Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 30 August 2008
[Reformat in March 2011]

Cybercrime legislation – country profile

BRAZIL

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:	**Brazil**
Signature of Convention:	No
Ratification/accession:	No
Provisions of the Convention	***Corresponding provisions/solutions in national legislation*** *(pls quote or summarise briefly; pls attach relevant extracts as an appendix)* The Ministry of External Relations, The Ministry of Justice (by Federal Police Department (DPF) and International Cooperation and Assets Recovery Department (DRCI)), the Office of Institutional Security of The Presidency of Republic (GSI), The Science and Technology Ministry (MCT) and The Parliament, where is running a legislative project, are involved in analysis of the Convention on Cybercrime.

Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data*":* For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*;* c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	"Computer system", "computer data", "traffic data", "computer network", "communication device", and "malicious code" – terms defined in art. 16 of the Substitute Amendment to Senate bills PLS 76/2000 and PLS 137/2000, in addition to House bill PLC 89/2003, from now on referred to as Substitute, that will be effective after it is passed by Congress; "service provider", is defined in art. 3, Law n. 8078/1990 – Consumer Protection Code Art. 16. For criminal purposes, it is deemed, among others: I – communication device: any means capable of processing, storing, capturing or transmitting data using magnetic, optical ou any other technology; II – computer system: any system capable of processing, capturing, storing or transmitting data electronically or digitally, or by means of an equivalent manner; III - computer network: the set of computers, communication devices and computer systems which are driven by a set of rules, parameters, codes, formats and other information grouped in protocols, in local, regional, national or international topology level, by means of which it is possible to exchange data and information; IV – malicious code: the set of instructions and tables of information or any other system designed to perform damaging action or to obtain data or information in an undue way; V – dados informáticos: any representation of facts, information or or concepts in a form suitable for processing in a computer network, communication device or computer system; VI - traffic data: all computer data related to their communication carried out by means of a computer network, computer system, or communication device, generated by which as elements of a communication chain, indicating the origin,

	destination, itinerary, time, data, size, duration or the kind of service inherent to the communication. Art. 16. Para os efeitos penais considera-se, dentre outros: I - dispositivo de comunicação: qualquer meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia; II - sistema informatizado: qualquer sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente; III - rede de computadores: o conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial através dos quais é possível trocar dados e informações; IV - código malicioso: o conjunto de instruções e tabelas de informações ou qualquer outro sistema desenvolvido para executar ações danosas ou obter dados ou informações de forma indevida; V - dados informáticos: qualquer representação de fatos, de informações ou de conceitos sob forma suscetível de processamento numa rede de computadores ou dispositivo de comunicação ou sistema informatizado; VI - dados de tráfego: todos os dados informáticos relacionados com sua comunicação efetuada por meio de uma rede de computadores, sistema informatizado ou dispositivo de comunicação, gerados por eles como elemento de uma cadeia de comunicação, indicando origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.
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.	Measures adopted to establish illegal access as a criminal offence. Provided for in art. 285-A of the Brazilian Criminal Law, as incorporated by art. 2 of the Substitute Amendment. Art. 285-A is generic and includes provisions as per art. 2 of the Convention; art. 154-B corresponds to **illegal access in its aggravated form** as provided for in the second part of art. 2 of the Convention. Art. 285-A. To access, by means of security violation, computer network, communication device or computer system, protected by access restriction: Penalty – imprisonment ("reclusão"), from 1 (one) to 3 (three) years, and fine. Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. The sole paragraph to Art. 285-A of the Brazilian Criminal Law, as incorporated by art. 2 of the Substitute Amendment, provides for digital larceny (**illegal access to data**) through unauthorized use of password: Sole paragraph. If the perpetrator uses false name or the identity of a third party for the perpetration of the crime, the penalty is increased by one sixth. Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte.
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	Measures adopted to establish illegal interception as a criminal offence. Law n. 9296 (24th. July, 1996), currently in force, in its art. 10, already establishes the interception of telephone, computer or telematic transmissions as criminal offences. It has also been provided for in art. 285-B of the Brazilian Criminal Law, as

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.	incorporated by art. 2 of the Substitute Amendment. Art. 285-B. To obtain or transfer, without authorization or in disconformity with authorization from the legitimate holder of a computer network, communication device or computer system, protected by express access restriction, data or information available in the latter: Penalty – imprisonment (reclusão), from 1 (one) to 3 (three) years, and fine. Sole paragraph. If the data or information obtained without authorization if supplied to third parties, the penalty in increased by one third. Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Se o dado ou informação obtida desautorizadamente é fornecida a terceiros, a pena é aumentada de um terço. To be analyzed the following aspects: - Does it refer to **non-public transmissions** of computer data to, from or within a computer system? Yes - **The act of interception of electromagnetic emissions** from a computer system carrying such computer data **is covered?** Yes (given the definition of computer data) - In order to avoid over criminalisation Art. 3 provides that the interception to be made **without right and by technical means**; Yes
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.	Provided for in art. 163 of the Brazilian Criminal Law, as amended by art. 4 of the Substitute Amendment. Art. 163, as amended, is generic and includes provisions as per art. 4 of the Convention; Art. 163. To destroy, make useless, or deteriorate third party's thing or electronic data:

	Penalty – Imprisonment (reclusão), from 1 (one) to 3 (three) years, and fine. Paragraph 1. If from the crime it results destruction, inutilization, deterioration, alteration, working impairment, or working unauthorized by the legitimate holder, of communication device, computer network, or computer system: Penalty – imprisonment (reclusão), from 2 (two) to 4 (four) years, and fine. Paragraph 2. If the perpetrator uses false name or the identity of a third party for perpetrating the crime, the penalty is increased by one sixth. Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio: Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado: Pena - reclusão, de 1 (um) a 3 (três) anos, e multa. § 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificultação do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. § 2º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."
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	Specific reference to computer system interference exists in Articles 313-A and 313-B of Brazilian Criminal Law regarding public systems, and perpetration by public employees or by service providers to governmental entities: Art. 313-A. To insert or to facilitate, the authorized employee, the insertion of false data, to unduly modify or exclude correct data in the computer systems or data bases of the Public Administration wit the purpose to obtain undue advantage for oneself or for a third party or to cause damage:

	Penalty – imprisonment (reclusão), from 1 (one) to 12 (twelve) years, and fine. Art. 313-B. To modify or alter, the employee, information system or computer program without authorization or request by the competent authority. Penalty – imprisonment (detention), from 3 (three) months to 2 (two) years, and fine. Sole paragraph. The penalties are increased by one third up to half if from the modification or alteration it results damage to the Public Administration or to the citizen. Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000)) Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Incluído pela Lei nº 9.983, de 2000) Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000) Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa. (Incluído pela Lei nº 9.983, de 2000) Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.(Incluído pela Lei nº 9.983, de 2000) Also, the reference to "third party's thing or electronic data" in connection with the crime of damage, in Section 163 of the Brazilian Criminal Law as amended by Article 4 of the Substitute Amendment, may possibly be interpreted as ultimately comprehending damages to computer systems. Finally, Articles 265 and 266 of the Brazilian Criminal Law have been amended

	by Article 7 of the Substitute Amendment so to make reference to the impairment of computer systems related to public services or to communication services. Article 266, as amended, is specific regarding system interference. Art. 265. To attack security or working of the services of water, electricity, energy, information or telecommunication, or any other public utility: Art. 266. To interrupt or disrupt telegraphic, radiotelegraphic, phone, telematic, or informatic service, or communication device, computer network, or computer or telecommunication system, or to impede or compromise its restore: Art. 265. Atentar contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação ou telecomunicação, ou qualquer outro de utilidade pública: Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico, telefônico, telemático, informático, de dispositivo de comunicação, de rede de computadores, de sistema informatizado ou de telecomunicação, assim como impedir ou dificultar-lhe o restabelecimento:
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	Provided for by Art. 154-A of the Brazilian Criminal Law, as incorporated by Art. 3 of the Substitute Amendment, contemplating the paragraph 1.a.ii of the latter (obs.: item 3 of Art. 3 of the Convention allows for the possibility of declaration regarding paragraph 1.a.i, reserving the right not to apply it). Art. 154-A. To communicate, use, commercialize, or make available data and information contained in computer system with finality other than the one which caused its input, except in the cases established by law or upon express concurrence by the person to which they refer, or by a legal representative of the latter: Penalty – imprisonment (detenção), from 1 (one) to 2 (two) years, and fine. Sole paragraph. If the perpetrator uses false name or identity of a third party for perpetrating the crime, the penalty is increased by one sixth.

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.	Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal: Pena - detenção, de 1 (um) a 2 (dois) anos, e multa. Parágrafo único. Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime, a pena é aumentada de sexta parte."
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.	Measures adopted to establish computer-related forgery as a criminal offence by the general provisions of the Criminal Code. Specific provisions in the Substitute Amendment were devised to address art. 7 of the Convention. It has been decided to include the penalty for the offences mentioned herein in the general provisions on offences of forgery (counterfeit another person's public or private documents, arts. 297 and 298 of the current Criminal Code). In its arts. 8 and 9, the Substitute Amendment has provided for special forgery offences, to amend arts. 297 and 298, of the Criminal Code. Art. 297. To falsify, in whole or in part, electronic data or public document, or modify truthful public document: Art. 298. To falsify, in whole or in part, electronic data or private document, or modify truthful private document: Art. 297. Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento público verdadeiro: Art. 298. Falsificar, no todo ou em parte, dado eletrônico ou documento

	particular ou alterar documento particular verdadeiro
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.	Measures adopted to establish computer-related fraud as a criminal offence by the general provisions of the Criminal Code. Specific provisions in the Substitute Amendment were devised to address art. 8 of the Convention. It has been decided to include the penalty for the offences mentioned herein in the general provisions on offences of fraud (larceny by fraud, art.171 of the current Criminal Code). Art. 171 (…): § 2º VIII – disseminates, in any media, malicious code with the purpose to facilitate or grant undue access to computer network, communication device or computer system. § 3º. If the perpetrator uses false name or the identity of a third party for perpetrating the crime set forth in item VII of paragraph 2, the penalty is increased by one sixth. Art. 171(...): § 2º Nas mesmas penas incorre quem: VII - difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado. § 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII do § 2º, a pena é aumentada de sexta parte." (NR)
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	Measures adopted in part. Art. 241 of Law n. 8069, of July 13th.,1990, as amended by Law n. 10764, of

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.	November 12th, 2003, punishes most of the offences typified as per art. 9 of the Convention (art. 241. - Cause the appearance, produce, sell, supply, expose or transmit by any means of communication whatever, including the world wide web or internet, pornographic photographs or images or scenes of explicit sexual activity involving children or adolescents. Provisions as per paragraph 1, d) and e) and as per paragraph 2, b) and c) of art. 9 of the Convention are hereby excluded. Further on, paragraph 4 provides for the right not to apply above paragraphs and sub-paragraphs. Art. 20 of the Substitute Amendement has amended Art. 241 of Law 8.069 so to include specific reference to storage of child pornography images: Art. 241. To present, produce, sell, receive, supply, communicate, publish or store with oneself, by any means of communication, including global computer network or Internet, pictures, images with pornography or scenes of explicit sex involving child or teenager: Art. 241. Apresentar, produzir, vender, receptar, fornecer, divulgar, publicar ou armazenar consigo, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias, imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
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	Measures adopted. Brazilian current legislation already addresses the protection implied in provisions as per art. 10: Law n. 9609 (February 19th, 1998 – Protection of Computer programs), Law n. 9610 (February 19th, 1998 – Protection of Copyrights), and Law n. 10695 (July 1st, 2003 – alters the Criminal Code to include offences related to infringements of copyrights – "Anti-Piracy" Act). The general provision in the Criminal Code has the following wording:

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.	Art. 184. To violate copyrights or connected rights: Penalty – Imprisonment (detenção), from 3 (three) months to 1 (one) year, and fine. Art. 184. Violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.
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.	General rule, set forth in the Brazilian Criminal Law: . Art. 349. To assist a perpetrator, beyond the hypothesis of co-autorship or of reception, to ensure the benefit of the crime Penalty – Imprisonment (detenção), from one (1) to six (6) months, and fine. Art. 349 - Prestar a criminoso, fora dos casos de co-autoria ou de receptação, auxílio destinado a tornar seguro o proveito do crime: Pena - detenção, de um a seis meses, e multa.

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.	The Brazilian criminal law does not address corporate liability unless in the case of offences against the environment. There are administrative and civil penalties for managers and for stockholders set forth in the Civil Code and in the Corporations Law.
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.	Measures adopted. The Brazilian Criminal Code and other criminal legislation provide for punishment with imprisonment together with or without fine.
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:	Measures adopted. Decree Law n. 3689, October 3rd., 1941 – Code of Penal Procedure (CPP), allows for preventive detention in certain situations. Article 19 of the Substitute Amendment amends Law 7.716 to the effect of suspension of electronic transmission of messages containing prejudice to color or race.

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	II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas, ou da publicação por qualquer meio.
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.	Measures adopted. 1998 Federal Constitution, Art. 5, Fundamental Rights and Guarantees. II – no one will be required to do or not to do anything except as required by law. II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;

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 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Measures adopted in part. Art. 22, Item II of the Substitute Amendment provides for expedited preservation of traffic data, user identification data and communications content.
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	Measures adopted. Art. 22, Items I and II of the Substitute Amendment provides for retention and expedited preservation of traffic data, user identification data and

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.	communications content. Art. 22 – The person in charge of providing commercial or governmental access to a global computer network, is required to: I – to maintain in a controlled and safe environment, for the period of 3 (three) years, with the purpose of assisting formal public investigation, the data of electronic address of origin, time, date and GMT reference of the connection made by means of a computer network, and to provide them exclusively to the investigation authority upon judicial order; II – to immediately preserve, upon judicial request, other information requested in the course of an investigation, being civil and criminally liable for its absolute confidentiality and inviolability; Art. 22. O responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público é obrigado a: I - manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial; II - preservar imediatamente, após requisição judicial, outras informações requisitadas em curso de investigação, respondendo civil e penalmente pela sua absoluta confidencialidade e inviolabilidade;
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.	Measures adopted. An injunction mechanism has been provided for under Art. 22, III, of the Substitute Amendment. III – to inform, in a secret manner, to the competent authority, denounce which has received and which contains signs of perpetration of a crime subject to public unconditioned action, which perpetration has taken place within a computer network under his responsibility. III - informar, de maneira sigilosa, à autoridade competente, denúncia que

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.	tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium;	No specific prevision of adoption. The Brazilian Criminal Procedure Code establishes general search and seizure provisions: **Art. 240 -** The search will be at domicile or in person: **§ 1º** The search will be at domicile where there is grounded reason, to: **II** – seizure things found or obtained through criminal means; **III** – seizure forgery or counterfeiting tools or objects; **Art. 240** - A busca será domiciliar ou pessoal. **§ 1º** - Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para: **b)** apreender coisas achadas ou obtidas por meios criminosos; **c)** apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos;

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.	
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal 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.	Measures adopted. Law n. 9296 (24/July/1996), art.1, sole paragraph, provides for the real-time collection of traffic data in computer or telematic systems; and art. 22 of the Substitute Amendment makes it compulsory for access providers to supply data capable of identifying users and connections when expressly authorized by judicial order during an investigation. Also, Art. 18 of the Substitute Amendment provides for structuring of Police forces dedicated to combating cybercrime: Art. 18. The agencies of the judicial Police shall structure, in accordance with regulation to be enacted, divisions and teams specialized in the combate to criminal actions in computer network, communication device or computer system. Art. 18. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Measures adopted. Law n. 9296 (24/July/1996), art.1, sole paragraph, provides for the real-time collection of traffic data in computer or telematic systems; and art. 22 of the Substitute Amendment makes it compulsory for access providers to supply data capable of identifying users and connections when expressly authorized by judicial order during an investigation **Same articles indicated for real time collection.**
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	For purposes of investigation and trial, and according to the body of Supreme Court case law, Brazilian Criminal Law takes into consideration the territory where the consequences of the offence were felt, the territory where the offence was committed being irrelevant. Art. 5. The Brazilian law applies, independently of treaties or conventions and rules of international law, to crimes perpetrated in the national territory.

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.	Paragraph 1. For criminal effects, it shall be deemed as national territory the Brazilian vessels and aircrafts, of public nature or to the service of the Brazilian government wherever they are, as well as merchant or private Brazilian aircrafts or vessels which are respectively in the corresponding air space or open sea. Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional. § 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty	**Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.** **Art. 784.** The rogatory letters issued by competent foreign authorities shall not dependo on homologation and shall be accepted if conveyed through diplomatic channels and provided that the crime, under the Brazilian laws, does not exclude extradition. **Art. 789.** The State Prosecutor-Attorney of the Brazilian Republic, whenever he is made aware of the existence of a foreign criminal Court decision, issued by a Country which hás a treaty on extradiction with Brazil and which has imposed personal security measures or accessory penalty which shall be enforced for obtaining elements which enable them to request homologation of the Court decision. **§ 1º** The homologation of a Court decision issued by the judicial authority of a Country which hás no treaty on extradiction with Brazil, shall depend on request to the Minister of Justice.

receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	**Art. 784** - As cartas rogatórias emanadas de autoridades estrangeiras competentes não dependem de homologação e serão atendidas se encaminhadas por via diplomática e desde que o crime, segundo a lei brasileira, não exclua a extradição. **Art. 789** - O procurador-geral da República, sempre que tiver conhecimento da existência de sentença penal estrangeira, emanada de Estado que tenha com o Brasil tratado de extradição e que haja imposto medida de segurança pessoal ou pena acessória que deva ser cumprida no Brasil, pedirá ao Ministro da Justiça providências para obtenção de elementos que o habilitem a requerer a homologação da sentença. **§ 1º** - A homologação de sentença emanada de autoridade judiciária de Estado, que não tiver tratado de extradição com o Brasil, dependerá de requisição do Ministro da Justiça.
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.	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.

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	Brazilian authorities have cooperated spontaneously with foreign authorities, by exchanging information. Art. 21 of the Substitute Agreement amends Art. 1 of Law 10.446 so to include cybercrimes among the areas subject to the competence of the Federal Police: V – the crimes perpetrated against or by means of computer network, communication device or computer system. V - os delitos praticados contra ou mediante rede de computadores, dispositivo

cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	de comunicação ou sistema informatizado.
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	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.

authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	

Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.

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	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.

involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application 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.	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.
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	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.

collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.
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.	Same as above. Art. 780 through 790 of the Brazilian Code of Penal Procedure address jurisdictional issues and relationship with foreign authorities.

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.	