

## Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

### Table of contents

Version 25 May 2020

[reference to the provisions of the Budapest Convention]

#### Chapter I – Use of terms

Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”

#### Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Article 2 – Illegal access

Article 3 – Illegal interception

Article 4 – Data interference

Article 5 – System interference

Article 6 – Misuse of devices

Article 7 – Computer-related forgery

Article 8 – Computer-related fraud

Article 9 – Offences related to child pornography

Article 10 – Offences related to infringements of copyright and related rights

Article 11 – Attempt and aiding or abetting

Article 12 – Corporate liability

Article 13 – Sanctions and measures

Section 2 – Procedural law

Article 14 – Scope of procedural provisions

Article 15 – Conditions and safeguards

Article 16 – Expedited preservation of stored computer data

Article 17 – Expedited preservation and partial disclosure of traffic data

Article 18 – Production order

Article 19 – Search and seizure of stored computer data

Article 20 – Real-time collection of traffic data

Article 21 – Interception of content data

Section 3 – Jurisdiction

Article 22 – Jurisdiction

#### Chapter III – International co-operation

Article 24 – Extradition

Article 25 – General principles relating to mutual assistance

Article 26 – Spontaneous information

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 28 – Confidentiality and limitation on use

Article 29 – Expedited preservation of stored computer data

Article 30 – Expedited disclosure of preserved traffic data

Article 31 – Mutual assistance regarding accessing of stored computer data

Article 32 – Trans-border access to stored computer data with consent or where publicly available

Article 33 – Mutual assistance in the real-time collection of traffic data

Article 34 – Mutual assistance regarding the interception of content data

Article 35 – 24/7 Network

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

<b>State:</b>	
<b>Signature of the Budapest Convention:</b>	N/A
<b>Ratification/accession:</b>	11/12/2019 (Observer)

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<b>Chapter I – Use of terms</b>	
<p><b>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”:</b></p> <p>For the purposes of this Convention:</p> <p>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;</p> <p>b “computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;</p> <p>c “service provider” means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>d “traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service</p>	
<b>Chapter II – Measures to be taken at the national level</b>	
<b>Section 1 – Substantive criminal law</b>	
<b>Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems</b>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p><b>Article 2 – Illegal access</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b>Código Penal</b></p> <p><b>Artigo 154-A</b></p> <p><b>Invasão de dispositivo informático</b></p> <p>Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:</p> <p>Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.</p> <p>§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no <i>caput</i>.</p> <p>§ 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.</p> <p>§ 3o Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:</p> <p>Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.</p> <p>§ 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.</p> <p>§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra:</p> <ul style="list-style-type: none"> <li>I - Presidente da República, governadores e prefeitos;</li> <li>II - Presidente do Supremo Tribunal Federal;</li> <li>III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou</li> <li>IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."</li> </ul> <p><b>Artigo 154-B</b></p> <p><b>Ação penal</b></p> <p>Nos crimes definidos no artigo 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p><b>Article 3 – Illegal interception</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b>Lei 9296/96</b></p> <p><b>Artigo 10</b></p> <p>Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:</p> <p>Pena – reclusão de 2 (dois) a 4 (quatro) anos, e multa.</p>
<p><b>Article 4 – Data interference</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.</p> <p>2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	
<p><b>Article 5 – System interference</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</p>	<p><b>Artigo 313-B</b></p> <p><b>Modificação ou alteração não autorizada de sistema de informações</b></p> <p>Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:</p> <p>Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.</p> <p>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.</p>
<p><b>Article 6 – Misuse of devices</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>a the production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;</p> <p>ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,</p> <p>with intent that it be used for the purpose of committing any of the offences</p>	<p><b>Código Penal</b></p> <p><b>Artigo 154-A</b></p> <p><b>Invasão de dispositivo informático</b></p> <p>Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:</p> <p>Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.</p> <p>§ 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no <i>caput</i>.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p> <p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p>	
Title 2 – Computer-related offences	
<p><b>Article 7 – Computer-related forgery</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p>	<p><b>Código Penal</b></p> <p><b>Artigo 297</b>  <b>Falsificação de documento público</b>  Falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro:  Pena - reclusão, de dois a seis anos, e multa.  § 1 - Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, aumenta-se a pena de sexta parte.  § 2 - Para os efeitos penais, equiparam-se a documento público o emanado de entidade paraestatal, o título ao portador ou transmissível por endosso, as ações de sociedade comercial, os livros mercantis e o testamento particular.</p> <p><b>Artigo 298</b>  <b>Falsificação de documento particular</b>  Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:  Pena - reclusão, de um a cinco anos, e multa.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p><b>Falsificação de cartão</b> Parágrafo único. Para fins do disposto no <i>caput</i>, equipara-se a documento particular o cartão de crédito ou débito.</p> <p><b>Artigo 313-A</b> <b>Inserção de dados falsos em sistema de informações</b> 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: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.</p>
<p><b>Article 8 – Computer-related fraud</b> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p> <ul style="list-style-type: none"> <li>a any input, alteration, deletion or suppression of computer data;</li> <li>b any interference with the functioning of a computer system,</li> </ul> <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p><b>Código Penal</b> <b>Artigo 171</b> <b>Estelionato</b> Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.</p> <p><b>Artigo 155</b> <b>Furto</b> Subtrair, para si ou para outrem, coisa alheia móvel: Pena - reclusão, de um a quatro anos, e multa. § 1 - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno. § 2 - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa. § 3 - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico. <b>Furto qualificado</b> § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido: I - com destruição ou rompimento de obstáculo à subtração da coisa; II - com abuso de confiança, ou mediante fraude, escalada ou destreza; III - com emprego de chave falsa; IV - mediante concurso de duas ou mais pessoas.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<b>Title 3 – Content-related offences</b>	
<p><b>Article 9 – Offences related to child pornography</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <ul style="list-style-type: none"> <li>a producing child pornography for the purpose of its distribution through a computer system;</li> <li>b offering or making available child pornography through a computer system;</li> <li>c distributing or transmitting child pornography through a computer system;</li> <li>d procuring child pornography through a computer system for oneself or for another person;</li> <li>e possessing child pornography in a computer system or on a computer-data storage medium.</li> </ul> <p>2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:</p> <ul style="list-style-type: none"> <li>a a minor engaged in sexually explicit conduct;</li> <li>b a person appearing to be a minor engaged in sexually explicit conduct;</li> <li>c realistic images representing a minor engaged in sexually explicit conduct</li> </ul> <p>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.</p> <p>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.</p>	<p><b>Estatuto da Criança e Adolescente</b></p> <p><b>Artigo 240</b></p> <p>Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:</p> <p>Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.</p> <p>§ 1 - Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no <i>caput</i> deste artigo, ou ainda quem com esses contracenar.</p> <p>§ 2 - Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:</p> <ul style="list-style-type: none"> <li>I – no exercício de cargo ou função pública ou a pretexto de exercê-la;</li> <li>II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou</li> <li>III – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.</li> </ul> <p><b>Artigo 241</b></p> <p>Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:</p> <p>Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.</p> <p><b>Artigo 241-A</b></p> <p>Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:</p> <p>Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.</p> <p>§ 1 - Nas mesmas penas incorre quem:</p> <ul style="list-style-type: none"> <li>I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o <i>caput</i> deste artigo;</li> <li>II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o <i>caput</i> deste artigo.</li> </ul>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p>§ 2 - As condutas tipificadas nos incisos I e II do § 1 deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o <i>caput</i> deste artigo.</p> <p><b>Artigo 241-B</b>          Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:          Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.</p> <p>§ 1 - A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o <i>caput</i> deste artigo.</p> <p>§ 2 - Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos artigos 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:</p> <ul style="list-style-type: none"> <li>I – agente público no exercício de suas funções;</li> <li>II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;</li> <li>III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.</li> </ul> <p>§ 3 - As pessoas referidas no § 2 deste artigo deverão manter sob sigilo o material ilícito referido.</p> <p><b>Artigo 241-C</b>          Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:          Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.          Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, pública ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do <i>caput</i> deste artigo.</p>



BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Title 4 – Offences related to infringements of copyright and related rights	
<p><b>Article 10 – Offences related to infringements of copyright and related rights</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.</p>	<p><b>Código Penal</b></p> <p><b>Artigo 184</b></p> <p>Violar direitos de autor e os que lhe são conexos:</p> <p>Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.</p> <p>§1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual, interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:</p> <p>Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.</p> <p><b>Lei 9609/98</b></p> <p><b>Artigo 2</b></p> <p>O regime de proteção à propriedade intelectual de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.</p> <p>§ 1 - Não se aplicam ao programa de computador as disposições relativas aos direitos morais, ressalvado, a qualquer tempo, o direito do autor de reivindicar a paternidade do programa de computador e o direito do autor de opor-se a alterações não-autorizadas, quando estas impliquem deformação, mutilação ou outra modificação do programa de computador, que prejudiquem a sua honra ou a sua reputação.</p> <p>§ 2 - Fica assegurada a tutela dos direitos relativos a programa de computador pelo prazo de cinquenta anos, contados a partir de 1 de janeiro do ano subsequente ao da sua publicação ou, na ausência desta, da sua criação.</p> <p>§ 3 - A proteção aos direitos de que trata esta Lei independe de registro.</p> <p>§ 4 - Os direitos atribuídos por esta Lei ficam assegurados aos estrangeiros domiciliados no exterior, desde que o país de origem do programa conceda, aos brasileiros e estrangeiros domiciliados no Brasil, direitos equivalentes.</p> <p>§ 5 - Inclui-se dentre os direitos assegurados por esta Lei e pela legislação de direitos autorais e conexos vigentes no País aquele direito exclusivo de autorizar ou proibir o aluguel comercial, não sendo esse direito exaurível pela venda, licença ou outra forma de transferência da cópia do programa.</p> <p>§ 6 - O disposto no parágrafo anterior não se aplica aos casos em que o programa em si não seja objeto essencial do aluguel.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Title 5 – Ancillary liability and sanctions	
<p><b>Article 11 – Attempt and aiding or abetting</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.</p> <p>3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.</p>	<p><b>Código Penal</b></p> <p><b>Artigo 14</b></p> <p>Diz-se o crime:</p> <p>Crime consumado</p> <p>I - (...)</p> <p>Tentativa</p> <p>II – tentado, quando iniciada a execução, não se consuma por circunstâncias alheias à vontade do agente.</p> <p>Pena de tentativa</p> <p>Parágrafo único – salvo disposição em contrário, pune-se a tentativa com a pena correspondente ao crime consumado, diminuída de um a dois terços.</p>
<p><b>Article 12 – Corporate liability</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:</p> <ul style="list-style-type: none"> <li>a a power of representation of the legal person;</li> <li>b an authority to take decisions on behalf of the legal person;</li> <li>c an authority to exercise control within the legal person.</li> </ul> <p>2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.</p> <p>3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.</p> <p>4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.</p>	
<p><b>Article 13 – Sanctions and measures</b></p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>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.</p> <p>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.</p>	
<b>Section 2 – Procedural law</b>	
<p><b>Article 14 – Scope of procedural provisions</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.</p> <p>2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <ul style="list-style-type: none"> <li>a the criminal offences established in accordance with Articles 2 through 11 of this Convention;</li> <li>b other criminal offences committed by means of a computer system; and</li> <li>c the collection of evidence in electronic form of a criminal offence.</li> </ul> <p>3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.</p> <p>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:</p> <ul style="list-style-type: none"> <li>i is being operated for the benefit of a closed group of users, and</li> </ul>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>ii does not employ public communications networks and is not connected with another computer system, whether public or private,</p> <p>that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21</p>	
<p><b>Article 15 – Conditions and safeguards</b></p> <p>1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.</p> <p>2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.</p> <p>3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.</p>	
<p><b>Article 16 – Expedited preservation of stored computer data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.</p>	<p><b>Lei nº 12.965/14 (Marco Civil da Internet)</b></p> <p><b>Artigo 13</b></p> <p>Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.</p> <p>(...)</p> <p><b>§2º</b> A autoridade policial ou administrativa ou o Ministério Público poderá</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.</p> <p><b>Artigo 15</b> O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (...)</p> <p><b>§2º</b> A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.</p>
<p><b>Article 17 – Expedited preservation and partial disclosure of traffic data</b></p> <p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <p>a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and</p> <p>b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Lei nº 12.965/14 (Marco Civil da Internet)</b></p> <p><b>Artigo 13</b> Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. (...)</p> <p><b>§2º</b> A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.</p> <p><b>Artigo 15</b> O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (...)</p> <p><b>§2º</b> A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p><b>Article 18 – Production order</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and</p> <p>b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:</p> <p>a the type of communication service used, the technical provisions taken thereto and the period of service;</p> <p>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;</p> <p>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.</p>	<p>prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.</p> <p><b>Lei nº 12.965/14 (Marco Civil da Internet)</b></p> <p><b>Artigo 11</b></p> <p>Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.</p> <p><b>§1º</b> O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.</p> <p><b>§2º</b> O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que ofereça serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.</p> <p><b>§3º</b> Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações</p> <p><b>Artigo 13</b></p> <p>Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento(...)</p> <p><b>§5º</b> Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.</p> <p><b>Artigo 15</b></p> <p>O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.</p> <p>(...)</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	<p><b>§3º</b> Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.</p>
<p><b>Article 19 – Search and seizure of stored computer data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <ul style="list-style-type: none"> <li>a a computer system or part of it and computer data stored therein; and</li> <li>b a computer-data storage medium in which computer data may be stored</li> </ul> <p style="padding-left: 40px;">in its territory.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:</p> <ul style="list-style-type: none"> <li>a seize or similarly secure a computer system or part of it or a computer-data storage medium;</li> <li>b make and retain a copy of those computer data;</li> <li>c maintain the integrity of the relevant stored computer data;</li> <li>d render inaccessible or remove those computer data in the accessed computer system.</li> </ul> <p>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.</p> <p>5 The powers and procedures referred to in this article shall be subject to</p>	<p><b>Código de Processo Penal</b></p> <p><b>Artigo 240</b></p> <p>A busca será domiciliar ou pessoal.</p> <p><b>§1º</b> Proceder-se á à busca domiciliar, quando fundadas razões a autorizarem, para:</p> <ul style="list-style-type: none"> <li>(...)</li> <li>e) descobrir objetos necessários à prova de infração ou à defesa do réu;</li> <li>(...)</li> <li>h) colher qualquer elemento de convicção.</li> </ul>



BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Articles 14 and 15.	
<p><b>Article 20 – Real-time collection of traffic data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <ul style="list-style-type: none"> <li>a collect or record through the application of technical means on the territory of that Party, and</li> <li>b compel a service provider, within its existing technical capability: <ul style="list-style-type: none"> <li>i to collect or record through the application of technical means on the territory of that Party; or</li> <li>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.</li> </ul> </li> </ul> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Lei 9296/96</b></p> <p><b>Art. 1º</b> A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob sigilo de justiça.</p> <p>Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.</p> <p><b>Art. 2º</b> Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:</p> <ul style="list-style-type: none"> <li>I - não houver indícios razoáveis da autoria ou participação em infração penal;</li> <li>II - a prova puder ser feita por outros meios disponíveis;</li> <li>III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.</li> </ul> <p>Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.</p> <p><b>Art. 3º</b> A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:</p> <ul style="list-style-type: none"> <li>I - da autoridade policial, na investigação criminal;</li> <li>II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.</li> </ul>
<p><b>Article 21 – Interception of content data</b></p> <p>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:</p> <ul style="list-style-type: none"> <li>a collect or record through the application of technical means on the territory of that Party, and</li> <li>b compel a service provider, within its existing technical capability: <ul style="list-style-type: none"> <li>ito collect or record through the application of technical means on</li> </ul> </li> </ul>	<p><b>Lei 9296/96</b></p> <p><b>Art. 1º</b> A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob sigilo de justiça.</p> <p>Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.</p> <p><b>Art. 2º</b> Não será admitida a interceptação de comunicações telefônicas quando</p>



BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>the territory of that Party, or</p> <p>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.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>ocorrer qualquer das seguintes hipóteses:</p> <p>I - não houver indícios razoáveis da autoria ou participação em infração penal;</p> <p>II - a prova puder ser feita por outros meios disponíveis;</p> <p>III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.</p> <p>Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.</p> <p><b>Art. 3º</b> A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:</p> <p>I - da autoridade policial, na investigação criminal;</p> <p>II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.</p>
<b>Section 3 – Jurisdiction</b>	
<p><b>Article 22 – Jurisdiction</b></p> <p>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:</p> <ul style="list-style-type: none"> <li>a in its territory; or</li> <li>b on board a ship flying the flag of that Party; or</li> <li>c on board an aircraft registered under the laws of that Party; or</li> <li>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.</li> </ul> <p>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.</p> <p>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</p>	<p><b>Código Penal</b></p> <p><b>Artigo 5º</b></p> <p>Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional</p> <p><b>§1º</b> - 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.</p> <p><b>§2º</b> - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em vôo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.</p> <p><b>Lugar do crime</b></p> <p><b>Art. 6º</b> - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>basis of his or her nationality, after a request for extradition.</p> <p>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>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.</p>	<p><b>Extraterritorialidade</b></p> <p><b>Art. 7º</b> - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:</p> <p>I - os crimes:</p> <p>a) contra a vida ou a liberdade do Presidente da República;</p> <p>b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;</p> <p>c) contra a administração pública, por quem está a seu serviço;</p> <p>d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil;</p> <p>II - os crimes:</p> <p>a) que, por tratado ou convenção, o Brasil se obrigou a reprimir;</p> <p>b) praticados por brasileiro;</p> <p>c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados.</p> <p><b>§1º</b> - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.</p> <p><b>§2º</b> - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições:</p> <p>a) entrar o agente no território nacional;</p> <p>b) ser o fato punível também no país em que foi praticado;</p> <p>c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição;</p> <p>d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;</p> <p>e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.</p> <p><b>§3º</b> - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior:</p> <p>a) não foi pedida ou foi negada a extradição;</p> <p>b) houve requisição do Ministro da Justiça.</p>
<b>Chapter III – International co-operation</b>	
<p><b>Article 24 – Extradition</b></p> <p>1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties</p>	<p><b>Lei 13.445/2017</b></p> <p><b>Artigo 81</b></p> <p>A extradição é a medida de cooperação internacional entre o Estado brasileiro e outro Estado pela qual se concede ou solicita a entrega de pessoa sobre quem</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.</p> <p>b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.</p> <p>2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.</p> <p>3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>	<p>recaia condenação criminal definitiva ou para fins de instrução de processo penal em curso.</p> <p><b>§1º</b> A extradição será requerida por via diplomática ou pelas autoridades centrais designadas para esse fim.</p> <p><b>§2º</b> A extradição e sua rotina de comunicação serão realizadas pelo órgão competente do Poder Executivo em coordenação com as autoridades judiciárias e policiais competentes.</p> <p><b>Artigo 82</b></p> <p>Não se concederá a extradição quando:</p> <p>I- o indivíduo cuja extradição é solicitada ao Brasil for brasileiro nato;</p> <p>II- o fato que motivar o pedido não for considerado crime no Brasil ou no Estado requerente;</p> <p>III- o Brasil for competente, segundo suas leis, para julgar o crime imputado ao extraditando;</p> <p>IV- a lei brasileira impuser ao crime pena de prisão inferior a 2 (dois) anos;</p> <p>V- o extraditando estiver respondendo a processo ou já houver sido condenado ou absolvido no Brasil pelo mesmo fato em que se fundar o pedido;</p> <p>VI- a punibilidade estiver extinta pela prescrição, segundo a lei brasileira ou a do Estado requerente;</p> <p>VII- o fato constituir crime político ou de opinião;</p> <p>VIII- o extraditando tiver de responder, no Estado requerente, perante tribunal ou juízo de exceção; ou</p> <p>IX- o extraditando for beneficiário de refúgio, nos termos da Lei nº 9.474, de 22 de julho de 1997, ou de asilo territorial.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>provisional arrest in the absence of a treaty.</p> <p>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</p>	
<p><b>Article 25 – General principles relating to mutual assistance</b></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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</p>	<p><b>Código de Processo Civil</b></p> <p><b>Artigo 26</b></p> <p>A cooperação jurídica internacional será regida por tratado de que o Brasil faz parte e observará:</p> <p>I – o respeito às garantias do devido processo legal no Estado requerente;</p> <p>II- a igualdade de tratamento entre nacionais e estrangeiros, residentes ou não no Brasil, em relação ao acesso à justiça e à tramitação dos processos, assegurando-se assistência judiciária aos necessitados;</p> <p>III - a publicidade processual, exceto nas hipóteses de sigilo previstas na legislação brasileira ou na do Estado requerente;</p> <p>IV -a existência de autoridade central para recepção e transmissão dos pedidos de cooperação;</p> <p>V – a espontaneidade na transmissão de informações a autoridades estrangeiras.</p> <p><b>§1º</b> Na ausência de tratado, a cooperação jurídica internaional poderá realizar-se com base em reciprocidade, manifestada por via diplomática.</p> <p><b>§2º</b> Não se exigirá a reciprocidade referida no §1º para homologação de sentença estrangeira.</p> <p><b>§3º</b> Na cooperação jurídica internacional não será admitida a prática de atos que contrariem ou que produzam resultados incompatíveis com as normas fundamentais que regem o Estado brasileiro.</p> <p><b>§4º</b> O Ministério da Justiça exercerá as funções de autoridade central na ausência de designação específica.</p>

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
<p><b>Article 26 – Spontaneous information</b></p> <p>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.</p> <p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	<p><b>Código de Processo Civil</b></p> <p><b>Artigo 26</b></p> <p>A cooperação jurídica internacional será regida por tratado de que o Brasil faz parte e observará:</p> <p>I – o respeito às garantias do devido processo legal no Estado requerente;</p> <p>II- a igualdade de tratamento entre nacionais e estrangeiros, residentes ou não no Brasil, em relação ao acesso à justiça e à tramitação dos processos, assegurando-se assistência judiciária aos necessitados;</p> <p>III - a publicidade processual, exceto nas hipóteses de sigilo previstas na legislação brasileira ou na do Estado requerente;</p> <p>IV -a existência de autoridade central para recepção e transmissão dos pedidos de cooperação;</p> <p>V – a espontaneidade na transmissão de informações a autoridades estrangeiras.</p> <p><b>§1º</b> Na ausência de tratado, a cooperação jurídica internaional poderá realizar-se com base em reciprocidade, manifestada por via diplomática.</p> <p><b>§2º</b> Não se exigirá a reciprocidade referida no §1º para homologação de sentença estrangeira.</p> <p><b>§3º</b> Na cooperação jurídica internacional não será admitida a prática de atos que contrariem ou que produzam resultados incompatíveis com as normas fundamentais que regem o Estado brasileiro.</p> <p><b>§4º</b> O Ministério da Justiça exercerá as funções de autoridade central na ausência de designação específica.</p>
<p><b>Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements</b></p> <p>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.</p> <p>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</p>	

**BUDAPEST CONVENTION****DOMESTIC LEGISLATION**

for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>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.</p> <p>b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).</p> <p>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.</p> <p>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.</p> <p>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.</p>	
<p><b>Article 28 – Confidentiality and limitation on use</b></p> <p>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.</p> <p>2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:</p> <p>a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or</p> <p>b not used for investigations or proceedings other than those stated in the request.</p> <p>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</p>	



BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>the requesting Party accepts the condition, it shall be bound by it.</p> <p>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.</p>	
<p><b>Article 29 – Expedited preservation of stored computer data</b></p> <p>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.</p> <p>2 A request for preservation made under paragraph 1 shall specify:</p> <ul style="list-style-type: none"> <li>a the authority seeking the preservation;</li> <li>b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;</li> <li>c the stored computer data to be preserved and its relationship to the offence;</li> <li>d any available information identifying the custodian of the stored computer data or the location of the computer system;</li> <li>e the necessity of the preservation; and</li> <li>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.</li> </ul> <p>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.</p> <p>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.</p> <p>5 In addition, a request for preservation may only be refused if:</p>	



BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p> <p>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.</p> <p>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.</p>	
<p><b>Article 30 – Expedited disclosure of preserved traffic data</b></p> <p>1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.</p> <p>2 Disclosure of traffic data under paragraph 1 may only be withheld if:</p> <p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	
<p><b>Article 31 – Mutual assistance regarding accessing of stored computer data</b></p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p>been preserved pursuant to Article 29.</p> <p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <ul style="list-style-type: none"> <li>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</li> <li>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</li> </ul>	
<p><b>Article 32 – Trans-border access to stored computer data with consent or where publicly available</b></p> <p>A Party may, without the authorisation of another Party:</p> <ul style="list-style-type: none"> <li>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</li> <li>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.</li> </ul>	
<p><b>Article 33 – Mutual assistance in the real-time collection of traffic data</b></p> <p>1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.</p>	
<p><b>Article 34 – Mutual assistance regarding the interception of content data</b></p> <p>The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.</p>	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
<p><b>Article 35 – 24/7 Network</b></p> <p>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:</p> <ul style="list-style-type: none"> <li>a the provision of technical advice;</li> <li>b the preservation of data pursuant to Articles 29 and 30;</li> <li>c the collection of evidence, the provision of legal information, and locating of suspects.</li> </ul> <p>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.</p> <p>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.</p> <p>3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	
<p><b>Article 42 – Reservations</b></p> <p>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.</p>	