Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 19 May 2009
[Reformat in May 2011]

Legislation on cybercrime – legislative profile

SENEGAL

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:	**Republic of Senegal**
Signature of the Convention:	No
Ratification/Accession	No
Article of the Budapest Convention on Cybercrime	***Solutions in domestic legislation (text of corresponding articles)*** **Law No. 2008-11 of 25 January 2008 on cybercrime**
Chapter I – Terminology	
Article 1 – Definitions For the purposes of this Convention:	**Article 431-7 :** For the purposes of this law:

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.	1. *"Electronic communication"* means making available to the public, or to a section of the public, by a process of electronic or magnetic communication, signs, signals, written material, images, sounds or messages of any kind; 2. *"Computerised data"* means any facts, information or concepts represented in a form which lends itself to computerised treatment; 3. *"Racist and xenophobic in respect of information and communicaton technologies"* means any written material, any image or any other representation of ideas or theories advocating or encouraging hatred, discrimination or violence against a person or group of persons on grounds of race, colour, parentage or national or ethnic origin or religion, in so far as such ground is used as a pretext for one or other of these elements or incites such acts; 4. *"Minor"* means any person below the age of 18 years within the meaning of the United Nations Convention on the Rights of the Child; 5. *"Child pornography"* means any data of whatever nature or form constituting a visual representation of a minor engaging in sexually explicit activity or realistic images representing a minor engaging in sexually explicit activity; 6. *"Computer system"* means any device, whether in isolation or otherwise, or any set of interconnected devices for the automated processing of data, in whole or in part, in the execution of a programme;
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	**Article 431-8:** Anyone fraudulently accessing or attempting to access all or part of a computer system shall be liable to imprisonment for between six (6) months and three (3) years and to a fine between 1,000,000 and 10,000,000 francs or to only one of these two penalties. Anyone fraudulently procuring or attempting to procure any advantage for himself or for another person by gaining access to a computer system shall be

other dishonest intent, or in relation to a computer system that is connected to another computer system.	liable to the same penalties. **Article 431-9 :** Anyone fraudulently remaining or attempting to remain in all or part of a computer system shall be liable to imprisonment for between six (6) months and three (3) years and to a fine between 1,000,000 and 10,000,000 francs or to only one of these two penalties. **Article 431-11 :** Anyone fraudulently accessing or attempting to access, or fraudulently inputting or attempting to input data into, a computer system shall be liable to imprisonment for between one (1) and five (5) years and to a fine between 5,000,000 and 10,000,000 francs or to only one of these two penalties.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, 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.	**Article 431-12:** Anyone fraudulently intercepting or attempting to intercept, by technical means, computer data transmitted non-publicly to, from or within a computer system shall be liable to imprisonment for between one (1) and five (5) years and to a fine between 5,000,000 and 10,000,000 francs or to only one of these two penalties.
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.	**Article 431-13:** Anyone fraudulently damaging or attempting to damage, deleting or attempting to delete, deteriorating or attempting to deteriorate, altering or attempting to alter computerised data shall be liable to imprisonment for between one (1) and five (5) years and to a fine between 5,000,000 and 10,000,000 francs or to only one of these two penalties.
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	**Article 431-10:** Anyone hindering or distorting, or attempting to hinder or distort, the functioning of a computer system shall be liable to imprisonment for between

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.	one (1) and five (5) years and to a fine between 5,000,000 and 10,000,000 francs or to only one of these two penalties.
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 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.	**Article 431-32:** Anyone producing, selling, importing, possessing, distributing, offering, disposing of or making available an item of equipment, computer program, any device or data designed or specially adapted for the commission of one or more of the offences provided for in Articles 431-8 to 431-16 of this law or a password, access code or similar computerised data affording access to all or part of a computer system, shall be liable to the penalties laid down either for the offence itself or for the offence carrying the heaviest penalty.
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.	**Article 431-14:** Anyone producing or making a set of computerised data by inputting, deleting or fraudulently suppressing computerised data stored, processed or transmitted by a computer system, resulting in counterfeit data with the intent that it be considered or acted upon for legal purposes as if it were original, shall be liable to imprisonment for between one (1) and five (5) years and to a fine between 5,000,000 and 10,000,000 francs or to only one of these two penalties. **Article 431-15:** Anyone who knowingly makes use or attempts to make use of the data obtained in the manner referred to in Article 431-14 of this law shall be liable to the same penalties.
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.	**Article 431-16:** Anyone fraudulently procuring any advantage for himself or for another person by inputting, altering, deleting or suppressing computerised data, or through any form of interference with the functioning of a computer system, shall be liable to imprisonment for between one (1) and five (5) years and to a fine between 5,000,000 and 10,000,000 francs or to only one of these two penalties.
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	**Article 431-7, 5:** For the purposes of this law: 5. "Child pornography" means any data of whatever kind or form constituting a visual representation of a minor engaging in sexually explicit activity or realistic images representing a minor engaging in sexually explicit activity; **Article 431-34:** Anyone producing, recording, offering, making available, distributing or transmitting an image or representation of a child pornography nature by means of a computer system shall be liable to imprisonment for between five (5) and

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.	ten (10) years and to a fine between 5,000,000 and 15,000,000 francs or to only one of these two penalties. **Article 431-35:** Anyone procuring for himself or for another person, importing or causing to be imported, exporting or causing to be exported, an image or representation of a child pornography nature by means of a computer system shall be liable to imprisonment for between five (5) and ten (10) years and to a fine between 5,000,000 and 15,000,000 francs or to only one of these two penalties. **Article 431-36:** Anyone possessing an image or representation of a child pornography nature in a computer system or any means of storage shall be liable to the same penalties. Anyone facilitating access for a minor to images, documents, sounds or representations of a pornographic nature shall be liable to the same penalties. **Article 431-37:** When they are committed by persons acting together, the offences set out in this law shall incur the maximum penalties provided for in Article 431-23 of this law.
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.	
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 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.	See the cases of aiding and abetting covered by previous articles. **Article 431-62:** Legal persons other than the state, local authorities and public establishments are criminally liable for the offences set down in this law and committed on their behalf by their organs or representatives. The liability of legal persons does not exclude that of natural persons who commit or are accomplices to the same offences. The penalties incurred by legal persons are: 1) a fine, the maximum amount of which is equal to five times that laid down for natural persons by the law covering the offence; 2) winding-up, where the legal person was set up or, in the case of a criminal offence for which a natural person incurs a penalty of imprisonment for more than five (5) years, was diverted from its purpose in order to commit the

	offences; 3) permanent prohibition or prohibition for a maximum period of five (5) years from engaging either directly or indirectly in one or more occupational or social activities; 4) permanent closure or closure for a maximum period of five (5) years of one or more establishments of the company which served to commit the offences; 5) permanent exclusion or exclusion for a maximum period of five (5) years from public tendering; 6) permanent prohibition or prohibition for a maximum period of five (5) years from inviting public investment; 7) prohibition for a maximum period of five (5) years from issuing cheques other than for the drawer to withdraw moneys from the drawee or certified cheques or from using payment cards; 8) confiscation of the object which was used or was intended to commit the offence or the object resulting from it; 9) public display of the decision handed down or its announcement either in the press or by any electronic medium of public communication.
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	**CHAPTER X: CRIMINAL LIABILITY** **Article 431-62:** Legal persons other than the state, local authorities and public establishments are criminally liable for the offences set down in this law and committed on their behalf by their organs or representatives. The liability of legal persons does not exclude that of natural persons who commit or are accomplices to the same offences. The penalties incurred by legal persons are: 1) a fine, the maximum amount of which is equal to five times that laid down

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.	for natural persons by the law covering the offence; 2) winding-up, where the legal person was set up or, in the case of a criminal offence for which a natural person incurs a penalty of imprisonment for more than five (5) years, was diverted from its purpose in order to commit the offences; 3) permanent prohibition or prohibition for a maximum period of five (5) years from engaging either directly or indirectly in one or more occupational or social activities; 4) permanent closure or closure for a maximum period of five (5) years of one or more establishments of the company which served to commit the offences; 5) permanent exclusion or exclusion for a maximum period of five (5) years from public tendering; 6) permanent prohibition or prohibition for a maximum period of five (5) years from inviting public investment; 7) prohibition for a maximum period of five (5) years from issuing cheques other than for the drawer to withdraw moneys from the drawee or certified cheques or from using payment cards; 8) confiscation of the object which was used or was intended to commit the offence or the object resulting from it; 9) public display of the decision handed down or its announcement either in the press or by any electronic medium of public communication. **Article 431-63:** However, with the exception of press offences committed via the internet, the criminal offences provided for in Book III, Title I, Chapter IV, Section IV of the criminal code, when committed through a digital communication medium, are subject to the rules on liability under the ordinary law. **Article 431-64:** Where there is a conviction for an offence committed through a digital communication medium, the court may impose by way of additional penalty a

	prohibition on transmitting digital messages or a permanent or temporary prohibition on access to the site which served to commit the offence, or block access to it by any available technical means or even prohibit its hosting. The court may place an order on any person legally responsible for the site, or on any person qualified to operate the requisite technical means, in order to ensure the prohibition on access or hosting or the blocking of access to the impugned site. Infringement of the prohibitions imposed by the court shall incur a penalty of imprisonment for between six (6) months and three (3) years and a fine between 300,000 and 5,000,000 francs. **Article 431-65:** In the case of a conviction for an offence committed through a digital communication medium, the court shall order by way of additional penalty that an extract of the decision be published in that same medium at the offender's expense. The publication referred to in the preceding paragraph shall take place within 15 days following the day on which the judgment became final. A convicted person who fails to have published or to publish the extract referred to in the preceding paragraph shall incur the penalties provided for in the criminal code. If the convicted person fails to have published or to publish that extract within fifteen (15) days after the judgment became final, the penalties laid down in this article shall be doubled. Article 2: A Title XVI shall be introduced into Book IV of the code of criminal procedure headed "Procedure in the case of offences committed by means of information and communication technologies", comprising Articles 677-34 to 677-42, to read as follows:
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.	
Section 2 – Procedural law	
Title 1 – Common provisions	
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 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.	
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. 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.	
Title 2 – Expedited preservation of stored computer data	
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	**Article 677-35:** If the needs of the investigation so require, especially where there is reason to think that computerised data stored in a computer system are particularly vulnerable to loss or modification, the investigating judge may order any person to preserve and protect the integrity of the data in his possession or under his

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.	control for a maximum period of two years, so as to enable the judicial inquiry to proceed correctly. The person holding the data or any other person responsible for preserving them is required to maintain confidentiality. *Any infringement of confidentiality shall incur the penalties applicable to the offence of violation of professional confidentiality..*
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 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.	
Title 3 – Production order	

Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to 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; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Title 4 – Search and seizure of stored computer data	
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	**Article 677-36:** Where data stored in a computer system or in a medium enabling computer data to be kept on Senegalese territory are useful for the purpose of establishing the truth, the investigating judge may conduct a search or access a computer system or part thereof or another computer system where this data is accessible from the original system or available to the original system. If it has previously been shown that this data, accessible from the original

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 Articles 14 and 15.	system or available to the original system, is stored in another computer system situated outside the national territory, it shall be collected by the investigating judge subject to the conditions of access laid down in the international agreements in force.
Title 5 – Real-time collection of computer data	
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and	**Article 677-38 :** If the needs of the investigation so require, the investigating judge may use the appropriate technical means for the real-time collection or recording of data associated with the content of specific communications transmitted by way of a

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 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.	computer system or oblige a service provider, within the framework of his technical capabilities, to collect or record the said computer data using existing technical means, or to help and assist the competent authorities in the collection and recording of that computer data. The service provider shall be obliged to observe confidentiality. Any infringement of confidentiality shall incur the penalties applicable to the offence of violation of professional confidentiality.
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	**Article 677-38:** If the needs of the investigation so require, the investigating judge may use the appropriate technical means for the real-time collection or recording of data associated with the content of specific communications transmitted by way of a computer system or oblige a service provider, within the framework of his technical capabilities, to collect or record the said computer data using existing technical means, or to help and assist the competent authorities in the collection and recording of that computer data. The service provider shall be obliged to observe confidentiality. Any infringement of confidentiality shall incur the penalties applicable to the

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.	offence of violation of professional confidentiality.
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.	

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5 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.	