section II COMPUTER RELATED FORGERY, FRAUD AND THEFT** **9. Computer Related Forgery** Whosoever falsifies a computer data, makes false computer data or makes use of such data to injure the rights or interests of another or to procure for himself or for another person any undue right or advantage shall be punishable with simple imprisonment not exceeding three years and fine not exceeding Birr 30,000 or in serious cases with rigorous imprisonment not exceeding ten years and fine from Birr 10,000 to 100,000.
Article 8 – Computer-related fraud 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: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**CCP 958/2016: Part II - Section II 10. Computer Related Fraud** 1/ Whosoever fraudulently causes a person to act in a manner prejudicial to his rights or those of third person by distributing misleading computer data, misrepresenting his status, concealing facts which he had a duty to reveal or taking advantage of the person's erroneous beliefs, shall be punishable with rigorous imprisonment not exceeding five years and fine not exceeding Birr 50,000. 2/ Whosoever, with fraudulent intent of procuring any benefit for himself or for another person, causes economic loss to another person by any change, deletion or any other damage of computer data shall be punishable with rigorous imprisonment not exceeding five years and fine from Birr 10,000 to 50,000 or in serious cases with rigorous imprisonment not exceeding ten years and fine from Birr 10,000 to 100,000.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	11. Electronic Identity Theft Whosoever, with intent to commit criminal act specified under Article 10 of this Proclamation or for any other purpose produces, obtains, sales, possesses or transfers any data identifying electronic identity of another person without authorization of that person shall be punishable with simple imprisonment not exceeding five years or fine not exceeding Birr 50,000.
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 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. 4 Each Party may reserve the right not to apply, in whole or in part,	**CCP 958/2016: Part II – Section III: ILLEGAL CONTENT DATA:** **12. Obscene or Indecent Crimes Committed Against Minors** 1/ Whosoever intentionally produces, transmits, sales, distributes, makes available or possesses without authorization any picture, poster, video or image through a computer system that depicts: a) a minor engaged in sexually explicit conduct; or b) a person appearing to be a minor engaged in sexually explicit conduct; shall be punishable with rigorous imprisonment from three years to ten years. 2/ Whosoever entices or solicits a minor for sexual explicit conduct by transmitting or sending erotic speeches, pictures, text messages or videos through computer system shall be punishable with rigorous imprisonment from five years to ten years.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law 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. 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. 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 Neighboring Rights Protection Proclamation No. 410/2004** (19 July 2004) **Copyright and Neighboring Rights Protection (Amendment) Proclamation No. 872/2014** (14 January 2015) (amends Proclamation 410/2004)
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 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	**CCP 958/2016: Part III PREVENTIVE AND INVESTIGATIVE MEASURES: 22. General** 2/ Without prejudice the provisions of this Part, for issues not clearly covered in this law, the provisions of the Criminal Code and other relevant laws shall be

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, 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. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	applicable to computer crimes. **Criminal Code Proclamation No 414/2004: Article 445**: Harbouring and Aiding. Whoever knowingly saves from prosecution a person who has fallen under a provision of criminal law, whether by warning him or hiding him, by concealing or destroying the traces or instruments of his crime, by misleading the investigation, or in any other way, is punishable with simple imprisonment or fine.
Article 12 – Corporate liability 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: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**CCP 958/2016: Part II Section IV OTHER OFFENCES:** **20. Penalty Imposed on Juridical Person** Notwithstanding Article 90 (1), (3) and (4) of the Criminal Code of the Federal Democratic Republic of Ethiopia, where any offence stipulated under this Part is committed by juridical person, 1/ the penalty shall be fine from Birr 50,000 to 500,000 for a crime punishable with fine; 2/ when the penalty provided for is imprisonment, the penalty shall be: a) a fine not exceeding 50,000 Birr for a crime punishable with simple imprisonment not exceeding three years, b) a fine not exceeding 100,000 Birr for a crime punishable with simple imprisonment not exceeding five years, c) a fine not exceeding 150,000 Birr for a crime punishable with rigorous imprisonment not exceeding five years, d) a fine not exceeding 200,000 Birr for a crime punishable with rigorous imprisonment not exceeding ten years, e) a fine of up to the general maximum laid down in sub-article (1) of this Article for a crime punishable with rigorous imprisonment exceeding ten years. 3/ Where fine is expressly provided as punishment for a crime, it shall be five fold.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance	**CCP 958/2016: Part II Section I: 8. Aggravated Cases** Where the crime stipulated under Article 3 to 6 of this Proclamation is committed: a) against a computer data or a computer system or network which is designated as top secrete by the concerned body for military interest or international relation, or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	b) while the country is at a state of emergency or threat, the punishment shall be rigorous imprisonment from fifteen years to twenty five years. **CCP 958/2016: Part II Section IV OTHER OFFENCES:** **18. Criminal Act Stipulated in Other Laws** Where any crime other than those provided for under this Part is committed by means of a computer, the relevant law shall apply. **19. Concurrent Crimes** Where any of the criminal acts provided for under this Part has resulted in the commission of another crime punishable under any special law or criminal code, the relevant provision shall apply concurrently.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 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. 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	**CCP 958/2016: Part III PREVENTIVE AND INVESTIGATIVE MEASURES** **22. General** 1/ Computer crime prevention and investigation shall be conducted in accordance with the provisions of this Part. 2/ Without prejudice the provisions of this Part, for issues not clearly covered in this law, the provisions of the Criminal Code and other relevant laws shall be applicable to computer crimes. **23. Investigative Power** 1/ The public prosecutor and police shall have joint power to investigate criminal acts provided for in this Proclamation. And the public prosecutor shall lead the investigation process. 2/ Where requested to support the investigation process, the Agency shall provide technical support, conduct analysis on collected information, and provide evidences if necessary. **27. Duty to Report** 1/ Any service provider or government organ who has knowledge of the commission of the crimes stipulated in this Proclamation or dissemination of any illegal content data by third parties through the computer system it administers shall immediately notify the Agency, accordingly report to the police about the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, 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	crime and take appropriate measures. **28. Arrest and Detention** Without prejudice the provisions stipulated in special laws, 1/ where there are reasonable grounds to believe that a computer crime is committed or under commission, police may arrest suspects in accordance with the provisions of the Criminal Procedure Code. 2/ Where the investigation on the person arrested pursuant to sub-article (1) of this Article is not completed, remand may be granted in accordance with the provisions of the Criminal Procedure Code; provided, however, the overall remand period may not exceed four months. **Part IV: EVIDENTIARY AND PROCEDURAL PROVISIONS** **33. Admissibility of Evidences** 1/ Any document or a certified copy of the document or a certified printout of any electronic record relating to computer data seized in accordance with this Proclamation may be produced as evidence during court proceedings and shall be admissible. 2/ Without prejudice to the admissibility of evidences to be produced in accordance with the Criminal Procedure Code and other relevant laws, any digital or electronic evidence: a) produced in accordance with this Proclamation; or b) obtained by appropriate foreign law enforcement bodies in accordance with Ethiopian Law shall be admissible in court of law in relation to computer crimes. 38. Public Prosecutor and Police Following up Cases of Computer Crime 1/ A Public prosecutor or investigative officer empowered to follows up computer crime cases in accordance with the powers conferred by law shall have the responsibility to enforce and cause to enforce the provisions of this Proclamation. 2/ The Attorney General and Police empowered in this Proclamation may organize separate specialized task units when necessary to follow up computer crimes. **Part V: INSTITUTIONS THAT FOLLOW UP CASES OF COMPUTER CRIME** **39. Duty of the Agency** The Agency shall have duty to establish online computer crimes investigation system and provide other necessary investigation technologies.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	40. Jurisdiction 1/ The Federal High Court shall have first instance jurisdiction over computer crime stipulated under this Proclamation. 2/ The judicial jurisdictions stipulated under Article 13 and Article 17 (1) (b) of the Federal Democratic Republic of Ethiopia Criminal Code shall include computer crimes. **41. Establishment of Executing Task Force** 1/ Without prejudice the power of the Agency to lead national cyber security operation as stipulated in other relevant laws, laws, a National Executing Task Force comprising the Federal Attorney General the Federal Police Commission, and other relevant bodies shall be established in order to prevent and control computer crimes. 2/ The Federal Attorney General shall lead the Executing Task Force, identify other relevant organizations to be incorporated in the Task Force and ensure their representation. 3/ The Task Force shall, for the prevention and control computer crimes, develop national discussion forum, discuss on occasional dangers materialized and provide recommendation thereof, design short and long term plans to be performed by the respective institutions as well as put in place synchronized system by coordinating various relevant organs.
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to 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. 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.	**CCP 958/2016: Part III PREVENTIVE AND INVESTIGATIVE MEASURES** **21. Principle** The prevention, investigation and evidence procedures provided in this Part and Part Four of this Proclamation shall be implemented and applied in a manner that ensure protection for human and democratic rights guaranteed under the Constitution of the Federal Democratic Republic of Ethiopia and all international agreements ratified by the country. **Constitution of the Federal Democratic Republic of Ethiopia (1995)** **Article 26: Right to Privacy** **Article 27: Freedom of Religion, Belief and Opinion** **Article 29: Right of Thought, Opinion and Expression** **Article 30: The Right of Assembly, Demonstration and Petition** **Article 31: Freedom of Association** **Article 32: Freedom of Movement**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Freedom of the Mass Media and Access to Information Proclamation No. 590/2008**
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or 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. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**CCP 958/2016: Part IV: EVIDENTIARY AND PROCEDURAL PROVISIONS** **30. Order for Preservation of Computer Data** 1/ Where there are reasonable grounds to believe that a computer data required for computer crime investigation is vulnerable to loss or modification, the investigatory organ may order, in writing, a person to preserve the specified data under his control or possession. 2/ The person ordered under sub-article (1) of this Article shall immediately take necessary measures to secure the specified computer data and preserve it for three months and keep such order confidential. 3/ The investigatory organ may order only a one-time extension for another three months up on the expiry of the period stipulated under sub-article (2) of this Article. **31. Order for Obtaining of Computer Data** 1/ Where a computer data under any person's possession or control is reasonably required for purposes of a computer crime investigation, the investigatory organ may apply to the court to obtain or gain access to that computer data. 2/ If the court is satisfied, it may, without requiring the appearance of the person concerned, order the person who is in possession or control of the specified computer data, to produce it to the investigatory organ or give access to same.
Article 17 – Expedited preservation and partial disclosure of traffic data 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: a ensure that such expeditious preservation of traffic data is available	**CCP 958/2016: Part IV: EVIDENTIARY AND PROCEDURAL PROVISIONS** **30. Order for Preservation of Computer Data** 1/ Where there are reasonable grounds to believe that a computer data required for computer crime investigation is vulnerable to loss or modification, the investigatory organ may order, in writing, a person to preserve the specified data under his control or possession.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
regardless of whether one or more service providers were involved in the transmission of that communication; and 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	2/ The person ordered under sub-article (1) of this Article shall immediately take necessary measures to secure the specified computer data and preserve it for three months and keep such order confidential. 3/ The investigatory organ may order only a one-time extension for another three months up on the expiry of the period stipulated under sub-article (2) of this Article. **31. Order for Obtaining of Computer Data** 1/ Where a computer data under any person's possession or control is reasonably required for purposes of a computer crime investigation, the investigatory organ may apply to the court to obtain or gain access to that computer data. 2/ If the court is satisfied, it may, without requiring the appearance of the person concerned, order the person who is in possession or control of the specified computer data, to produce it to the investigatory organ or give access to same.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: 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 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. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 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: a the type of communication service used, the technical provisions taken thereto and the period of service; 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;	**CCP 958/2016: Part IV: EVIDENTIARY AND PROCEDURAL PROVISIONS:** **31. Order for Obtaining of Computer Data** 1/ Where a computer data under any person's possession or control is reasonably required for purposes of a computer crime investigation, the investigatory organ may apply to the court to obtain or gain access to that computer data. 2/ If the court is satisfied, it may, without requiring the appearance of the person concerned, order the person who is in possession or control of the specified computer data, to produce it to the investigatory organ or give access to same.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part 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. 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: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 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. 5 The powers and procedures referred to in this article shall be subject to	**CCP 958/2016: Part III PREVENTIVE AND INVESTIGATIVE MEASURES**: **26. Protection of Computer, Computer System or Infrastructure from Danger** 1/ Where there are reasonable grounds to believe that a computer crime is to be committed and it is necessary to prevent and control the crime, provide early warning to citizens, to minimize the risks or for effectiveness of the investigation, the Agency, in collaboration with the investigatory organ, and upon court warrant, may conduct sudden searches, conduct digital forensic investigation, provide appropriate security equipment or take other similar measures on computers, computer systems or infrastructures that are suspected to be attacked or deemed to be the sources of attack. 2/ For the implementation of the provision of sub-article (1) of this Article, as may be necessary and upon request, concerned organs shall have duty to cooperate. **Part IV: EVIDENTIARY AND PROCEDURAL PROVISIONS:** **32. Access, Search and Seizure** 1/ Where it is necessary for computer crime investigation, the investigatory organ may, upon getting court warrant, search or access physically or virtually any computer system, network or computer data. 2/ Where the investigatory organ reasonably believes that the computer data sought is stored in another computer system and can be obtained by same computer system, the search or access may be extended to that other computer system without requesting separate search warrant. 3/ In the execution of search under sub-article (1) or (2) of this Article, the investigatory organ may: a) seize any computer system or computer data; b) make and retain a copy or photograph data obtained through search;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Articles 14 and 15.	c) maintain the integrity of the relevant stored data by using any technology; d) render inaccessible the stored data from the computer system on which search is conducted; or e) recover deleted data. 4/ In the execution of search, the investigatory organ may order any person who has knowledge in the course of his duty about the functioning of the computer system or network or measures applied to protect the data therein to provide the necessary information or computer data that can facilitate the search or access. 5/ Where the investigatory organ finds the functioning of a computer system or computer data is in violation of the provisions this Proclamation or other relevant laws, it may request the court to order for such computer data or computer system to be rendered inaccessible or restricted or blocked. The court shall give the appropriate order within 48 hours after the request is presented. 6/ Where the search process on juridical person requires the presence of the manager or his agent, the investigatory organ shall take appropriate measure to do so.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: 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, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal	**CCP 958/2016: Part III PREVENTIVE AND INVESTIGATIVE MEASURES**: **25. Real-time Collection of Computer Data** Without prejudice special provisions stipulated under other laws, 1/ to prevent computer crimes and collect evidence related information, the investigatory organ may, request court warrant to intercept in real-time or conduct surveillance, on computer data, data processing service, or internet and other related communications of suspects, and the court shall decide and determine a relevant organ that could execute interception or surveillance as necessary. 2/ Sub-article (1) of this Article shall only be applicable when there is no other means readily available for collecting such data and this is approved and decided by the Attorney General. 3/ Notwithstanding the provisions of sub-article (1) and (2) of this Article, the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Attorney General may give permission to the investigatory organ to conduct interception or surveillance without court warrant where there are reasonable grounds and urgent cases to believe that a computer crime that can damage critical infrastructure is or to be committed. 4/ The Attorney General shall present the reasons for interception or surveillance without court warrant under sub-article (3) of this Article to the President of the Federal High Court within 48 hours, and the president shall give appropriate order immediately. 5/ Any irrelevant information collected pursuant to sub-articles (1) to (4) of this Article shall be destroyed immediately upon the decision of the Attorney General. 6/ Any service provider shall cooperate when requested to carry on activities specified under sub-articles (1) and (3) of this Article. 7/ Without prejudice sub-article (5) of this Article, any information collected in accordance with this Article shall be kept confidential.
Article 21 – Interception of content data 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: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: 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. 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.	**CCP 958/2016: Part III PREVENTIVE AND INVESTIGATIVE MEASURES**: **25. Real-time Collection of Computer Data** Without prejudice special provisions stipulated under other laws, 1/ to prevent computer crimes and collect evidence related information, the investigatory organ may, request court warrant to intercept in real-time or conduct surveillance, on computer data, data processing service, or internet and other related communications of suspects, and the court shall decide and determine a relevant organ that could execute interception or surveillance as necessary. 2/ Sub-article (1) of this Article shall only be applicable when there is no other means readily available for collecting such data and this is approved and decided by the Attorney General. 3/ Notwithstanding the provisions of sub-article (1) and (2) of this Article, the Attorney General may give permission to the investigatory organ to conduct interception or surveillance without court warrant where there are reasonable grounds and urgent cases to believe that a computer crime that can damage

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	critical infrastructure is or to be committed. 4/ The Attorney General shall present the reasons for interception or surveillance without court warrant under sub-article (3) of this Article to the President of the Federal High Court within 48 hours, and the president shall give appropriate order immediately. 5/ Any irrelevant information collected pursuant to sub-articles (1) to (4) of this Article shall be destroyed immediately upon the decision of the Attorney General. 6/ Any service provider shall cooperate when requested to carry on activities specified under sub-articles (1) and (3) of this Article. 7/ Without prejudice sub-article (5) of this Article, any information collected in accordance with this Article shall be kept confidential.
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 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: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 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.	**CCP 958/2016: Part V: INSTITUTIONS THAT FOLLOW UP CASES OF COMPUTER CRIME** **40. Jurisdiction** 1/ The Federal High Court shall have first instance jurisdiction over computer crime stipulated under this Proclamation. 2/ The judicial jurisdictions stipulated under Article 13 and Article 17 (1) (b) of the Federal Democratic Republic of Ethiopia Criminal Code shall include computer crimes. **Criminal Code Proclamation No. 414/2004** **Article 13.- Crimes Committed against Ethiopia Outside Its Territory** This Code shall apply to any person who outside Ethiopia has committed one of the crimes against the State of Ethiopia, its safety or integrity, its institutions, essential interests or currency as defined in Book III, Title I, Chapter I, and under Title V of this Book (Art. 238 -260 and Art. 355-374). **Article 17.-Crimes Committed Outside Ethiopia Against International Law or Universal Order**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 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.	(1) Any person who has committed outside Ethiopia: (a) a crime against international law or an international crime specified in Ethiopian legislation, or an international treaty or a convention to which Ethiopia has adhered; or (b) a crime against public health or, morals specified in Articles 525, 599, 635, 636, 640 or 641 of this Code; shall be liable to trial, in Ethiopia in accordance with the provisions of this Code and subject to the general conditions mentioned hereinafter (Arts. 19 and 20(2)) unless a final judgment has been given after being prosecuted in the foreign country. > Article 525.- Producing, Making, Trafficking in or Using Poisonous or Narcotic and Psychotropic Substances. > Article 599.- Participation of Illegal Associations and Juridical Persons in Crimes Specified in this Chapter [CRIMES AGAINST PERSONAL LIBERTY] > Article 635.- Traffic in Women and Minors. > Article 636.- Aggravation to the Crime [trafficking of persons] > Article 640.- Obscene or Indecent Publications > Article 641.- Obscene or Indecent Performances
Chapter III – International co-operation	
Article 24 – Extradition 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. 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. 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.	**CCP 958/2016: Part VI - MISCELLANEOUS PROVISIONS:** **42. International Cooperation** 1/ The Federal Attorney General shall cooperate or enter in to an agreement with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, and extradition and other assistances in accordance with this Proclamation and agreements to which Ethiopia is a party and within the limits of the country's legal system. **Criminal Code Proclamation No. 414/2004** **Article 12.- Special Case: Delegation.** (1) Where a foreigner who has committed a crime in Ethiopia cannot be tried or punished, because he has taken refuge in a foreign country and his extradition cannot be obtained, the Ethiopian authorities may request that he be tried in the country of refuge. **Article 18.- Other Crimes Committed Outside Ethiopia**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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. 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. 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. 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. 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	(1) This Code shall also apply to any person who has committed a crime outside Ethiopia against an Ethiopian national or to any Ethiopian national who has committed outside Ethiopia a crime .of another kind than those specified in the foregoing Articles, if the criminal was not tried in the foreign country for the crime, provided that: (a) the act to be tried is prohibited by the law of the State where it was committed and by Ethiopian law; and (b) it is of sufficient gravity under the latter law to justify extradition. (2) In the case of all other crimes committed outside Ethiopia by a foreign national, the criminal shall, save as otherwise expressly provided, failing extradition, be prosecuted and tried only if the crime is punishable under Ethiopian law with death or with rigorous imprisonment for not less than ten years. **Article 19.- Conditions for Subsidiary Application** (1) This Code shall apply where: (a) the complaint by the victim or his dependants was lodged when it is a condition for prosecution under the law of the place of commission of the crime or under Ethiopian law, (b) the criminal is within the territory of Ethiopia and has not been extradited, or extradition to Ethiopia was obtained by reason of the crime committed; and (c) the crime was not legally pardoned in the country of commission and that prosecution is not barred either under the taw of the country where the crime was committed or under Ethiopian law. (2) The condition specified under sub-article 1 (a) and (c) of this Article need not necessarily be satisfied as regards the lands of crimes prowled for under Article 17 and 18(2) of this code. (3) The prosecution shall consult with the Minister of Justice before instituting proceedings. (4) In case of disparity between the punishments prescribed under this Code and the law of the country of commission, the punishment to be imposed shall be the one, which is more favourable to the accused. **Article 21: Extradition** (1) Any foreigner who commits an ordinary crime outside the territory of Ethiopia and who takes refuge in Ethiopia may be extradited in accordance with the provisions of the law, treaties or international custom; extradition shall be granted on the application made in proper form by the State where the crime was committed for the purpose of trial under the territorial law when the crime does not directly and principally concern the Ethiopian State (Art. 13).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(2) No Ethiopian national having that status at the time of the commission of the crime or at the time of the request for his extradition may be handed over to a foreign country. However, he shall be tried by Ethiopian courts under Ethiopian law. (3) In all cases where a crime raises a question of extradition the request shall be dealt with In accordance with Ethiopian Law and existing treaties. **Article 738.- Application as to Place** (2) Petty offences committed in Ethiopia shall always be tried in accordance with Ethiopian law when the petty offender is in Ethiopia. They shall give rise neither to delegation (Art. 12) nor to extradition (Art. 21).
Article 25 – General principles relating to mutual assistance 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. 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. 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. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.	**CCP 958/2016: Part VI - MISCELLANEOUS PROVISIONS:** **42. International Cooperation** 1/ The Federal Attorney General shall cooperate or enter in to an agreement with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, and extradition and other assistances in accordance with this Proclamation and agreements to which Ethiopia is a party and within the limits of the country's legal system. 2/ For the effective implementation of this Proclamation, the investigatory organ may exchange information with institutions of another country having similar mission, perform joint cooperation in other forms or sign agreement with institutions of another country, when necessary. 3/ Any information or evidence obtained pursuant to this Article shall apply for the purpose of prevention or investigation of computer crimes.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 26 – Spontaneous information 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. 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.	**CCP 958/2016: Part VI - MISCELLANEOUS PROVISIONS:** **42. International Cooperation** 1/ The Federal Attorney General shall cooperate or enter in to an agreement with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, and extradition and other assistances in accordance with this Proclamation and agreements to which Ethiopia is a party and within the limits of the country's legal system. 2/ For the effective implementation of this Proclamation, the investigatory organ may exchange information with institutions of another country having similar mission, perform joint cooperation in other forms or sign agreement with institutions of another country, when necessary. 3/ Any information or evidence obtained pursuant to this Article shall apply for the purpose of prevention or investigation of computer crimes.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 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. 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. b The central authorities shall communicate directly with each other;	**CCP 958/2016: Part VI - MISCELLANEOUS PROVISIONS:** **42. International Cooperation** 1/ The Federal Attorney General shall cooperate or enter in to an agreement with the competent authority of another country in matters concerning computer crime, including the exchange of information, joint investigations, and extradition and other assistances in accordance with this Proclamation and agreements to which Ethiopia is a party and within the limits of the country's legal system. 2/ For the effective implementation of this Proclamation, the investigatory organ may exchange information with institutions of another country having similar mission, perform joint cooperation in other forms or sign agreement with institutions of another country, when necessary.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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; 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. 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. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 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. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 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. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities	3/ Any information or evidence obtained pursuant to this Article shall apply for the purpose of prevention or investigation of computer crimes.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). 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. 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. 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 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. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 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. 4 Any Party that supplies information or material subject to a condition	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and 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. 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. 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 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. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 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. 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 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. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 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. 2 The requested Party shall respond to the request through the application	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or 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 A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	
Article 33 – Mutual assistance in the real-time collection of traffic data 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. 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.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 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. 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. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	
Article 42 – Reservations 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