Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version May 2011

Cybercrime legislation – country profile

FRANCE

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:	**France**
Signature of Convention:	23.11.2001
Ratification/accession:	10.01.2006
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)*
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;	

b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	
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 other dishonest intent, or in relation to a computer system that is connected to another computer system.	**ARTICLE 323-1 Criminal Code** Fraudulently accessing or remaining within all or part of an automated data processing system is punished by two year's imprisonment and a fine of €30,000. Where this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is three years' imprisonment and a fine of €45,000.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**ARTICLE 226-15, Paragraph 2 Criminal Code** The same penalty applies to the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by means of telecommunication, or the setting up of a device designed to produce such interceptions.

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 323-1, paragraph 2 Criminal Code** Where this behaviour causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence is three years' imprisonment and a fine of €45,000.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	**ARTICLE 323-1 Criminal Code** Fraudulently accessing or remaining within all or part of an automated data processing system is punished by two year's imprisonment and a fine of €30,000.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise 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	**ARTICLE 323-3-1 Criminal Code** A person who, without lawful authority, imports, possesses, offers, transfers or makes available any equipment, instrument, computer programme or information created or specially adapted to commit one or more of the offences prohibited by articles 323-1 to 323-3, is punished by the penalties prescribed for the offence itself, or the one that carries the heaviest penalty.

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.	
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 323-4 Criminal Code** Participating in a group or conspiracy established with a view to the preparation of one or more offences set out under articles 323-1 to 323-3-1, and demonstrated by one or more material actions, is punished by the penalties prescribed for offence in preparation, or the one that carries the heaviest penalty.
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 323-3-1 Criminal Code** A person who, without lawful authority, imports, possesses, offers, transfers or makes available any equipment, instrument, computer programme or information created or specially adapted to commit one or more of the offences prohibited by articles 323-1 to 323-3, is punished by the penalties prescribed for the offence itself, or the one that carries the heaviest penalty.
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	**ARTICLE 227-23 Criminal Code** Taking, recording or transmitting a picture or representation of a minor with

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.	a view to circulating it, where that image or representation has a pornographic character, is punished by three years' imprisonment and a fine of €45,000. Attempting to do so is subject to the same penalties. The same penalty applies to offering or distributing such a picture or representation by any means, and to importing or exporting it, or causing it to be imported or exported. The penalties are increased to five years' imprisonment and a fine of €75,000 where use was made of a communication network for the circulation of messages to an unrestricted public in order to circulate the image or representation of a minor. Possessing such an image or representation is punished by two years' imprisonment and a fine of €30,000. The offences set out in the second, third and fourth paragraphs are punished by ten years' imprisonment and by a fine of €500,000 where they are committed by an organised gang. The provisions of the present article also apply to the pornographic images of a person whose physical appearance is that of a minor unless it is proved that the person was over eighteen on the day his picture was taken or recorded. **ARTICLE 227-24 Criminal Code** The manufacture, transport, distribution by whatever means and however supported, of a message bearing a pornographic or violent character or a character seriously violating human dignity or incite minors to engage in games involving physical danger, or the trafficking in such a message, is punished by three years' imprisonment and a fine of €75,000, where the message may be seen or perceived by a minor. Where the offences under the present article are committed through the press or by broadcasting, the specific legal provisions governing those matters are applicable to define the persons who are responsible.
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.	**ARTICLE 323-7 Criminal Code** Attempt to commit the misdemeanours referred to under articles 323-1 to 323-3-1 is subject to the same penalties

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**ARTICLE 323-6 Criminal Code** Legal persons may incur criminal liability for the offences referred to under the present chapter pursuant to the conditions set out under article 121-2. The penalties incurred by legal persons are: 1° a fine, pursuant to the conditions set out under article 131-38; 2° the penalties referred to under article 131-39. The prohibition referred to under 2° of article 131-39 applies to the activity in the course of which or on the occasion of the performance of which the offence was committed.
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.	**ARTICLE 323-6 Criminal Code** Legal persons may incur criminal liability for the offences referred to under the present chapter pursuant to the conditions set out under article 121-2. The penalties incurred by legal persons are: 1° a fine, pursuant to the conditions set out under article 131-38; 2° the penalties referred to under article 131-39. The prohibition referred to under 2° of article 131-39 applies to the activity in the course of which or on the occasion of the performance of which the offence was committed.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.	**For ART. 14 (1-2)- ART. 56 Criminal Procedure Code ART. 57-1 Criminal Procedure Code et ART. 94 Criminal Procedure Code**

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 56 Criminal Procedure Code** Where the type of the felony is such that evidence of it may be collected by seizing papers, documents, electronic data or other articles in the possession of the persons who appear to be involved in the felony or to be in possession of documents, information or articles pertaining to the criminal offence, the judicial police officer proceeds forthwith to the domicile of such persons to initiate a search, in respect of which he draws up an official report. He is the only person, together with those persons mentioned under article 57 and any persons upon whom he calls pursuant to article 60, to be allowed to examine the papers or documents electronic data before proceeding to seize them. However, he has the duty first to initiate any step appropriate to ensure the observance of professional secrecy and of the defendant's rights. Any article or document seized is immediately entered on an inventory and placed under official seals. However, if it is difficult to make such an inventory on the spot, they are put under temporary closed official seals until such time as an inventory can be taken and they can be placed under final official seals. This is done in the presence of the persons who have witnessed the search pursuant to the conditions set out by article 57. The seizure of any electronic data necessary for the discovery of the truth is carried out by placing in the hands of justice, either the physical medium holding this data or a copy of the data made in the presence of those persons present at the seizure. If a copy is made, then on the orders of the district prosecutor, any electronic data the possession or use of which is illegal or dangerous to the safety of persons or property may be permanently erased from any physical medium that has not been placed in judicial safekeeping. With the agreement of the district prosecutor, the judicial police officer only allows the seizure of articles, documents or electronic data useful for the discovery of the truth. Where the seizure involves money, ingots, property or securities, the preservation of which in their original form is not necessary for the discovery of the truth, the district prosecutor may authorise their deposit in the Deposit and Consignment Office or at the Bank of France. Where the seizure involves forged euro bank notes or coins, the judicial police officer must send at least one example of each type of note or coin

	suspected of being false to the national laboratory authorised for this task, for analysis and identification,. The national laboratory may open the official seals. It draws up an inventory in a report which must mention any opening or re-opening of the seals. When these operations are completed, the report and the sealed objects are put into the hands of the clerk of the appropriate court. This transfer is recorded in an official report. The provisions of the previous paragraph do not apply where only one example of a particular type of suspect banknote or coin exists and it is needed for the discovery of the truth. If they are seem able to provide information about articles, documents or electronic data seized, the persons present when the seizure is made may be kept at the scene of the seizure by the judicial police officer for as long as is necessary to complete these operations. **Article 57-1 Criminal Procedure Code** Judicial police officers or judicial police agents under their supervision may, during the course of a seizure carried out in the conditions laid down by the present Code, access any data relevant to the inquiry in progress stored in a computer system set up within the premises where the seizure is carried out or in another computer system, provided the data is accessible from the initial system or is available for the initial system. Where it is known in advance that data which is accessible from the initial system or available for the initial system is stored in another computer system situated outside the territory of the French Republic, it is collected by a judicial police officer, pursuant to the conditions of access provided by any international agreements currently in force. The data which has been accessed pursuant to the conditions of the present article may be copied onto any medium. Any computer storage equipment may be seized and placed in judicial safekeeping under the conditions laid down by the present Code. **Article 94 Criminal Procedure Code** Searches are made in all the places where items or electronic data may be found which could be useful for the discovery of the truth.

	Article 97 Criminal Procedure Code Where in the course of an investigation there is a need to search for documents or electronic data, and subject to the requirements of the investigation and compliance, where necessary, with the obligation imposed by the third paragraph of the previous article, the investigating judge or the judicial police officer commissioned by him has the sole right to examine such documents before carrying out the seizure. An inventory is made of all items, documents and electronic data placed in judicial safekeeping, which are immediately placed under official seals. However, if this is difficult to do on the spot, the judicial police officer proceeds as indicated under the fourth paragraph of article 56. The seizure of any electronic data necessary for the discovery of the truth is carried out either by seizure of the physical medium in which the data is held or by means of a copy of the data made in the presence of those persons who were present at the seizure. If a copy is made, then on the orders of the district prosecutor, any electronic data the possession or use of which is illegal or dangerous to the safety of persons or property may be permanently erased from any physical medium that has not been placed in judicial safekeeping. With the agreement of the investigating judge, the judicial police officer only allows the seizure of articles, documents or electronic data useful for the discovery of the truth. If these official seals are closed, they may be opened and the documents examined only in the presence of the person under judicial examination in the presence of his advocate, or where the latter has been duly summoned. The third party in whose residence the seizure was made is also invited to attend during this operation. Unless the requirements of the investigation prevent it, a copy or photocopy of the documents or electronic data placed under judicial safekeeping may be delivered as soon as possible to any persons concerned who request it at their own expense. If the seizure comprises monies, ingots, papers or securities which do not necessarily have to be preserved in kind for the discovery of the truth or for the safeguarding of the rights of the parties, he may authorise the clerk to deposit them with the Deposit and Consignment Office or with the Bank of France.

	If the seizure comprises counterfeit banknotes or coins, the investigating judge or the judicial police officer working with him must provide the national analysis centre with at least one example of each type of coin or banknote suspected of being fake. The national analysis centre may proceed to open any seals. It makes a list in a report which must record any opening or reopening of the seals. When the process of testing is complete, the report and the seals must be put into the hands of a clerk in the relevant court of law. An official record is made of their being so deposited. The requirements of the preceding paragraph do not apply in cases where there is only one suspected fake coin or note, and this is needed to establish the truth.
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.	**Article 57 Criminal Procedure Code** Subject to the terms of the previous article concerning the observance of professional secrecy and of the defendant's rights, the operations prescribed by that article are made in the presence of the person in whose domicile the search is made. Where this is impossible, the judicial police officer has the duty to ask him to appoint a representative of his choice; failing this, the judicial police officer will appoint two witnesses, chosen for this purpose from among persons who are not under his administrative authority. The official report of these operations is drafted as described under article 66 and is signed by the persons mentioned by the present article; in the event of a refusal, this is noted in the official report. Article 96 Paragraph 3 Criminal Procedure Code The provisions of articles 56, 56-1, 56-2 and 56-3 apply to searches carried out by the investigating judge. **Article 97 Paragraph 2 Criminal Procedure Code** An inventory is made of all items, documents and electronic data placed in judicial safekeeping, which are immediately placed under official seals. However, if this is difficult to do on the spot, the judicial police officer proceeds as indicated under the fourth paragraph of article 56
Article 16 – Expedited preservation of stored computer data	**Article 56, paragraph 7, Criminal Procedure Code**

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	With the agreement of the district prosecutor, the judicial police officer only allows the seizure of articles, documents or electronic data useful for the discovery of the truth. Where the seizure involves money, ingots, property or securities, the preservation of which in their original form is not necessary for the discovery of the truth, the district prosecutor may authorise their deposit in the Deposit and Consignment Office or at the Bank of France.
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.	**Article 60-2, paragraph 2 Criminal Procedure Code** A judicial police officer, intervening on the orders of a district prosecutor authorised in advance by a decree from the liberty and custody judge, may require telecommunications operators, particularly those mentioned in 1 of I of article 6 of Law no. 2004-575 of 21 June 2004 relating to confidence in the digital economy, to take without delay all appropriate measures to ensure the preservation, for a period that may not exceed one year, of the text of the information consulted by persons using the services provided by the operators

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
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.	**Article 56 Paragraph 1 Criminal Procedure Code** If they are seem able to provide information about articles, documents or electronic data seized, the persons present when the seizure is made may be kept at the scene of the seizure by the judicial police officer for as long as is necessary to complete these operations. **Article 60-1 Criminal Procedure Code** A judicial police officer may order any person, establishment or organisation, whether public or private, or any public services likely to possess any documents relevant to the inquiry in progress, including those produced from a registered computer or data processing system, to provide them with these documents. Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance. Where such orders relate to the persons mentioned in articles 56-1 to 56-3, the transfer of these documents may only take place with their consent. With the exception of the persons mentioned in articles 56-1 to 56-3, the failure to respond to such an order as quickly as possible is punished by a fine of €3,570. Legal persons are criminally responsible for the offence set out in the present paragraph, under the conditions provided for by article 121-2 of the Criminal Code. **Article 60-2 Criminal Procedure Code** At the request of a judicial police officer, who can intervene by means of telecommunications or computers, public organisations or private legal persons, with the exception of those set out in the second paragraph of article 31 and article 33 of Law no. 78-17 of 6 January 1978 relating to computers, databases and liberties, must make available information helpful for the discovery of the truth, with the exception of information the secrecy of which is protected by statute, where it is stored in one or more computer or data processing systems that they administer.

	A judicial police officer, intervening on the orders of a district prosecutor authorised in advance by a decree from the liberty and custody judge, may require telecommunications operators, particularly those mentioned in 1 of I of article 6 of Law no. 2004-575 of 21 June 2004 relating to confidence in the digital economy, to take without delay all appropriate measures to ensure the preservation, for a period that may not exceed one year, of the text of the information consulted by persons using the services provided by the operators. The organisations or persons to which this article applies must make the required information available as quickly as possible by means of telecommunication or computers. Refusal to respond to such a request without a legitimate reason is punished by a fine of €3,750. Legal persons may be declared criminally responsible for the offence set out in the present article under the conditions laid down by article 121-2 of the Criminal Code. The penalty incurred by these legal persons is a fine, pursuant to the provisions outlined in article 131-38 of the Criminal Code. A Decree of the Conseil d'Etat made on the advice of the National Commission for Data Protection determines the categories of organisation covered by the first paragraph, and also the methods for examining, transmitting and processing the required information. **Article 99-3** An investigating judge or judicial police officer delegated by him may order any person, establishment or organisation, whether public or private, or any public services liable to possess any documents relevant to the investigation, including those produced from a registered computer or data processing system, to provide them with these documents. Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance with such an order. Where these orders relate to the persons mentioned in articles 56-1 to 56-3, the transfer of these documents may only take place with their consent. Where the person does not respond to this order, the provisions of the second paragraph of article 60-1 are applicable
Article 19 – Search and seizure of stored computer data	**Article 56 Criminal Procedure Code**

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Where the type of the felony is such that evidence of it may be collected by seizing papers, documents, electronic data or other articles in the possession of the persons who appear to be involved in the felony or to be in possession of documents, information or articles pertaining to the criminal offence, the judicial police officer proceeds forthwith to the domicile of such persons to initiate a search, in respect of which he draws up an official report. He is the only person, together with those persons mentioned under article 57 and any persons upon whom he calls pursuant to article 60, to be allowed to examine the papers or documents electronic data before proceeding to seize them. However, he has the duty first to initiate any step appropriate to ensure the observance of professional secrecy and of the defendant's rights. Any article or document seized is immediately entered on an inventory and placed under official seals. However, if it is difficult to make such an inventory on the spot, they are put under temporary closed official seals until such time as an inventory can be taken and they can be placed under final official seals. This is done in the presence of the persons who have witnessed the search pursuant to the conditions set out by article 57. The seizure of any electronic data necessary for the discovery of the truth is carried out by placing in the hands of justice, either the physical medium holding this data or a copy of the data made in the presence of those persons present at the seizure. If a copy is made, then on the orders of the district prosecutor, any electronic data the possession or use of which is illegal or dangerous to the safety of persons or property may be permanently erased from any physical medium that has not been placed in judicial safekeeping. With the agreement of the district prosecutor, the judicial police officer only allows the seizure of articles, documents or electronic data useful for the discovery of the truth.

	Where the seizure involves money, ingots, property or securities, the preservation of which in their original form is not necessary for the discovery of the truth, the district prosecutor may authorise their deposit in the Deposit and Consignment Office or at the Bank of France. Where the seizure involves forged euro bank notes or coins, the judicial police officer must send at least one example of each type of note or coin suspected of being false to the national laboratory authorised for this task, for analysis and identification,. The national laboratory may open the official seals. It draws up an inventory in a report which must mention any opening or re-opening of the seals. When these operations are completed, the report and the sealed objects are put into the hands of the clerk of the appropriate court. This transfer is recorded in an official report. The provisions of the previous paragraph do not apply where only one example of a particular type of suspect banknote or coin exists and it is needed for the discovery of the truth. If they are seem able to provide information about articles, documents or electronic data seized, the persons present when the seizure is made may be kept at the scene of the seizure by the judicial police officer for as long as is necessary to complete these operations. **Article 97 Paragraph 3 and 4 Criminal Procedure Code** The seizure of any electronic data necessary for the discovery of the truth is carried out either by seizure of the physical medium in which the data is held or by means of a copy of the data made in the presence of those persons who were present at the seizure. If a copy is made, then on the orders of the district prosecutor, any electronic data the possession or use of which is illegal or dangerous to the safety of persons or property may be permanently erased from any physical medium that has not been placed in judicial safekeeping.
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be	**Article 60-2 Criminal Procedure Code**

necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal 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.	At the request of a judicial police officer, who can intervene by means of telecommunications or computers, public organisations or private legal persons, with the exception of those set out in the second paragraph of article 31 and article 33 of Law no. 78-17 of 6 January 1978 relating to computers, databases and liberties, must make available information helpful for the discovery of the truth, with the exception of information the secrecy of which is protected by statute, where it is stored in one or more computer or data processing systems that they administer. A judicial police officer, intervening on the orders of a district prosecutor authorised in advance by a decree from the liberty and custody judge, may require telecommunications operators, particularly those mentioned in 1 of I of article 6 of Law no. 2004-575 of 21 June 2004 relating to confidence in the digital economy, to take without delay all appropriate measures to ensure the preservation, for a period that may not exceed one year, of the text of the information consulted by persons using the services provided by the operators. The organisations or persons to which this article applies must make the required information available as quickly as possible by means of telecommunication or computers. Refusal to respond to such a request without a legitimate reason is punished by a fine of €3,750. Legal persons may be declared criminally responsible for the offence set out in the present article under the conditions laid down by article 121-2 of the Criminal Code. The penalty incurred by these legal persons is a fine, pursuant to the provisions outlined in article 131-38 of the Criminal Code. A Decree of the Conseil d'Etat made on the advice of the National Commission for Data Protection determines the categories of organisation covered by the first paragraph, and also the methods for examining, transmitting and processing the required information.
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	**Article 706-95 Criminal Procedure Code** If the needs of a flagrancy inquiry or a preliminary inquiry into one of the offences within the scope of article 706-73 justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor,

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.	authorise the interception, recording or transcription of correspondence by telecommunication, under the provisions of paragraph two of article 100, article 100-1 and articles 100-3 to 100-7, for a maximum period of fifteen days, renewable once under the same conditions of form and duration. These operations are carried out under the supervision of the liberty and custody judge. For the application of the provisions of articles 100-3 to 100-5, the powers conferred on the investigating judge or the judicial police officer nominated by him are exercised by the district prosecutor or the judicial police officer appointed by him. The liberty and custody judge who has authorised this interception is immediately informed by the district prosecutor of any actions carried out in accordance with the first paragraph. **Article 100 Criminal Procedure Code** For the investigation of felonies and misdemeanours, if the penalty incurred is equal to or in excess of two years' imprisonment, the investigating judge may order the interception, recording and transcription of telecommunication correspondence where the requirements of the investigation call for it. Such operations are made under his authority and supervision. The interception decision is made in writing. It is not a jurisdictional decision and is unappealable **Article 100-3 Criminal Procedure Code** The investigating judge or the judicial police officer appointed by him may require any qualified agent of a service or institution placed under the authority or supervision of the Minister in charge of telecommunications, or any qualified agent of a network operator or authorised purveyor of telecommunication services to set up an interception device. **Article 100-6 Criminal Procedure Code** The recordings are destroyed on the request of the district prosecutor or of the

	public prosecutor upon the expiry of the limitation period for prosecution. An official record is made of the destruction.
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. 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.	
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties	**Article 696-1 Criminal Procedure Code** No surrender to a foreign government may be made of any person who is not the object of a prosecution or a conviction for an offence provided for by the

concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or	present section. **Article 692-2 Criminal Procedure Code** The French government may hand over any person who does not have French nationality and who is the subject of a prosecution initiated in the name of the requesting state or of a conviction imposed by its courts, to foreign governments, at their request, where this person is found on French national territory. However, extradition is only granted if the offence for which the application has been made was committed: - either on the territory of the requesting state by a national of this state or by a foreigner; -or outside the territory of the requesting state by a national from that state; -or outside the territory of the requesting state by a foreigner, where the offence features among those for which French law authorises prosecution in France, even if they are committed by a foreigner abroad. **Article 696-3 Criminal Procedure Code** The offences which may result in extradition, whether this is the application for or the granting of extradition, are the following: 1° all offences punished as felonies by the law of the requesting state; 2° offences punished as misdemeanours by the law of the requesting state, where the maximum prison sentence incurred, under that law, is two years or more, or, in the case of a convicted person, where the sentence imposed by the court of the requesting state is at least two years' imprisonment. In no case is extradition granted by the French government if the offence does not incur a punishment for felony or misdemeanour under French law. Facts constituting attempt or complicity are subject to the above rules, on condition that they are punishable under laws of both the requesting and the requested state.

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	If the application concerns a number of offences committed by the requested person and these have not yet been tried, extradition is only granted if the maximum sentence incurred under the law of the requesting state, for all of the offences together, is not less than two years' imprisonment. **Article 696-4 Criminal Procedure Code** Extradition is not granted: 1° where the requested person is of French nationality, as determined at the date of the offence for which the extradition is requested; 2° where the felony or misdemeanour has a political flavour, or where the circumstances reveal that the extradition is requested for political reasons; 3° where the felonies or misdemeanours were committed on French national territory; 4° where the felonies and misdemeanours, while they were committed outside French national territory, were prosecuted and finally disposed of in France; 5° where, under the law of the requesting state or French law, the limitation period for the prosecution has expired prior to the request for extradition, or the limitation period for the penalty has expired prior to the requested person's arrest, and in general whenever the right to prosecute in the requesting state is extinguished; 6° where the offence for which the extradition has been requested is punished by the law of the requesting state which imposes a penalty or a safety measure contrary to French public policy; 7° where the requested person would be tried in the requesting state by a court which does not provide fundamental procedural guarantees and protection for the rights of the defence; 8° where the felony or misdemeanour constitutes a military offence under Book III of the Military Justice Code. **Article 696-5 Criminal Procedure Code** If, for one single offence, extradition is requested concurrently by several states, preference is given to the application by the state against whose interests the offence was directed, or on whose the territory it was committed. If the concurrent applications concern different offences, in order to

	determine priority account is taken of all the circumstances and, in particular, the relative seriousness the offences and the place of their commission, as well as the respective dates of the applications and any undertaking which the requesting state may have made to re-extradite the person concerned. **Article 696-6 Criminal Procedure Code** Subject to the exceptions provided for by article 696-34, extradition is only granted on condition that the extradited person will neither be prosecuted nor convicted for an offence other than the one for which the extradition was requested, this being committed prior to the surrender. **Article 696-7 Criminal Procedure Code** Where a requested person is being prosecuted or has been convicted in France, and the French government is requested to extradite him for another offence, surrender is only carried out after the prosecution is over and, in the case of a conviction, after the sentence has been executed. However, this provision does not prevent the requested person from being temporarily sent to appear before the courts of the requesting state, on the express condition that he will be sent back as soon as the foreign courts have ruled. The provisions of the present article also apply where the requested person is subject to imprisonment in default under the provisions of Title VI of Book V of the present Code.
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.	**Article 695-10 Criminal Procedure Code** The provisions of sections 1 and 2 of Chapter II are applicable to requests for judicial assistance between France and other states which are parties to any Conventions which include stipulations similar to those of the Convention of 29 May 2000 relating to judicial assistance in criminal matters between the member states of the European Union.

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	**Article 695-10 Criminal Procedure Code** The provisions of sections 1 and 2 of Chapter II are applicable to requests for judicial assistance between France and other states which are parties to any Conventions which include stipulations similar to those of the Convention of 29 May 2000 relating to judicial assistance in criminal matters between the member states of the European Union.

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.	**Article 694 Criminal Procedure Code** In the absence of any international conventions stipulating otherwise: 1° Requests for mutual assistance coming from French judicial authorities and addressed to foreign judicial authorities are sent through the intermediary of the Minister of Justice. The enforcement documents are sent to the authorities of the requesting State through the same channels. 2° Requests for judicial assistance coming from foreign judicial authorities are sent through diplomatic channels. The enforcement documents are sent to the authorities of the requesting State through the same channels. In urgent cases, requests for mutual assistance sought by the French or foreign authorities may be directly sent to the authorities of the State who are competent to enforce them. The transmission of the enforcement documents to the authorities of the requested State is carried out in the same way and under the same conditions. However, unless there is an international convention stipulating otherwise, requests for judicial assistance coming from foreign judicial authorities and addressed to the French judicial authorities must be the subject of an opinion sent through diplomatic channels by the foreign government concerned. **Article 694-1 Criminal Procedure Code** In urgent cases, requests for judicial assistance coming from foreign judicial authorities are sent, according to the distinctions set out in article 694-2, to the district prosecutor or the investigating judge of the territorially competent district court. They may also be sent to these judges through the intermediary of the prosecutor general. If the district prosecutor receives a request for judicial assistance directly from a foreign authority which may only be executed by the investigating judge, he sends it to the latter to be carried out, or seises the prosecutor general in the case provided for by article 694-4. Before executing a request for judicial assistance of which he has directly be seised, the investigating judge immediately sends this to the district

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.	prosecutor for his opinion. **Article 694-2 Criminal Procedure Code** Requests for judicial assistance coming from foreign judicial authorities are executed by the district prosecutor or by judicial police officers or agents nominated for this purpose by this prosecutor. They are executed by the investigating judge or judicial police officers acting in the context of a rogatory letter where they require particular procedural acts which may not be ordered or executed in the course of a preparatory investigation. **Article 694-3 Criminal Procedure Code** Requests for judicial assistance coming from foreign judicial authorities are executed according to the procedural rules provided for by the present Code. However, if the request for judicial assistance specifies this, it is executed in accordance with the procedural rules indicated by the competent authorities of the requesting State, on the condition, under penalty of nullity, that these rules do not reduce the rights of the parties or the procedural guarantees provided for by the present Code. Where the request for judicial assistance may not be executed in accordance with the stipulations of the requesting State, the competent French authorities immediately inform the authorities of the requesting State and indicate under which conditions the request may be executed. The competent French authorities and those of the requesting State may agree on the outcome of this request later on, where appropriate by subjecting it to the aforesaid conditions. The irregularity of the sending of the request for judicial assistance may not constitute grounds for nullity of the acts executed in enforcing this request. **Article 694-4 Criminal Procedure Code** If the enforcement of a request for judicial assistance coming from a foreign judicial authority is liable to threaten public order or the fundamental interests of the nation, the district prosecutor seised of this request in accordance with the third paragraph of article 694-1 sends this to the prosecutor general who decides, if appropriate, to seise the Minister of Justice and gives, where

	applicable, notice of this reference to the investigating judge. If he is seised, the Minister of Justice informs the authority which made the request, if appropriate, that no action, total or partial, may be taken in relation to the request. This information is communicated to the judicial authority concerned and blocks the enforcement of the request for judicial assistance or the return of the enforcement documents.
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 695-10 Criminal Procedure Code** The provisions of sections 1 and 2 of Chapter II are applicable to requests for judicial assistance between France and other states which are parties to any Conventions which include stipulations similar to those of the Convention of 29 May 2000 relating to judicial assistance in criminal matters between the member states of the European Union.
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	**Article 695-10 Criminal Procedure Code** The provisions of sections 1 and 2 of Chapter II are applicable to requests for judicial assistance between France and other states which are parties to any Conventions which include stipulations similar to those of the Convention of 29 May 2000 relating to judicial assistance in criminal matters between the member states of the European Union.

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. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	**Article 695-10 Criminal Procedure Code** The provisions of sections 1 and 2 of Chapter II are applicable to requests for judicial assistance between France and other states which are parties to any Conventions which include stipulations similar to those of the Convention of 29 May 2000 relating to judicial assistance in criminal matters between the member states of the European Union.
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	**Article 695-10 Criminal Procedure Code** The provisions of sections 1 and 2 of Chapter II are applicable to requests for judicial assistance between France and other states which are parties to any Conventions which include stipulations similar to those of the Convention of 29 May 2000 relating to judicial assistance in criminal matters between the member states of the European Union.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored	**Article 695-10 Criminal Procedure Code** The provisions of sections 1 and 2 of Chapter II are applicable to requests for judicial assistance between France and other states which are parties to any Conventions which include stipulations similar to those of the Convention of 29 May 2000 relating to judicial assistance in criminal matters between the member

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.	states of the European Union.
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	**Article 695-10 Criminal Procedure Code** The provisions of sections 1 and 2 of Chapter II are applicable to requests for judicial assistance between France and other states which are parties to any Conventions which include stipulations similar to those of the Convention of 29 May 2000 relating to judicial assistance in criminal matters between the member states of the European Union.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	**Article 695-10 Criminal Procedure Code** The provisions of sections 1 and 2 of Chapter II are applicable to requests for judicial assistance between France and other states which are parties to any Conventions which include stipulations similar to those of the Convention of 29 May 2000 relating to judicial assistance in criminal matters between the member states of the European Union.
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.	
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	**Declaration contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.** In accordance with Article 21 of the Convention, France shall apply the provisions contained in Article 21 only if the prosecuted offence is punished with a deprivation of liberty superior or equal to two years of custody. **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 21 **Declaration contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.** In accordance with Article 27 of the Convention, France declares that, even in cases of urgency : - requests for mutual assistance from the French judiciary authorities and directed to foreign judiciary authorities are transmitted through the Ministry of Justice (*Ministère de la Justice, 13, Place Vendôme, 75042 Paris Cedex 01*); - requests for mutual assistance from foreign judiciary authorities and directed to the French judiciary authorities are transmitted through diplomatic channel (*Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP*). **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 27

Reservation contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.

In accordance with Article 9, paragraph 2.b, of the Convention, France shall apply Article 9, paragraph 1, to any pornographic material that visually depicts a person appearing to be a minor engaged in sexually explicit conduct, in so far as it is not proved that the said person was 18 years old on the day of the fixing or the registering of his or her image.
Period covered: 1/5/2006 -
The preceding statement concerns Article(s) : 9

Reservation contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.

In accordance with Article 22 of the Convention, France reserves itself the right not to establish jurisdiction when the offence is committed outside the territorial jurisdiction of any State. France declares also that, whenever the offence is punishable under criminal law where it has been committed, proceedings shall be instituted only upon request from the public prosecutor and must be preceded by a complaint from the victim or his/her beneficiaries or by an official complaint from the authorities of the State where the act was committed (Article 22, paragraph1.d).
Period covered: 1/5/2006 -
The preceding statement concerns Article(s) : 22

Declaration contained in the instrument of approval deposited on 10 January 2006 - Or. Fr.

In accordance with Article 24 of the Convention, France declares that :

- the Ministry for Foreign Affairs is the authority responsible for making or receiving requests for extradition in the absence of a treaty (*Ministère des Affaires étrangères, 37,*

	Quai d'Orsay, 75700 Paris 07 SP); - the territorially competent State Prosecutor shall be the authority responsible for making or receiving requests for provisional arrest in the absence of a treaty. **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 24 **Declaration contained in the instrument of approval deposited on 10 January 2006 - Or. Fr., updated by a communication from France registered at the Secretariat General on 7 July 2010 - Or. Fr.** In accordance with Article 35 of the Convention, France designates as point of contact the Ministry of Interior Central Direction of Judiciary Police (DCPJ)/NCB Interpol France *Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)* 11, Rue des Saussaies F - 75008 Paris Email: oclctic-sec.dcpjaef@interieur.gouv.fr **[Note by the Secretariat** : Detailed contact information are available on the restricted access part of the Convention Committee on Cybercrime's website on www.coe.int/tcy.**]** **Period covered: 1/5/2006 -** The preceding statement concerns Article(s) : 35