Angola

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version [03.08.2020]

[reference to the provisions of the Budapest Convention]

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.

COUNCIL OF EUROPE
CONSEIL DE L'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	***Draft Penal Code*** ***Article 439 b, c, e and j*** b) «Dados de tráfego», os dados informáticos relacionados com uma comunicação efectuada 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 trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente; c) «Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função; e) «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 respectivos utilizadores; j) «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, protecção e manutenção;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Draft Penal Code ***Article 252 d and e*** d) "Dado" é qualquer representação de factos informações ou conceitos, incluindo programas de computador, que é armazenada, transmitida ou processada num sistema de informação; e) "Sistema de informação" é qualquer dispositivo ou conjunto de dispositivos, bem como a rede que suporta a comunicação entre eles, que, de forma separada ou conjunta armazena, trata, transmite, recebe ou recupera dados, que inclui mas não se limita a sistemas informáticos, de comunicações electrónicas, de radiodifusão e telemáticos.
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.	***Draft Penal Code*** ***illegal access*** ***Article 440*** Artigo 440.º (Acesso ilegítimo a sistema de informação e devassa através de sistema de informação) 1- Quem, sem autorização, aceder à totalidade ou a parte de um sistema de informação, de que não for titular, é punido com a pena de prisão até 2 anos ou com a de multa até 240 dias. 2- Se o acesso for conseguido através da violação das regras de segurança ou se tiver sido efectuado a um serviço protegido, a pena é de 2 a 8 anos de prisão. 3- A mesma pena é aplicável sempre que, no caso descrito no n.º 1, o agente: a) Tomar conhecimento de segredo comercial ou industrial ou de dados confidenciais protegidos por lei; b) Obtiver benefício ou vantagem patrimonial de valor elevado, conforme este é definido na alínea b) do artigo 393.º.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	4- É punido com pena do n.º 1, quem, sem estar devidamente autorizado: a) Proceder a tratamento informático de dados ou informações individualmente identificáveis; b) Transmitir a terceiros, para fins diferentes dos autorizados, dados ou informações informaticamente tratados; c) Criar, manter ou utilizar ficheiro informático de dados pessoalmente identificáveis relativos a convicções políticas, religiosas ou filosóficas, a filiação partidária ou sindical ou à vida privada de outrem. 5- A tentativa é sempre punível. 6- Para os efeitos do n.º 2, serviço protegido significa qualquer serviço de radiodifusão ou da sociedade da informação, desde que prestado mediante remuneração e com acesso condicional, conforme este é descrito no artigo 252.º.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	***Draft Penal Code*** ***illegal interception*** ***Article 441*** Artigo 441.º (Intercepção ilegítima em sistema de informação) 1- Quem, através de meios técnicos, interceptar ou registar transmissões não públicas de dados que se processem no interior de um sistema de informação, conforme este é definido no artigo 252.º a ele destinados ou dele provenientes, é punido com a pena de prisão até 2 anos ou com a de multa até 240 dias. 2- A mesma pena é aplicável a quem abrir mensagem de correio electrónico que não lhe seja dirigida ou tomar conhecimento do seu conteúdo ou, por qualquer modo, impedir que seja recebida pelo seu destinatário. 3- A mesma pena é aplicável a quem divulgar o conteúdo das comunicações referidas nos números anteriores. 4- Se a intercepção for conseguida através da violação das regras de segurança ou for efectuada a partir de um serviço legalmente protegido, a pena é de 2 a 8 anos de prisão. 5- A tentativa é sempre punível.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	***Draft Penal Code*** ***computer damage (or data interference)*** ***Article 442*** Artigo 442.º (Dano em dados informáticos) 1- Quem, com intenção de causar prejuízo a terceiro ou de obter benefício para si ou para terceiro, alterar, deteriorar, inutilizar, apagar, suprimir, ou destruir, no todo ou em parte, ou, de qualquer forma, tornar não acessíveis dados alheios, conforme os define o artigo 252.º ou lhes afectar a capacidade de uso, é punido com a pena de prisão até 2 anos ou com a de multa até 240 dias. 2- A mesma pena é aplicável a quem, com intenção de causar prejuízo a terceiro ou de obter benefício para si ou para terceiro, destruir, total ou parcialmente, inutilizar, apagar, alterar, danificar, embaraçar, impedir, interromper, perturbar gravemente o funcionamento ou afectar a capacidade de uso de um sistema de informação, conforme é definido no artigo 252.º. 3- Em cada um dos casos descritos nos números anteriores, a pena é de: a) De prisão de 6 meses a 3 anos ou de multa de 60 a 360 dias, se o prejuízo for elevado; b) De prisão de 2 a 5 anos, se o valor do prejuízo for consideravelmente elevado; c) De prisão de 3 a 8 anos, se a perturbação ou dano causados atingirem de forma grave e duradoura um sistema de informação que apoie actividades destinadas a assegurar o abastecimento de bens ou a prestação serviços essenciais, nomeadamente de saúde, fornecimento de água e electricidade, transportes e comunicações. 4- Se o dano causado não for relevante, nos termos do artigo 412.º, não há lugar à qualificação. 5- A tentativa é sempre punível.
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	***Draft Penal Code*** ***computer sabotage (or system interference)*** ***Article 443*** Artigo 443.º (Sabotagem informática) 1- É punido com pena de prisão até 2 anos ou multa até 240 dias quem, de modo ilícito:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	a) Alterar, danificar, interromper, destruir, parte ou todo de uma rede de comunicações electrónicas ou sistema informáticos; b) Perturbar gravemente o funcionamento de uma rede de comunicações electrónicas, e sistemas informáticos ; c) Afectar a capacidade de uso, através da introdução, transmissão, danificação, alteração, e impedimento do acesso ou supressão de dados informáticos ou através de qualquer outra forma de interferência na rede de comunicações electrónicas e sistema informáticos, 2- Se o dano emergente da perturbação for de valor elevado, o agente é punido com a pena de prisão de 2 a 5 anos. 3- Se o dano emergente da perturbação for de valor consideravelmente elevado, ou atingir de forma grave ou duradoura uma rede de comunicações electrónica, e sistemas informáticos que apoiem uma actividade destinada a assegurar funções sociais essenciais, o agente é punido com a pena é de prisão de 2 a 8 anos.
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	Not covered

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	
Article 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.	***Draft Penal Code*** ***computer forgery*** ***Article 444*** Artigo 444.º (Falsidade informática) 1- Quem, com intenção de enganar, introduzir, alterar, eliminar ou suprimir dados em sistema de informação ou, em geral, interferir no tratamento desses dados, por forma a dar origem a dados falsos que possam ser considerados verdadeiros e utilizados como meio de prova, é punido com a pena de prisão até 2 anos ou com a de multa até 240 dias. 2- Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações electrónicas ou a serviço de acesso condicionado, a pena é de 2 a 5 anos de prisão. 3- As penas estabelecidas nos n.ºs 1 e 2 são aplicáveis a quem, não sendo o autor dos crimes descritos nesses números, utilizar, com a intenção de causar prejuízo a outrem ou de obter benefício para si ou para terceiro, respectivamente, os dados falsos referidos no n.º 1 ou o cartão ou dispositivo em que se encontrem registados ou incorporados os dados obtidos com os factos descritos no n.º 2. 4- Se o autor dos factos descritos nos números anteriores for funcionário público no exercício das suas funções, a pena é de: a) Prisão de 6 meses a 3 anos ou multa de 60 a 360 dias, no caso do n.º 1; b) 4 a 10 anos no caso dos n.ºs 2 e 3.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	***Draft Penal Code*** ***computer fraud*** ***Article 445*** Artigo 445.º (Burla informática e nas comunicações) É punido com as penas estabelecidas para o crime de furto qualificado no n.º 3 do artigo 395.º, atendendo ao valor do prejuízo material causado quem, com o propósito de obter para si ou para terceiros vantagem patrimonial pelas formas descritas, causar a outrem prejuízos de natureza patrimonial: a) Interferir no resultado de tratamento de dados, conforme definido no artigo 252.º, mediante estruturação incorrecta de programa de computador, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização, ou mediante intervenção, por qualquer outro modo não autorizado, no processamento; b) Usar programas, dispositivos ou outros meios que, separada ou conjuntamente, se destinem a diminuir, alterar ou impedir, no todo ou em parte, o normal funcionamento ou exploração do serviço de telecomunicações.
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.	***Draft Penal Code*** ***child pornography*** ***Article 200*** Artigo 200.º (Pornografia infantil) 1- É punido com pena de prisão de 1 a 5 anos, quem: a) Promover, facilitar ou permitir que menor de 18 anos participe de leitura obscena, conversa, assista a espectáculo, projecção de filmes, audição de gravações, exposição de fotografias ou observe ou examine instrumentos pornográficos; b) Utilizar menor de 18 anos em fotografia, filme ou gravação pornográfica, independentemente do seu suporte ou o aliciar para esse fim; c) Ceder a menor de 18 anos escritos, fotografias, filmes, gravações ou instrumentos de natureza pornográfica,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	2- É punido com pena de prisão de 2 a 10 anos, quem: a) Produzir pornografia infantil para ser difundida através de sistema de informação; b) Oferecer, disponibilizar, difundir ou transmitir pornografia infantil através de um sistema de informação, 3- Quem adquirir, detiver, acordar ou facilitar o acesso a material pornográfico infantil por qualquer meio é punido com pena de prisão de 1 a 5 anos. 4- Se o agente fizer profissão dos actos descritos nos números anteriores ou os praticar com fim lucrativo, a pena é de prisão de 3 a 10 anos. 5- Para os efeitos do n.º 2, entende-se por: a) "Pornografia infantil" qualquer material pornográfico que represente, de forma visual ou sonora, menor de 18 anos ou pessoa, real ou virtual, aparentando ser menor de 18 anos, envolvidos em comportamentos sexualmente explícitos ou que incitem à prática desses comportamentos. b) "Sistema de informação" o definido na alínea e) do artigo 252.º.
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions,	***Draft Penal Code*** ***copyright infringement on computer programs*** ***Article 446*** Artigo 446.º (Reprodução ilegítima de programa de computador, bases de dados e topografia de produtos semicondutores) 1- Quem ilegitimamente reproduzir, distribuir, comunicar ao público ou colocar à disposição do público um programa de computador protegido por lei é punido com pena de prisão até 2 anos ou multa até 240 dias. 2- Quem, não estando para tanto autorizado, reproduzir, distribuir, comunicar ao público ou colocar à disposição do público, com fins comerciais, uma base de dados criativa, é punido com pena de prisão até 3 anos ou pena de multa até 360 dias. 3- Quem, não estando para tanto autorizado, proceder à extracção ou reutilização de uma base de dados protegida por lei é punido com uma pena de prisão até 2 anos ou pena de multa de 240 dias.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	4- A pena do número 2 é aplicável a quem ilegitimamente reproduzir, distribuir, divulgar ou colocar à disposição do público uma topografia de um produto semicondutor. 5- Em caso de reprodução não autorizada, são apreendidas as cópias ilícitas de programas de computador, bases de dados ou topografia de produtos semicondutores, podendo igualmente ser apreendidos dispositivos em comercialização que tenham por finalidade exclusiva facilitar a supressão não autorizada ou a neutralização de qualquer salvaguarda técnica eventualmente colocada para protecção destes.
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.	***Draft Penal Code*** ***Attempt*** ***Articles 20 and 21*** Artigo 20.º (Tentativa) 1- Há tentativa quando o agente praticar, com dolo, actos de execução de um crime, sem que este chegue a consumar-se. 2- São actos de execução: a) Os que preencherem um elemento constitutivo de um tipo de crime; b) Os que forem idóneos à produção do resultado típico; c) Os que, segundo a experiência comum e salvo circunstâncias imprevisíveis, forem de natureza a fazer esperar que se lhe sigam actos das espécies indicadas nas alíneas anteriores. Artigo 21.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. 2- A tentativa é punível com a pena aplicável ao crime consumado, especialmente atenuada. 3- A tentativa não é punível quando for manifesta: a) A ineptidão do meio empregado pelo agente; b) A inexistência do objecto essencial à consumação do crime.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Aiding ***Article 25*** Artigo 25.º (Cumplicidade) 1- É punível como cúmplice quem, fora dos casos previstos no artigo anterior, prestar, directa e dolosamente, auxílio material ou moral à prática por outrem de um facto doloso. 2- É aplicável ao cúmplice a pena fixada para o autor, especialmente atenuada.
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.	***Draft Penal Code*** ***Article 9*** Artigo 9.º (Responsabilidade penal das pessoas colectivas) 1- As pessoas colectivas, com excepção do Estado e das organizações internacionais de direito público, são susceptíveis de responsabilidade criminal. 2- As pessoas colectivas e entidades equiparadas, ainda que irregularmente constituidas, são responsáveis pelas infracções cometidas em seu nome, por sua conta e no seu interesse, ou em seu benefício, a título individual ou no desempenho de funções, pelos seus órgãos, representantes, ou por pessoas que nela detenham uma posição de liderança. 3- Os entes colectivos referidos no n.º 2 são ainda responsáveis por crimes cometido em seu nome, por sua conta e no seu interesse, ou em seu benefício, por pessoas singulares que actuem sob a autoridade das pessoas referidas no número anterior, sempre que o crime se tenha tornado possível em virtude de uma violação dolosa dos deveres de vigilância ou controlo que às últimas incumbem. 4- Quando a lei determinar a responsabilização de entes colectivos como tais, deve entender-se que se trata de pessoas colectivas ou de meras associações de facto. 5- A responsabilidade penal das pessoas colectivas e entidades equiparadas não exclui a responsabilidade individual dos respectivos agentes nem depende da responsabilização destes. 6- A responsabilidade penal das pessoas colectivas e entidades equiparadas é excluída quando o agente tiver actuado contra ordens ou instruções expressas da entidade competente para o efeito.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	7- A transmissão, cisão e a fusão não determinam a extinção da responsabilidade penal das pessoas colectivas, respondendo pela prática do crime: a) A pessoa colectiva ou entidade equiparada em que a transmissão ou fusão se tiver efectivado; b) As pessoas colectivas ou entidades equiparadas que resultaram da cisão. 8- Se as multas ou indemnizações forem aplicadas a uma entidade sem personalidade jurídica, responde por elas o património comum e, na sua falta ou insuficiência, solidariamente, o património de cada um dos respectivos membros, sócios, associados ou integrantes.
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	***Constitution of the Republic of Angola 2010*** ***Access to courts and effective judicial protection of the citizens*** ***Article 29*** Artigo 29.º (Acesso ao direito e tutela jurisdicional efectiva) 1. A todos é assegurado o acesso ao direito e aos tribunais para defesa dos seus direitos e interesses legalmente protegidos, não podendo a justiça ser denegada por insuficiência dos meios económicos. 2. Todos têm direito, nos termos da lei, à informação e consulta jurídicas, ao patrocínio judiciário e a fazer-se acompanhar por advogado perante qualquer autoridade. 3. A lei define e assegura a adequada protecção do segredo de justiça. 4. Todos têm direito a que uma causa em que intervenham seja objecto de decisão em prazo razoável e mediante processo equitativo. 5. Para defesa dos direitos, liberdades e garantias pessoais, a lei assegura aos cidadãos procedimentos judiciais caracterizados pela celeridade e prioridade, de modo a obter tutela efectiva e em tempo útil contra ameaças ou violações desses direitos.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Respect for privacy ***Article 32*** Artigo 32.º (Direito à identidade, à privacidade e à intimidade) 1. A todos são reconhecidos os direitos à identidade pessoal, à capacidade civil, à nacionalidade, ao bom nome e reputação, à imagem, à palavra e à reserva de intimidade da vida privada e familiar. 2. A lei estabelece as garantias efectivas contra a obtenção e a utilização, abusivas ou contrárias à dignidade humana, de informações relativas às pessoas e às famílias. ***Secrecy of communications*** ***Article 34*** Artigo 34.º (Inviolabilidade da correspondência e das comunicações) 1. É inviolável o sigilo da correspondência e dos demais meios de comunicação privada, nomeadamente das comunicações postais, telegráficas, telefónicas e telemáticas. 2. Apenas por decisão de autoridade judicial competente proferida nos termos da lei, é permitida a ingerência das autoridades públicas na correspondência e nos demais meios de comunicação privada.
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	***Law no. 7/2017 of 16 February 2017*** ***Expedited preservation of data*** ***Article 20*** Artigo 20. (Conservação expedita de dados) 1. Os responsáveis pelo tratamento dos dados específicos armazenados numa rede de comunicações electrónicas e sistemas da sociedade da informação, inluindo os dados de tráfego, ficam obrigados a asegurar a confidencialidade e devem ordenar a conservação expedita de dados, sob pena de nulidade.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	2. Os dados referidos no número anterior devem ser preservados até 6 (seis) meses. 3. O responsável pelo tratamento dos dados debe pôr em práctica as medidas técnicas e organizativas adequadas para proteger od dados informáticos contra a destruição, acidental ou ilicita, a perda acidental, a alteração, a difusão ou o acceso nao autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede e contra qualquer outra forma de tratamento ilícito.
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.	***Law no. 7/2017 of 16 February 2017*** ***Expedited preservation and disclosure of traffic data*** ***Article 21.*** Artigo 21 (Conservação expedita de dados de tráfego e de localização) Ao operador de comunicacoes electrónicas do ciberespaço acessível ao público ou prestador de serviços da sociedade da informação, a quem a preservação dos dados de tráfego e de localização, relativos à uma determinada comunicação que tenha sido ordenada à conservação, nos termos da legislação processual penal, debe indicar as otras entidades que nela participem, permitindo a indetificação das mesmas.
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	
Article 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;	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	***Draft Penal Procedure Code*** ***Article 247 extends the regime of telephonic interceptions to the interception of other communications, including telematic communications*** ***Artigo 247.º*** (Extensão do regime) O disposto no presente capítulo é correspondentemente aplicável às comunicações transmitidas à distância através de qualquer outro meio técnico análogo, designadamente, correio electrónico ou outras formas de transmissão de dados por via telemática, ainda que estes se encontrem guardadas em suporte digital, assim como à gravação de conversas ou comunicações entre pessoas presentes.

Back to the Table of Contents

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.	***Draft Penal Procedure Code*** ***Article 247 extends the regime of telephonic interceptions to the interception of other communications, including telematic communications*** ***Artigo 247.º*** (Extensão do regime) O disposto no presente capítulo é correspondentemente aplicável às comunicações transmitidas à distância através de qualquer outro meio técnico análogo, designadamente, correio electrónico ou outras formas de transmissão de dados por via telemática, ainda que estes se encontrem guardadas em suporte digital, assim como à gravação de conversas ou comunicações entre pessoas presentes.
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	***Law 13/2015*** ***Article 1*** ***International judicial cooperation in criminal matters, respecting extradition, transmission of criminal proceedings, execution of criminal sentences, transfer of sentenced persons, surveillance of convicted or conditionally released persons and other mutual legal assistance measures in criminal matters.*** ***A particular focus is put on cybercrime, according to Article 1, g.*** Artigo 1.º

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(Objecto) 1- A presente lei regula as formas de cooperação judiciária internacional em matéria penal, nomeadamente: a) Extradição; b) Transmissão de processos penais; c) Execução de sentenças penais; d) Transferência de pessoas condenadas a penas ou medidas de segurança privativas da liberdade; e) Vigilância de pessoas condenadas ou libertadas condicionalmente; f) Auxílio judiciário mútuo em matéria penal; g) Cooperação no âmbito do cibercrime. 2- O disposto no número anterior aplica-se, com as devidas adaptações, à cooperação da República de Angola com as entidades judiciárias internacionais estabelecidas no âmbito de tratados ou convenções que vinculem o Estado Angolano. 3- A presente lei é subsidiariamente aplicável à cooperação em matéria de infracções de natureza penal, na fase em que tramitem perante autoridades administrativas, bem como de infracções que constituam ilícito transgressional, cujos processos admitam recurso judicial.
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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; 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.	**Law 13/2015** **Articles 169 to 172** **Expedited preservation of data** Artigo 169.º (Solicitação de dados informáticos) 1- Pode ser solicitada à República de Angola a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes informáticos, ou cometidos através de meios informáticos, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos. 2- A solicitação deve especificar: 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	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. Artigo 170.º (Preservação expedita de dados informáticos) 1- 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. 2- A preservação pode também ser ordenada pelo Serviço de Investigação Criminal 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 168.º. 3- A ordem de preservação deve especificar, 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) 3 meses. 4- 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. 5- A autoridade judiciária competente, ou o Serviço de Investigação Criminal mediante autorização daquela autoridade, 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- Quando seja apresentado o pedido de auxílio referido no n.º 1 do artigo anterior, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à adopção de uma decisão final sobre o pedido. 7- 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 do artigo anterior, nos mesmos termos em que

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	poderiam sê-lo, em caso nacional semelhante, nos termos definidos por lei própria; b) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo da legislação competente. Artigo 171.º (Comunicação de dados de tráfego) 1- 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. 2- O disposto nos nºs 1 e 2 do artigo 166.º aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades angolanas. Artigo 172.º (Motivos de recusa) 1- A solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando: a) Os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do Direito angolano; b) Atentar contra a soberania, segurança, ordem pública ou otros interesses da República Angolana, constitucionalmente definidos; c) O Estado terceiro requisitante não oferecer garantias adequadas de protecção dos dados pessoais. 2- A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver razões fundadas para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	***Law 13/2015*** ***Article 173*** ***Access to data stored in Angola*** Artigo 173.º (Acesso a dados informáticos) 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 localizado na República de Angola, relativos a crimes informáticos ou cometidos através de sistemas informáticos, 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. O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias angolanas.
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	***Law 13/2015*** ***Article 174*** ***Access to data stored in Angola without authorisation of the Angolan authorities*** Artigo 174.º

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	(Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento) As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades angolanas, de acordo com as normas sobre transferência de dados previstas na Lei n.º 22/11, de 17 de Junho – Da Protecção de Dados Pessoais, podem: a) Aceder a dados informáticos armazenados em sistema informático localizado na República de Angola, quando publicamente disponíveis; b) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Angola, 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.	***Law 13/2015*** ***Article 162 and Article 175*** ***Interception of communications on international cooperation*** Artigo 162.º (Intercepção de telecomunicações) 1- Pode ser autorizada a intercepção de telecomunicações realizadas em Angola, a pedido das autoridades competentes de Estado estrangeiro, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seria admissível, nos termos da lei de processo penal, em caso nacional semelhante. 2- São competentes para a recepção dos pedidos de intercepção os órgãos de polícia criminal, que os apresentam ao magistrado do Ministério Público titular na respectiva Comarca, para autorização. 3- O despacho referido no número anterior inclui autorização para 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. Artigo 175.º (Intercepção de comunicações)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	1- Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo magistrado do Ministério Público a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado na República de Angola, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos previstos em lei própria, em caso nacional semelhante.
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.	***Law 13/2015*** ***Article 162 and Article 175*** ***Interception of communications on international cooperation*** (Intercepção de telecomunicações) 1- Pode ser autorizada a intercepção de telecomunicações realizadas em Angola, a pedido das autoridades competentes de Estado estrangeiro, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seria admissível, nos termos da lei de processo penal, em caso nacional semelhante. 2- São competentes para a recepção dos pedidos de intercepção os órgãos de polícia criminal, que os apresentam ao magistrado do Ministério Público titular na respectiva Comarca, para autorização. 3- O despacho referido no número anterior inclui autorização para 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. Artigo 175.º (Intercepção de comunicações) 1- Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo magistrado do Ministério Público a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado na República de Angola, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos previstos em lei própria, em caso nacional semelhante.
Article 35 – 24/7 Network	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	***Law 13/2015*** ***Article 168*** ***Permanent contact point for the purposes of international cooperation on cybercrime and digital evidence*** Artigo 168.º (Ponto de contacto permanente) 1- Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, o Serviço de Investigação Criminal 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 solicitado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que a República de Angola se encontre vinculada, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários 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 urgencia 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.
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents