

Cybercrime legislation – country profile

RUSSIAN FEDERATION

This profile has been prepared within the framework of the Council of Europe’s capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.

Comments may be sent to:

Economic Crime Division
 Directorate General of Human Rights and Legal Affairs
 Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506
 Fax: +33-3-9021-5650
 Email: alexander.seger@coe.int
www.coe.int/cybercrime

| | |
|---|---|
| Country: | Russian Federation |
| Signature of Convention: | No |
| Ratification/accession: | No |
| Provisions of the Convention | Corresponding provisions/solutions in national legislation <i>(pls quote or summarise briefly; pls attach relevant extracts as an appendix)</i> |
| 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 | |

| | |
|---|---|
| <p>automatic processing of data;</p> <p>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;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>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</p> | |
| <p>Chapter II – Measures to be taken at the national level</p> | |
| <p>Section 1 – Substantive criminal law</p> | |
| <p><i>Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems</i></p> | |
| <p>Article 2 – Illegal access</p> <p>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.</p> | <p>Article 272. Illegal Accessing of Computer Information, Criminal Code of Russian Federation</p> <p>1. Illegal accessing of legally-protected computer information, that is, information on machine-readable media, in computers, computer systems, and their networks, if this deed has involved the destruction, blocking, modification, or copying of information, or the disruption of the work of the computers, computer systems, or their networks, shall be punishable by a fine in the amount up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period up to 18 months, or by corrective labour for a term of six to twelve months, or by deprivation of liberty for a term of up to two years.</p> <p>2. The same deed, committed by a group of persons in a preliminary conspiracy or by an organized group, or by a person through his official position, and likewise by a person who has access to computers, computer systems, or their networks, shall be punishable by a fine in the amount of 100 thousand to 300 thousand rubles, or in the amount of the wage or salary, or any other income of the</p> |

| | |
|---|---|
| | convicted person for a period of one to two years, or by corrective labour for a term of one to two years, or by deprivation of liberty for a term of up to five years. |
| <p>Article 3 – Illegal interception</p> <p>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.</p> | |
| <p>Article 4 – Data interference</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p> | <p>Article 273. Creation, Use, and Dissemination of Harmful Computer Viruses, Criminal Code of Russian Federation</p> <p>1. Creation of computer viruses for the introduction of changes to existing programmes, which knowingly leads to the unsanctioned destruction, blocking, modification, or copying of information, the disruption of the work of computers, computer systems, or their networks, and also the use or dissemination of such viruses or machine-readable media with such viruses, shall be punishable by deprivation of liberty for a term of up to three years, with a fine in the amount up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period up to 18 months.</p> <p>2. The same acts, which have involved by negligence grave consequences, shall be punishable by deprivation of liberty for a term of three to seven years.</p> |
| <p>Article 5 – System interference</p> <p>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</p> | <p>Partially, Article 273. Creation, Use, and Dissemination of Harmful Computer Viruses, Criminal Code of Russian Federation</p> <p>1. Creation of computer viruses for the introduction of changes to existing programmes, which knowingly leads to the unsanctioned destruction, blocking, modification, or copying of information, the disruption of the work of computers, computer systems, or their networks, and also the use or dissemination of such viruses or machine-readable media with such viruses, shall be punishable by deprivation of liberty for a term of up to three years, with a fine in the amount up to 200 thousand rubles, or in the amount of the wage or</p> |

| | |
|--|---|
| | <p>salary, or any other income of the convicted person for a period up to 18 months.</p> <p>2. The same acts, which have involved by negligence grave consequences, shall be punishable by deprivation of liberty for a term of three to seven years.</p> |
| <p>Article 6 – Misuse of devices</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>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;</p> <p>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</p> <p>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.</p> <p>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.</p> <p>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.</p> | <p>For Art. 6 (1/a/i) – Partially, Article 273. Creation, Use, and Dissemination of Harmful Computer Viruses, Criminal Code of Russian Federation</p> <p>1. Creation of computer viruses for the introduction of changes to existing programmes, which knowingly leads to the unsanctioned destruction, blocking, modification, or copying of information, the disruption of the work of computers, computer systems, or their networks, and also the use or dissemination of such viruses or machine-readable media with such viruses, shall be punishable by deprivation of liberty for a term of up to three years, with a fine in the amount up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period up to 18 months.</p> <p>2. The same acts, which have involved by negligence grave consequences, shall be punishable by deprivation of liberty for a term of three to seven years.</p> |

| <i>Title 2 – Computer-related offences</i> | |
|---|---|
| <p>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.</p> | <p>Partially see Art. 274 Violation of Rules for the Operation of Computers, Computer Systems, or Their Networks, Criminal Code of Russian Federation</p> <p>1. Violation of rules for the operation of computers, computer systems, or their networks by a person who has access to computers, computer systems, or their networks, which has involved the destruction, blocking, or modification of legally-protected computer information, if this act has inflicted substantial damage,</p> <p>shall be punishable by disqualification to hold specified offices or to engage in specified activities for a term of up to five years, or by compulsory works for a term of 180 to 240 hours, or by restraint of liberty for a term of up to two years.</p> <p>2. The same act, which has involved by negligence grave consequences,</p> <p>shall be punishable by deprivation of liberty for a term of up to four years.</p> |
| <p>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:</p> <ul style="list-style-type: none"> a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p> | |
| <i>Title 3 – Content-related offences</i> | |
| <p>Article 9 – Offences related to child pornography</p> | <p>Art. 242, 242.1 of Criminal Code of Russian Federation</p> |

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally 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, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

Article 242. Illegal Distribution of Pornographic Materials or Objects

Illegal making for the purpose of distribution or advertising, dissemination, or advertising of pornographic materials or objects, and likewise illegal trade in printed publications, cine-and-video-materials, pictures, or any other pornographic objects,

shall be punishable by a fine in the amount of 100 thousand to 300 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of one to two years, or by deprivation of liberty for a period of up to two years.

Article 242.1. Making and Circulating Materials or Articles with Pornographic Images of Minors

1. Making, keeping or moving across the State Border of the Russian Federation for the purpose of dissemination, public showing or advertising, or dissemination, public showing or advertising, of materials or articles with pornographic images of known minors, as well as drawing known minors as performers to entertainment events of pornographic nature by a person who has reached the age of 18 years -

shall be punishable by deprivation of liberty for a term of up to six years.

2. The same deeds committed:

- a) by a parent or other person which is obliged under laws to bring up a minor, as well as by a pedagogue or other employee working for an educational, pedagogical, medical or other institution who is obliged to exercise supervision over a minor;
- b) in respect of a person which is known to be under 14 years old;
- c) by a group of persons in a preliminary conspiracy or by an organized group -

| | |
|---|--|
| | shall be punishable by deprivation of liberty for a term of three to eight years. |
| <i>Title 4 – Offences related to infringements of copyright and related rights</i> | |
| <p>Article 10 – Offences related to infringements of copyright and related rights</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the 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.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law 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.</p> <p>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.</p> | <p>Art. 146, 147 of Criminal Code of Russian Federation</p> <p>Article 146. Violation of Copyright and Neighboring Rights.</p> <p>1. Appropriation of authorship (plagiarism), if this act has caused significant damage to the author or another possessor of right,- shall be punishable with a fine in an amount up to 200 thousand rubles or in an amount of the wages or another income of the convicted person for a period up to 18 months, or with obligatory work for a period of one hundred and eighty to two hundred and forty hours, or with an arrest for a period of three to six months.</p> <p>2. Illegal use of objects of copyright or neighboring rights, as well as the acquisition, storage or carriage of counterfeited copies of works or phonograms for the purpose of sale carried out on a large scale- shall be punishable with a fine in an amount up to 200 thousand rubles or in an amount of the wages or another income of the convicted person for a period up to 18 months, or with obligatory work for a period of one hundred and eighty to two hundred and forty hours, or with deprivation of freedom for a period of up to two years.</p> <p>3. Acts stipulated by Item two of this Article, if they have been committed:</p> <ul style="list-style-type: none"> a) abolished b) By a group of persons in preliminary collusion or by an organized group; c) on an especially large scale; d) by a person with the use of his official position,- shall be punishable with deprivation of freedom for a period up to five years with or without a fine in the amount up to 500 thousand rubles or in the amount of the wage or salary, or any other income of the convicted person for a period of up to three years. <p>Note. Acts stipulated by this Article shall be deemed to have been committed on a large scale if the value of the copies of the works or phonograms or the value of the rights for the use of the objects of copyright or neighboring rights exceed 50 thousand rubles, and on an especially large scale - 250 thousand rubles.</p> <p>Article 147. Violation of Inventor's Rights and Patent Rights</p> |

| | |
|--|---|
| | <p>1. Illegal use of an invention, useful model, or industrial design, disclosure of the essence of an invention, useful model, or industrial design, without the consent of its author or applicant and before the official publication of information about them, the illegal acquisition of authorship, or the compelling of co-authorship, if these acts have inflicted damage to a person, shall be punishable by a fine in the amount up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period up to 18 months, or by compulsory works for a term of 180 to 240 hours, or by deprivation of liberty for a term of up to two years.</p> <p>2. The same deeds committed by a group of persons under a preliminary conspiracy or by an organized group, shall be punishable by a fine in the amount of 100 thousand to 300 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of four to eight months, or by arrest for a term of one to two years, or by deprivation of liberty for a term of up to five years.</p> |
| <i>Title 5 – Ancillary liability and sanctions</i> | |
| <p>Article 11 – Attempt and aiding or abetting</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, 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.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p> | <p>Art. 15, 32-36 of Criminal Code of Russian Federation</p> <p>Article 15. Categories of Crimes</p> <p>1. Depending on the nature and degree of social danger, the deeds provided for by this Code shall be divided into crimes of little gravity, crimes of average gravity, grave crimes, and especially grave crimes.</p> <p>2. Intentional and careless acts, for the commission of which the maximum penalty stipulated by this Code does not exceed two years deprivation of liberty, shall be recognized as crimes of little gravity.</p> <p>3. Qualified as the medium-gravity crimes shall be deliberate offences for whose commitment the maximum punishment stipulated by the present Code does not exceed five years of the deprivation of freedom, and careless crimes for whose commitment the maximum punishment stipulated by the present Code exceeds two years of the deprivation of freedom.</p> <p>4. Intentional acts, for the commission of which the maximum penalty stipulated by this Code does not exceed 10 years deprivation of liberty, shall be recognized as grave crimes.</p> |

5. Intentional acts, for the commission of which this Code provides a penalty in the form of deprivation of liberty for a term exceeding 10 years, or a more severe punishment, shall be recognized as especially grave crimes.

Article 32. The Concept of Complicity in a Crime

The intentional joint participation of two or more persons in the commission of a deliberate crime shall be deemed to be complicity in a crime.

Article 33. Types of Accomplices of a Crime

1. In addition to the perpetrator, organizers, instigators, and accessories shall be deemed accomplices.

2. A person who has actually committed a crime or who directly participated in its commission together with other persons (co-perpetrators), and also a person who has committed a crime by using other persons who are not subject to criminal responsibility by reason of age, insanity, or other circumstances provided for by this Code, shall be deemed to be a perpetrator.

3. A person who has organized the commission of a crime or has directed its commission, and also a person who has created an organized group or a criminal community (criminal organization) or has guided them, shall be deemed an organizer.

4. A person who has abetted another person in committing a crime by persuasion, bribery, threat, or by any other method shall be deemed an instigator.

5. A person who has assisted in the commission of a crime by advice, instructions on committing the crime, or removal obstacles to it, and also a person who has promised beforehand to conceal the criminal, means and instruments of commission of the crime, traces of the crime, or objects obtained criminally, and equally a person who has promised beforehand to acquire such objects, shall be deemed to be an accessory.

Article 34. The Responsibility of Accomplices in a Crime

1. The responsibility of accomplices in a crime shall be determined by the character and the degree of the actual participation of each of them in the commission of the crime.

2. Co-perpetrators shall be answerable under the Article of the Special Part of this Code for a crime committed by them jointly, without reference to Article 33

of this Code.

3. The criminal responsibility of an organizer, instigator, and accessory shall ensue under the Article that provides for punishment for the crime committed, with reference to Article 33 of this Code, except for in cases when they simultaneously were co-perpetrators of the crime.

4. A person who is not a participant in a crime specially indicated in the respective Article of the Special Part of this Code and who has taken part in the commission of the crime, stipulated by this Article, shall bear criminal responsibility for the given offence as its organizer, instigator, or accessory.

5. If the perpetrator of a crime fails to carry out this crime owing to circumstances beyond his control, then the rest of the co-perpetrators shall bear criminal responsibility for preparations for a crime or attempted crime. A person who has not managed to abet other persons in committing a crime owing to circumstances, beyond his control shall also bear criminal responsibility for preparations for the crime.

Article 35. The Commission of a Crime by a Group of Persons, by a Group of Persons Under a Preliminary Conspiracy, and by an Organized Group of a Criminal Community (Criminal Organization)

1. A crime shall be deemed to be committed by a group of persons if two or more perpetrators have jointly participated in its commission without a preliminary conspiracy.

2. A crime shall be deemed to be committed by a group of persons in a preliminary conspiracy, if the persons took part in it after they had reached an agreement on the joint commission of a crime.

3. A crime shall be deemed to be committed by an organized group, if it has been committed by a stable group of persons who in advance united for the commission of one or more offences.

4. A crime shall be deemed to be committed by a criminal community (criminal organization), if it has been perpetrated by a united organized group (organization), set up to commit grave and especially grave crimes, or by an association of organized groups set up for these purposes.

5. A person who has created an organized group or a criminal community (criminal organization), or has directed them, shall be subject to criminal responsibility for their organization in cases, provided for by the respective Articles of the Special Part of this Code, and also for all the offences committed by the organized group or the criminal community (criminal organization), if

| | |
|---|---|
| | <p>they have been embraced by his intent. Other participants in the organized group or criminal community (criminal organization) shall bear criminal responsibility for their participation in cases provided for by the relevant Articles of the Special Part of this Code, and also for the crimes, in the preparation and commission of which they have taken part.</p> <p>6. The creation of an organized group in cases which are not envisaged by Articles of the Special Part of this Code shall involve criminal responsibility for preparations for those offences for which it was set up.</p> <p>7. The commission of a crime by a group of persons, a group of persons in a preliminary conspiracy, by an organized group, or a criminal community (criminal organization) shall involve strict punishment on the ground and within the limits provided for by this Code.</p> <p>Article 36. Excess Perpetration of Crimes</p> <p>The commission of a crime that is not embraced by the intent of other accomplices shall be deemed to be an excess of the perpetrator. Other accomplices to the crime shall not be subject to criminal responsibility for the excess of the perpetrator.</p> |
| <p>Article 12 – Corporate liability</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for 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:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the</p> | |

natural persons who have committed the offence.

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 with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Art. 272-274, 146, 147 of Criminal Code of Russian Federation

Article 272. Illegal Accessing of Computer Information

1. Illegal accessing of legally-protected computer information, that is, information on machine-readable media, in computers, computer systems, and their networks, if this deed has involved the destruction, blocking, modification, or copying of information, or the disruption of the work of the computers, computer systems, or their networks, shall be punishable by a fine in the amount up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period up to 18 months, or by corrective labour for a term of six to twelve months, or by deprivation of liberty for a term of up to two years.

2. The same deed, committed by a group of persons in a preliminary conspiracy or by an organized group, or by a person through his official position, and likewise by a person who has access to computers, computer systems, or their networks, shall be punishable by a fine in the amount of 100 thousand to 300 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of one to two years, or by corrective labour for a term of one to two years, or by deprivation of liberty for a term of up to five years.

Article 273. Creation, Use, and Dissemination of Harmful Computer Viruses

1. Creation of computer viruses for the introduction of changes to existing programmes, which knowingly leads to the unsanctioned destruction, blocking, modification, or copying of information, the disruption of the work of computers, computer systems, or their networks, and also the use or dissemination of such viruses or machine-readable media with such viruses, shall be punishable by deprivation of liberty for a term of up to three years, with a fine in the amount up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period up to 18 months.

2. The same acts, which have involved by negligence grave consequences, shall be punishable by deprivation of liberty for a term of three to seven years.

Article 274. Violation of Rules for the Operation of Computers, Computer Systems, or Their Networks

1. Violation of rules for the operation of computers, computer systems, or their networks by a person who has access to computers, computer systems, or their networks, which has involved the destruction, blocking, or modification of legally-protected computer information, if this act has inflicted substantial damage,

shall be punishable by disqualification to hold specified offices or to engage in specified activities for a term of up to five years, or by compulsory works for a term of 180 to 240 hours, or by restraint of liberty for a term of up to two years.

2. The same act, which has involved by negligence grave consequences, shall be punishable by deprivation of liberty for a term of up to four years.

Article 146. Violation of Copyright and Neighboring Rights.

1. Appropriation of authorship (plagiarism), if this act has caused significant damage to the author or another possessor of right,- shall be punishable with a fine in an amount up to 200 thousand rubles or in an amount of the wages or another income of the convicted person for a period up to 18 months, or with obligatory work for a period of one hundred and eighty to two hundred and forty hours, or with an arrest for a period of three to six months.

2. Illegal use of objects of copyright or neighboring rights, as well as the

acquisition, storage or carriage of counterfeited copies of works or phonograms for the purpose of sale carried out on a large scale- shall be punishable with a fine in an amount up to 200 thousand rubles or in an amount of the wages or another income of the convicted person for a period up to 18 months, or with obligatory work for a period of one hundred and eighty to two hundred and forty hours, or with deprivation of freedom for a period of up to two years.

3. Acts stipulated by Item two of this Article, if they have been committed:

a) abolished

b) By a group of persons in preliminary collusion or by an organized group;

c) on an especially large scale;

d) by a person with the use of his official position,-

shall be punishable with deprivation of freedom for a period up to five years with or without a fine in the amount up to 500 thousand rubles or in the amount of the wage or salary, or any other income of the convicted person for a period of up to three years.

Note. Acts stipulated by this Article shall be deemed to have been committed on a large scale if the value of the copies of the works or phonograms or the value of the rights for the use of the objects of copyright or neighboring rights exceed 50 thousand rubles, and on an especially large scale - 250 thousand rubles.

Article 147. Violation of Inventor's Rights and Patent Rights

1. Illegal use of an invention, useful model, or industrial design, disclosure of the essence of an invention, useful model, or industrial design, without the consent of its author or applicant and before the official publication of information about them, the illegal acquisition of authorship, or the compelling of co-authorship, if these acts have inflicted damage to a person,

shall be punishable by a fine in the amount up to 200 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period up to 18 months, or by compulsory works for a term of 180 to 240 hours, or by deprivation of liberty for a term of up to two years.

2. The same deeds committed by a group of persons under a preliminary conspiracy or by an organized group,

shall be punishable by a fine in the amount of 100 thousand to 300 thousand rubles, or in the amount of the wage or salary, or any other income of the convicted person for a period of four to eight months, or by arrest for a term of one to two years, or by deprivation of liberty for a term of up to five years.

| | |
|---|--|
| Section 2 – Procedural law | |
| Article 14 – Scope of procedural provisions | |
| <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.</p> <p>2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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, <p>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</p> | |
| Article 15 – Conditions and safeguards | Art. 2 of the Constitution of Russian Federation, |

| | |
|--|---|
| <p>1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to 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.</p> <p>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.</p> <p>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.</p> | <p>Man, his rights and freedoms are the supreme value. The recognition, observance and protection of the rights and freedoms of man and citizen shall be the obligation of the State.</p> <p>Art. 2 of the Code of Criminal Procedure of Russian Federation Operation of the Criminal Procedural Law in Space</p> <p>1. Proceedings on a criminal case on the territory of the Russian Federation, regardless of the place of committing the crime, shall be conducted in conformity with this Code, unless otherwise stipulated by an international treaty of the Russian Federation.</p> <p>2. The norms of the present Code shall also be applied in the procedure on a criminal case for a crime committed on an air, sea or river vessel, flying the Flag of the Russian Federation, and outside the territory of the Russian Federation, if the said ship is registered in a port of the Russian Federation.</p> |
| <p>Article 16 – Expedited preservation of stored computer data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or 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.</p> <p>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.</p> <p>3 Each Party shall adopt such legislative and other measures as may be</p> | |

| | |
|--|--|
| <p>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.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> | |
| <p>Article 17 – Expedited preservation and partial disclosure of traffic data</p> <p>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:</p> <p>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</p> <p>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.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> | |
| <p>Article 18 – Production order</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>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</p> <p>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.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the 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</p> | |

| | |
|--|--|
| <p>than traffic or content data and by which can be established:</p> <ul style="list-style-type: none"> 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; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. | |
| <p>Article 19 – Search and seizure of stored computer data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <ul style="list-style-type: none"> 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 <p style="padding-left: 40px;">in its territory.</p> <p>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.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:</p> <ul style="list-style-type: none"> 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. <p>4 Each Party shall adopt such legislative and other measures as may be</p> | <p>Art. 182, 183 of Code of Criminal Procedure of Russian Federation</p> <p>Article 182. Grounds and Procedure for Making a Search</p> <ol style="list-style-type: none"> 1. Seen as a ground for making a search shall be the existence of sufficient data to believe that such and such person may keep in such and such place the instruments of crime, objects, documents and valuables which may prove to be of importance to the criminal case. 2. The search shall be performed on the ground of an investigator's resolution. 3. A search in the living quarters shall be effected on the ground of a court decision to be adopted in accordance with the procedure, laid down by Article 165 of the present Code. 4. Before the start of the search, the investigator shall present the resolution on its performance, and in the cases stipulated by the third part of the present Article - the court decision, permitting to make such. 5. Before the start of the search, the investigator shall suggest that the objects, the documents and the valuables, subject to the seizure, which may prove of importance for the criminal case, be given out voluntarily. If these are given out voluntarily and there are no grounds for an apprehension that they may be concealed, the investigator shall have the right not to perform the search. 6. When making a search, any premises may be forced into, if the owner refuses to open them voluntarily. In this case, no unnecessary damage shall be done to the property. 7. The investigator shall take measures to prevent laying bare the circumstances of the private life of the person, in whose living quarters the search was performed, his private and/or family secrets, as well as the circumstances of the private lives of other persons exposed during the search. 8. The investigator shall have the right to prohibit the persons present at the |

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 Articles 14 and 15.

place where the search is carried out, to leave this place and to communicate with one another or with the other persons until the end of the search.

9. While carrying out the search, the objects and the documents which not allowed for possession shall be seized by all means.

10. The seized objects, documents and valuables shall be presented to the attesting witnesses and to the other persons, present at the search, and if necessary, shall be packed and sealed at the scene of the search, which shall be certified with the signatures of the above-said persons.

11. When a search is performed the person whose premises are subjected to it or adult members of the family thereof shall take part. When a search is performed a counsel for the defense and also a lawyer of the person whose premises are subjected to it are entitled to be in attendance.

12. When making a search, a protocol shall be compiled in conformity with Articles 166 and 167 of the present Code.

13. In the protocol shall be pointed out, in what place and under what circumstances the objects, the documents or the valuables were revealed, and whether they were issued of a free will or seized under coercion. All the seized objects, documents and valuables shall be listed, with a precise indication of their quantity, weight, individual features and, if possible, their cost.

14. If during the search attempts were made to destroy or conceal the objects, documents and valuables, subject to seizure, the corresponding entry to this effect shall be made in the protocol with an indication of the taken measures.

15. A copy of the protocol shall be handed in to the person, in whose living quarters the search was made, or to an adult member of his family. If the search was carried out in the premises of an organization, a copy of the protocol shall be handed in against his signature to a representative of the administration of the corresponding organization.

16. The search may also be aimed at finding the wanted persons and the corpses.

Article 183. Grounds and Procedure for Making a Seizure

1. If it is necessary to seize certain objects and documents of importance for the criminal case, and if it is known exactly where they are and who is keeping them, their seizure shall be performed.

2. The seizure shall be carried out in accordance with the order established by Article 182 of the present Code, with the exceptions stipulated by the present Article.

| | |
|--|---|
| | <p>3. The seizure of objects and documents which contain state secrets or other kinds of secrets protected by federal law shall be made by the investigator with the sanction of the public prosecutor.</p> <p>4. The seizure of the documents, containing information on the deposits and the accounts of the citizens in the banks and in the other credit institutions, shall be affected on the ground of the court decision to be adopted in accordance with the procedure established by Article 165 of the present Code.</p> <p>5. Before the start of the seizure, the investigator shall suggest that the objects and the documents, subject to the seizure, be given out voluntarily, and if the refusal follows, he shall make the seizure under coercion.</p> |
| <p>Article 20 – Real-time collection of traffic data</p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> | |

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.

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.

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

Art. 2 of Code of Criminal Procedure Of Russian Federation, Operation of the Criminal Procedural Law in Space

1. Proceedings on a criminal case on the territory of the Russian Federation, regardless of the place of committing the crime, shall be conducted in conformity with this Code, unless otherwise stipulated by an international treaty of the Russian Federation.

2. The norms of the present Code shall also be applied in the procedure on a criminal case for a crime committed on an air, sea or river vessel, flying the Flag

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.

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.

of the Russian Federation, and outside the territory of the Russian Federation, if the said ship is registered in a port of the Russian Federation.

Art. 11, 12 of Criminal Code of Russian Federation

Article 11. The Operation of Criminal Law in Respect of Persons Who Have Committed Crimes in the Territory of the Russian Federation

1. Any person who has committed a crime in the territory of the Russian Federation shall be brought to criminal responsibility under this Code.

2. Crimes committed within the limits of the territorial waters or the air space of the Russian Federation shall be deemed to have been performed in the territory of the Russian Federation. The validity of this Code shall also be extended to offences committed on the continental shelf and in the exclusive economic zone of the Russian Federation.

3. A person who has committed a crime on board a ship registered in a port of the Russian Federation and to or on one on the open sea or in the air space outside the confines of the Russian Federation shall be brought to criminal responsibility under this Code, unless otherwise stipulated by an international agreement of the Russian Federation. Under this Code, criminal responsibility shall also be borne by a person who has committed an offence on board a warship or in a military aircraft of the Russian Federation, regardless of the place of their location.

4. Question of the criminal responsibility of diplomatic representatives of foreign States and other individuals who enjoy immunity shall be settled in conformity with the standards of international law, if these persons have committed crimes in the territory of the Russian Federation.

Article 12. The Operation of Criminal Law in Respect of Persons Who Have Committed Offences Outside the Boundaries of the Russian Federation

1. Citizens of the Russian Federation and stateless persons who permanently reside in the Russian Federation and who have committed crimes outside the boundaries of the Russian Federation shall be brought to criminal responsibility under this Code, if their deeds have been recognized as crimes in the State on whose territory they were committed, and unless these persons have been convicted in the foreign State. In case of conviction of said persons, the punishments may not exceed the upper limit of the sanction provided for by the

| | |
|--|--|
| | <p>laws of the foreign State on whose territory the crimes have been committed.</p> <p>2. Servicemen of the military units of the Russian Federation located beyond the confines of the Russian Federation shall bear criminal responsibility for their crimes committed in the territories of foreign states under this Code, unless otherwise stipulated by international agreements of the Russian Federation.</p> <p>3. Foreign nationals and stateless persons who do not reside permanently in the Russian Federation and who have committed their crimes outside the boundaries of the Russian Federation shall be brought to criminal responsibility under this Code in cases, if the crimes run counter to the interests of the Russian Federation, and in cases provided for by international agreement of the Russian Federation, and unless they have been convicted in a foreign state and are brought to criminal responsibility in the territory of the Russian Federation.</p> |
| <p>Chapter III – International co-operation</p> | |
| <p>Article 24 – Extradition</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> | <p>Art. 13 of Criminal Code of Russian Federation, The Extradition of Persons Who Have Committed Crimes</p> <p>1. Citizens of the Russian Federation who have committed crimes in foreign states shall not be subject to extradition to these states.</p> <p>2. Foreign nationals and stateless persons who have committed offences outside the boundaries of the Russian Federation and who are to be found in the territory of the Russian Federation may be extradited to a foreign state for bringing to be brought to criminal responsibility or to serve their sentences in conformity with international agreement of the Russian Federation.</p> |

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

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.

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.

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;

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 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 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, 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.

| | |
|--|--|
| <p>2 Disclosure of traffic data under paragraph 1 may only be withheld if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p> | |
| <p>Article 31 – Mutual assistance regarding accessing of stored computer data</p> <p>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.</p> <p>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.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <p>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</p> <p>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</p> | |
| <p>Article 32 – Trans-border access to stored computer data with consent or where publicly available</p> <p>A Party may, without the authorisation of another Party:</p> <p>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</p> <p>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.</p> | |
| <p>Article 33 – Mutual assistance in the real-time collection of traffic data</p> <p>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.</p> | |

| | |
|--|--|
| <p>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.</p> | |
| <p>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.</p> | |
| <p>Article 35 – 24/7 Network 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.</p> | |
| <p>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</p> | |

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.