

Sao Tome and Principe

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version [12.07.2020]

[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.

State:	
Signature of the Budapest Convention:	No
Ratification/accession:	No

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	Lei n.º 15/2017 Artigo 2.º Definições Para efeitos da presente Lei, considera-se: a) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção; b) «Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função; c) «Dados de tráfego», os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente; d) «Fornecedor de serviço», qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respetivos utilizadores;

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(...)
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.	Lei n.º 15/2017 Artigo 7.º Acesso ilegítimo 1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias. 2. Na mesma pena incorre quem ilegítimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. 3. A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança. 4. A pena é de prisão de 1 a 5 anos quando: a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado. 5. A tentativa é punível, salvo nos casos previstos no n.º 2. 6. Nos casos previstos nos n.os 1, 3 e 5 o procedimento penal depende de queixa.
Article 3 – Illegal interception	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Lei n.º 15/2017 Artigo 8.º Interceção ilegítima 1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa. 2. A tentativa é punível. 3. Incorre na mesma pena prevista no n.º 1 quem ilegítimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número.
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.	Lei n.º 15/2017 Artigo 5.º Dano relativo a programas ou outros dados informáticos 1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa. 2. A tentativa é punível. 3. Incorre na mesma pena do n.º 1 quem ilegítimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número. 4. Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 300 dias. 5. Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	6. Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa.
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	Lei n.º 15/2017 Artigo 6.º Sabotagem informática 1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 300 dias. 2. Na mesma pena incorre quem ilegítimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. 3. Nos casos previstos no número anterior, a tentativa não é punível. 4. A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado. 5. A pena é de prisão de 1 a 10 anos se: a) O dano emergente da perturbação for de valor consideravelmente elevado; b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	Lei n.º 15/2017 Artigo 4.º Falsidade informática (...) 4. Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos. 5. Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos. Artigo 5.º Dano relativo a programas ou outros dados informáticos (...) 3. Incorre na mesma pena do n.º 1 quem ilegítimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número. (...) Artigo 6.º Sabotagem informática (...) 2. Na mesma pena incorre quem ilegítimamente produzir, vender, distribuir

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. (...) Artigo 7.º Acesso ilegítimo (...) 2. Na mesma pena incorre quem ilegítimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior. (...)
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.	Lei n.º 15/2017 Artigo 4.º Falsidade informática 1. Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 10 a 300 dias. 2. Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão. 3. Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente. 4. Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos. 5. Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.
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.	Código Penal ARTIGO 240.º Burla informática e nas comunicações 1. Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa até 300 dias. 2. A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações. 3. A tentativa é punível. 4. o procedimento criminal depende de queixa. 5. se o prejuízo for: a) superior a 40 vezes do índice cem do vencimento da Função Pública, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 300 dias; b) superior a 80 vezes do índice cem do vencimento da Função Pública, o agente é punido com pena de prisão de 1 a 8 anos. 6. É correspondentemente aplicável o disposto no artigo 226º.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: - a producing child pornography for the purpose of its distribution through a computer system; - b offering or making available child pornography through a computer system; - c distributing or transmitting child pornography through a computer 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.	Código Penal ARTIGO 180.º Pornografia de menores 1. Quem: a) Produzir, distribuir, importar, exportar, divulgar, exhibir ou ceder, a qualquer título ou por qualquer meio, fotografia, filme ou gravação de carácter pornográfico representando um menor de 14 anos, independentemente do seu suporte; b) Detiver materiais previstos na alínea anterior com o propósito de os distribuir, importar, exportar, divulgar, exhibir ou ceder; é punido com pena de prisão até 5 anos. 2. Quem praticar os actos descritos no número anterior relativamente a menor entre 14 e 18 anos é punido com pena de prisão até 3 anos. 3. Quem praticar os actos descritos no n.º 1 utilizando material pornográfico simulado ou manipulado de menor de 18 anos, não existente é punido com pena de prisão até 2 anos. 4. Quem praticar os actos descritos no n.º1 utilizando material pornográfico com representação realista de menor de 18 anos é punido com pena de prisão de 2 a 8 anos. 5. Quem praticar os actos descritos no n.º 2 com intenção lucrativa é punido com pena de prisão de 1 a 5 anos. 6. Quem adquirir ou detiver os materiais previstos na alínea a) do n.º 1 e no n.º 2 é punido com pena de prisão até 1 ano ou com pena de multa até 100 dias. 7. A tentativa é punível.
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	Lei n.º 15/2017 Artigo 9.º Reprodução ilegítima de programa protegido 1. Quem ilegítimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	2. Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semiconductor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semiconductor fabricado a partir dessa topografia. 3. A tentativa é punível.
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.	Código Penal ARTIGO 22.º Tentativa 1. Há tentativa quando o agente pratica actos de execução de um crime que decidiu cometer, sem que este chegue a consumir-se. 2. são actos de execução: a) os que preenchem um elemento constitutivo de um tipo de crime; b) os que são idóneos a produzir o resultado típico; c) os que, segundo a experiência comum e salvo circunstâncias imprevisíveis, são de natureza a fazer esperar que se lhes sigam actos das espécies indicadas nas alíneas anteriores. ARTIGO 23.º Punibilidade da tentativa 1. Salvo disposição em contrário, a tentativa só é punível se ao crime consumado respectivo corresponder pena superior a 3 anos de prisão.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2. A tentativa é punível com a pena aplicável ao crime consumado, especialmente atenuada. 3. A tentativa não é punível quando for manifesta a inaptidão do meio empregado pelo agente ou a inexistência do objecto essencial à consumação do crime.
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.	Código Penal Artigo 11.º Responsabilidade penal das pessoas colectivas e entidades equiparadas As pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente Lei nos termos e limites do regime de responsabilização previsto no Código Penal.
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	
Article 14 – Scope of procedural provisions	Lei n.º 15/2017

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: - a the criminal offences established in accordance with Articles 2 through 11 of this Convention; - b other criminal offences committed by means of a computer system; and - c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: - i is being operated for the benefit of a closed group of users, and - ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	Artigo 14.º Âmbito de aplicação das disposições Processuais 1. Com excepção do disposto nos artigos 21.º e 22.º, as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes: a) Previstos na presente Lei; b) Cometidos por meio de um sistema informático; ou c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico. 2. As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 3/2016, de 10 de Maio, Lei de Protecção de Dados Pessoais.
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	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <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. 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.	Lei n.º 15/2017 Artigo 15.º Preservação expedita de dados 1. Se no decurso do processo for necessário a produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa. 2. A preservação pode também ser ordenada pelo órgão de polícia judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no n.º 6. 3. A ordem de preservação discrimina, sob pena de nulidade: a) A natureza dos dados; b) A sua origem e destino, se forem conhecidos; e

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	c) O período de tempo pelo qual devem ser preservados, até um máximo de três meses. 4. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual. 5. A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 3, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano. 6. Em cumprimento das diligências previstas no n.º 2, os órgãos de polícia criminal que procederem a diligências referidas nos artigos anteriores elaboram um relatório onde mencionam, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas. 7. O relatório é remetido ao Ministério Público ou ao juiz de instrução conforme os casos.
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party’s competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Lei n.º 15/2017 Artigo 16.º Revelação expedita de dados de tráfego Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior, indica à autoridade judiciária ou ao órgão de polícia judiciária, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person’s possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider’s possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term “subscriber information” means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber’s identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	Lei n.º 15/2017 Artigo 17.º Injunção para apresentação ou concessão do acesso a dados 1. Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência. 2. A ordem referida no número anterior identifica os dados em causa. 3. Em cumprimento da ordem descrita nos n.os 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados. 4. O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar: a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	5. A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo. 6. Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista. 7. O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 253.º do Código de Processo Penal é aplicável com as necessárias adaptações.
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; - 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.	Lei n.º 15/2017 Artigo 18.º Pesquisa de dados informáticos 1. Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência. 2. O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade. 3. O órgão de polícia judiciária pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando: a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado; b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa. 4. Quando o órgão de polícia judiciária proceder à pesquisa nos termos do número anterior:

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	a) No caso previsto na alínea b) do número anterior, a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação; b) Os órgãos de polícia judiciária que procederem a diligências referidas nos termos da presente Lei, elaboram um relatório onde mencionam, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas, que deve ser remetido ao Ministério Público ou ao juiz de instrução, conforme os casos. 5. Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.ºs 1 e 2. 6. À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista. Artigo 19.º Apreensão de dados informáticos 1. Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos. 2. O órgão de polícia judiciária pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora. 3. Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	nulidade esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto. 4. As apreensões efectuadas por órgão de polícia judiciária são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas. 5. As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia, das actividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas nos n.ºs 6 e 7 do artigo 15.º e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista. O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 253.º do Código de Processo Penal é aplicável com as necessárias adaptações. 6. A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes: a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura; b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou d) Eliminação não reversível ou bloqueio do acesso aos dados. 7. No caso da apreensão efectuada nos termos da alínea b) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital. Artigo 20.º

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Apreensão de correio electrónico e registos de comunicações de natureza semelhante Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutra a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.
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. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	Lei n.º 15/2017 Artigo 21.º Intercepção de comunicações 1. É admissível o recurso à intercepção de comunicações em processos relativos a crimes: a) Previstos na presente Lei; ou b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 258.º do Código de Processo Penal. 2. A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público. 3. A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação. 4. Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 258.º, 259.º e 260.º do Código de Processo Penal. Lei n.º 15/2017 Artigo 21.º Intercepção de comunicações 1. É admissível o recurso à intercepção de comunicações em processos relativos a crimes: c) Previstos na presente Lei; ou d) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 258.º do Código de Processo Penal. 5. A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público. 6. A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação. 7. Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 258.º, 259.º e 260.º do Código de Processo Penal.
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:	Código Penal ARTIGO 4.º Aplicação no espaço: princípio geral

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	Salvo tratado ou convenção internacional em contrário, a lei penal da república Democrática de são Tomé e Príncipe é aplicável: a) A factos praticados em território da república Democrática de são Tomé e Príncipe, seja qual for a nacionalidade do agente; b) A factos praticados a bordo de navios ou aeronaves são-tomenses. ARTIGO 5.º Factos praticados fora do território nacional 1. A lei penal da república Democrática de são Tomé e Príncipe é ainda aplicável, salvo tratado ou convenção em contrário: a) A factos praticados fora do território nacional quando constituam os crimes previstos nos artigos 240.º, 292.º, 304.º a 315.º, 359.º, 360.º, 367.º a 385.º e 389.º a 414.º; b) A factos praticados fora do território nacional, desde que o agente seja encontrado dentro da república Democrática de são Tomé e Príncipe e não possa ser extraditado, quando constituam os crimes previstos nos artigos 159.º a 164.º, 172.º, 175.º, 176.º, 179.º, 180.º, 207.º a 211.º, 213.º, 214.º e 216.º; c) A factos praticados fora do território nacional por são-tomenses ou por estrangeiros contra são-tomenses, sempre que: i) os agentes sejam encontrados na república Democrática de são Tomé e Príncipe; ii) sejam também puníveis pela legislação do lugar em que foram praticados, salvo quando nesse lugar não se exerça poder punitivo; iii) constituam crime que admite extradição e esta não possa ser concedida; d) Aos factos cometidos fora do território nacional contra são-tomenses, por são-tomenses que vivam habitualmente na república Democrática de são Tomé e Príncipe ao tempo da sua prática e nele sejam encontrados. e) A factos por pessoa colectiva, ou contra esta, que tenha sede em território de são Tomé e Príncipe. 2. A lei penal são-tomense é ainda aplicável a quaisquer factos cometidos fora do território nacional de que o estado são-tomense se tenha obrigado a julgar por tratado ou convenção internacional ARTIGO 6.º Restrições à aplicação da lei são-tomense

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	1. A aplicação da lei penal são-tomense a factos praticados fora do território nacional só tem lugar quando o agente não tenha sido julgado no País da prática do facto ou se haja subtraído ao cumprimento total ou parcial da condenação. 2. embora seja aplicável a lei são-tomense, nos termos do número anterior, o facto é julgado segundo a lei do país em que foi praticado sempre que esta seja concretamente mais favorável ao agente. A pena aplicável é convertida naquela que corresponder no sistema são-tomense, ou, não havendo correspondência directa, naquela que a lei são-tomense prevê para o facto. 3. o regime do número anterior não se aplica aos crimes previstos na alínea a) do n.º 1 do artigo 5.º. Lei n.º 15/2017 Artigo 30.º Aplicação no espaço da lei penal são-tomense e a competência dos tribunais nacionais 1. Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal são-tomense, e salvo tratado ou convenção internacional em contrário, para efeitos da presente Lei, a lei penal são-tomense é ainda aplicável a factos: a) Praticados por são-tomenses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado; b) Cometidos em benefício de pessoas colectivas com sede em território são-tomense; c) Fisicamente praticados em território são-tomense, ainda que visem sistemas informáticos localizados fora desse território; ou d) Que visem sistemas informáticos localizados em território são-tomense, independentemente do local onde esses factos forem fisicamente praticados. 2. Se, em função da aplicabilidade da Lei penal são-tomense, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente Lei, os tribunais são-tomense e os tribunais de outro Estado com o qual aquele tenha acordo ou tratado ou convenção, pode em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos, a autoridade judiciária competente recorre aos órgãos e

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	mecanismos instituídos para facilitar a cooperação entre as autoridades judiciárias dos Estados e a coordenação das respectivas acções, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infracção, tendo em vista centralizá-lo num só deles. 3. A decisão de aceitação ou transmissão do procedimento é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos: a) O local onde foi praticada a infracção; b) A nacionalidade do autor dos factos; e c) O local onde o autor dos factos foi encontrado. 4. São aplicáveis aos crimes previstos na presente Lei as regras gerais de competência dos tribunais previstas no Código de Processo Penal. 5. Em caso de dúvida quanto ao tribunal territorialmente competente, designadamente por não coincidirem o local onde fisicamente o agente actuou e o local onde está fisicamente instalado o sistema informático visado com a sua actuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos.
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	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal	Lei n.º 15/2017 Artigo 23.º

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	Âmbito da cooperação internacional As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 3/2016, de 10 de Maio, Lei de Protecção de Dados Pessoais.
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	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or	Lei n.º 15/2017 Artigo 23.º Âmbito da cooperação internacional As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 3/2016, de 10 de Maio, Lei de Protecção de Dados Pessoais.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b it considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence;	Lei n.º 15/2017 Artigo 25.º Preservação e revelação expeditas de dados Informáticos em cooperação internacional 1. Pode ser solicitada a República Democrática de São Tomé e Príncipe a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 15.º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos. 2. A solicitação específica:

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> 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.	a) A autoridade que pede a preservação; b) A infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados; c) Os dados informáticos a conservar e a sua relação com a infracção; d) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático; e) A necessidade da medida de preservação; e f) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados. 3. Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve. 4. A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no n.º 4 do artigo anterior. 5. A ordem de preservação específica, sob pena de nulidade: a) A natureza dos dados; b) Se forem conhecidos, a origem e o destino dos mesmos; e c) O período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses. 6. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	7. A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 5, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano. 8. Quando seja apresentado o pedido de auxílio referido no n.º 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adopção de uma decisão final sobre o pedido. 9. Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos: a) À autoridade judiciária competente, em execução do pedido de auxílio referido no n.º 1, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo dos artigos 17.º a 21.º; b) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo do artigo 15.º 10. A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efectuada, comunica-os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos. 11. O disposto nos n.ºs 1 e 2 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades são-tomenses.
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if:	Lei n.º 15/2017 Artigo 25.º Preservação e revelação expeditas de dados Informáticos em cooperação internacional 3. Pode ser solicitada a República Democrática de São Tomé e Príncipe a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 15.º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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, <i>ordre public</i> or other essential interests.	4. A solicitação específica: g) A autoridade que pede a preservação; h) A infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados; i) Os dados informáticos a conservar e a sua relação com a infracção; j) Todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático; k) A necessidade da medida de preservação; e l) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos dados. 6. Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que os preserve. 7. A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no n.º 4 do artigo anterior. 8. A ordem de preservação específica, sob pena de nulidade: d) A natureza dos dados; e) Se forem conhecidos, a origem e o destino dos mesmos; e f) O período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses. 10. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade. 11. A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 5, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano. 12. Quando seja apresentado o pedido de auxílio referido no n.º 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adopção de uma decisão final sobre o pedido. 13. Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos: c) À autoridade judiciária competente, em execução do pedido de auxílio referido no n.º 1, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo dos artigos 17.º a 21.º; d) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo do artigo 15.º 12. A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efectuada, comunica-os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos. 13. O disposto nos n.ºs 1 e 2 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades são-tomenses.
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.	Lei n.º 15/2017 Artigo 27.º Acesso a dados informáticos em cooperação internacional 1. Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	localizado na República Democrática de São Tomé e Príncipe, relativos a crimes previstos no artigo 12.º, quando se trata de situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante. 2. A autoridade judiciária competente procede com a maior rapidez possível quando existam razões para crer que os dados informáticos em causa são especialmente vulneráveis à perda ou modificação ou quando a cooperação rápida se encontre prevista em instrumento internacional aplicável. 3. O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias São-tomense.
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.	Lei n.º 15/2017 Artigo 28.º Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento 1. As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades são-tomenses, de acordo com as normas sobre transferência de dados pessoais previstas na Lei de Protecção de Dados Pessoais, podem: a) Aceder a dados informáticos armazenados em sistema informático localizado na República Democrática de São Tomé e Príncipe, quando publicamente disponíveis; b) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em São Tomé e Príncipe, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los.
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	Lei n.º 15/2017 Artigo 29.º Intercepção de comunicações em cooperação internacional 1. Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado na República Democrática de São Tomé e Príncipe, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	intercepção seja admissível, nos termos do artigo 20.º, em caso nacional semelhante. 2. É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresenta ao Ministério Público, para que os apresente ao juiz de instrução criminal para autorização. 3. O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido. 4. O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias nacionais.
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.	Lei n.º 15/2017 Artigo 29.º Intercepção de comunicações em cooperação internacional 1. Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado na República Democrática de São Tomé e Príncipe, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos do artigo 20.º, em caso nacional semelhante. 2. É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresenta ao Ministério Público, para que os apresente ao juiz de instrução criminal para autorização. 3. O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido. 4. O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias nacionais.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Lei n.º 15/2017 Artigo 24.º Ponto de contacto permanente para a cooperação internacional 1. Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana. 2. Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que São Tomé e Príncipe se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciais ou policiais. 3. A assistência imediata prestada por este ponto de contacto permanente inclui: a) A prestação de aconselhamento técnico a outros pontos de contacto; b) A preservação expedita de dados nos casos de urgência ou perigo na demora, em conformidade com o disposto no artigo seguinte; c) A recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora; d) A localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora; e) A transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas nas alíneas b) a d), fora dos casos aí previstos, tendo em vista a sua rápida execução. 4. Sempre que actue ao abrigo das alíneas b) a d) do número anterior, a Polícia judiciária dá notícia imediata do facto ao Ministério Público e remetelhe o relatório previsto no artigo 18.º.
Article 42 – Reservations	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	