Angola

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version [12 August 2022]

[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	**Lei n.º 38/20 Código Penal Angolano** (Angola's Penal Code/ CPA, 11 November 2020) LIVRO II Parte Especial, TÍTULO III Crimes Contra a Fé Pública, CAPÍTULO I Falsificação de Documentos e Registos Técnicos, ARTIGO 250.º (Definições) Para efeitos do presente capítulo: a) «Documento» é todo o suporte material ou técnico, nomeadamente, papel, disco, fita gravada, banda magnética ou outro meio de natureza similar que incorpore declaração feita por uma pessoa e possua idoneidade para provar um facto juridicamente relevante e, ainda, o sinal, com relevância jurídica e eficácia probatória, gravado ou aposto numa coisa para indicar a sua origem, natureza b) ou qualidade; c) «Registo Técnico» é o registo, com eficácia probatória, de um valor, peso ou medida de um estado ou do decurso de um acontecimento, feito por intermédio de um aparelho técnico que, actuando, no todo ou em parte, de forma automática, permite obter resultados referidos a factos juridicamente relevantes: d) «Acesso Condicionado» é a sujeição do acesso a um serviço através de uma assinatura ou qualquer outra forma de autorização prévia individual; e) «Dado» é qualquer representação de factos informações ou conceitos, incluindo programas de computador, que é armazenada, transmitida ou processada num sistema de informação; f) «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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	TÍTULO VIII Crimes Informáticos, CAPÍTULO I, Disposições Gerais, ARTIGO 437.º (Definições) Para efeitos do presente título, considera-se: a) «Código de Acesso», dado ou senha que permite aceder no todo ou em parte e sob forma inteligível, a um sistema de informação; 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; d) «Dispositivo», qualquer equipamento, material electromagnético, acústico, mecânico, técnico ou outro ou programa de computador; 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; f) «Intercepção», o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos, técnicos ou outros; g) «Produto semicondutor», a forma final ou intermedia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica; h) «Programa de Computador» o conjunto de instruções (software) usado directa ou indirectamente num computador, tendo em vista a obtenção de determinado resultado, incluindo o material de concepção; i) «Rede de Comunicações Electrónicas», sistemas de transmissão e, se for o caso, os equipamentos de comutação ou encaminhamento e os demais recursos que permitem o envio de sinais por cabo, meios radioeléctricos,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo internet) e móveis, os sistemas de cabos de electricidade, na medida em que sejam, utilizados para a transmissão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida; 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; k) «Topografia», uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respective fabrico. **Regulamento Geral das Comunicações Electrónicas** (General Regulation of Electronic Communications, 25 May 2016) TITULO I Disposições Gerais, ARTIGO 5.º (Definições) v) «Dispositivo ilicito», um equipamento ou programa informatico concebido ou adaptado com vista a permitir o acesso ou a visualização de um serviço protegido, sob forma inteligivel, sem autorização do prestador do serviço; w) «Serviço protegido», qualquer conteudo audiovisual, prestado mediante remuneração e com base em acesso condicional. **Lei nº. 7/17 Protecção das Redes e Sistemas Informáticos** (Law no. 7/17 Law for the Protection of IT Systems) CAPÍTULO I, Disposições Gerais, ARTIGO 4 (Definições) Para efeitos de presente Lei, considera-se: g) «Cibercrime» – O crime cometido com o recurso aos sistemas electronicos e as novas technologicas de informação e comunicação;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	l) «Dados» – Qualquer representação de factos, videos ou imagens, informacoes ou conceitos, incluindo de programas de computador, que sao armazenados, transmitidos ou processandos num sistema de informação; m) «Dados de base pessoais» – Os dados que permitem identificar uma pessoa, como seja o nome, idade, morada, telephone e endereço de correio electronico; n) «Dados de localização» – Quaisquer dados tratados num system de informação que indiquem a posição geografica do equipamento terminal ou de um utilizador de um servico prestado atraves de um systema de informação; o) «Dados de tráfego» – Qualquer dado tratado para efeitos do envoi de uma comunicação, atraves de um sistema de informação ou para efeitos de facturação daquela, incluido os dados que indicam a origem, destino, trajecto, hora, data, tamanho e duração da comunicação, ou o tipo de servico subjacente; q) «Dispositivo» – Qualquer equipamento, material electromagnetico, acustico, mecanico, tecnico ou outros ou programa de computador; x) «Intercepção de Comunicação» – O acto destinado a captar dados contidos ou transmitidos atraves de um system de informação mediante o recurso a dispositivos; aa) «Prestador de serviço» – Qualquer pessoa, singular ou colectiva, publica ou privada, que faculte aos utilizadores dos seus servicos a possibilidade de comunicar por meio de um systema de informação, bem como qualquer outra entidade que trate ou armazene dados em nome e por conta daquela ou dos respectivos utilizadores, incluindo, mas nao se limitando, a operadores de comunicaçoes electronicas e prestadores de servicos da sociedade da informação; bb) «Programa de computador» – O conjunto de instruçoes (software) usado directa ou indirectamente num computador, tendo em vista a obtenção de determinado resultado, incluido o material de concepção; ee) «Roubo informatico» – Qualquer apropriacao indevida de uma rede, Sistema informatico, bases de dados, equipamento informatico, programa informatico, usando a violencia, ameaca, acesso ilegitimo com vista a estruturacao incorrecta de programa ou sistmea informatico;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	hh) «Sistema de Informação» – Qualquer dispositivo ou conjunto de dispositivos, bem como a rede que suporta a comunicação entre eles, que, de forma separada ou conjunta, armazenam, tratam, transmitem, recebem ou recuperam dados; ii) «Sistema Informático» – Qualquer dispositivo ou conjunto de dispositivos que procedem ao armazenamento, tratamento, recuperação, ou transmissão de dados informáticos em execução de um programa de computador;
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.	**CPA** (11 November 2020) LIVRO II Parte Especial, TÍTULO VIII Crimes Informáticos, CAPÍTULO II Crimes Contra os Dados Informáticos, ARTIGO 438.º (Acesso ilegítimo a sistema de informação e devassa através de sistema de informação) 1. Quem, sem autorização, aceder à totalidade ou à 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 391.º 4. É punido com pena do n.º 1 quem, sem estar devidamente autorizado: a) Proceder ao 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	d) 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 condicionado, conforme este é descrito na alínea c) do artigo 250.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.	**CPA** (11 November 2020) LIVRO II Parte Especial, TÍTULO VIII Crimes Informáticos, CAPÍTULO II Crimes Contra os Dados Informáticos, ARTIGO 439.º (Intercepção ilegítima em sistema de informação) 1. Quem, através de meios técnicos, interceptar ou registrar transmissões não públicas de dados que se processem no interior de um sistema de informação, conforme este é definido na alínea e) do artigo 250.º a ele destinados ou dele proveniente, 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.
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.	**CPA** (11 November 2020) LIVRO II Parte Especial, TÍTULO VIII Crimes Informáticos, CAPÍTULO II Crimes Contra os Dados Informáticos, ARTIGO 440.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 a alínea d) do artigo 250.º ou lhes afectar a capacidade de uso, é punido com as penas previstas nos artigos 392.º e 393.º em razão do valor do prejuízo causado.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 na alínea e) do artigo 250.º 3. Nos casos descritos nos números anteriores, as penas previstas são agravadas em um terço, nos seus limites mínimo e máximo, se a perturbação ou dano causado atingirem de forma grave e duradoura um sistema de informação que apoie actividades destinadas a assegurar o abastecimento de bens ou a prestação de serviços essenciais, de transporte, de comunicações, de saneamento básico ou gestão de resíduos, ou de protecção contra forças da natureza. 4. Se o dano causado não for relevante, nos termos do n.º 2 do artigo 410.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	**CPA** (11 November 2020) LIVRO II Parte Especial, TÍTULO VIII Crimes Informáticos, CAPÍTULO III Crimes Contra as Comunicações e Sistemas Informáticos, ARTIGO 441.º (Sabotagem informática) 1. É punido com pena de prisão até 2 anos ou multa até 240 dias quem, de modo ilícito: 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	**Regulamento Geral das Comunicações Electrónicas** (General Regulation of

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Electronic Communications, 25 May 2016) TITULO II Oferta de Redes e Serviços de Comunicaçãoes Eletrônicas, CAPITULO IV Exploração, SECÇÃO VI Conteúdos Audiovisuais, ARTIGO 64.º (Dispositivos ilicitos) São proibidas as seguintes actividades: a) Fabrico, importação, distribuição, venda, locação ou detenção, para fins comerciais, de dispositivos ilicitos; b) Instalação, manutenção ou substituição, para fins comerciais, de dispositivos ilicitos; c) Utilização de publicidade para a promoção de dispositivos ilicitos; d) Aquisição, utilização, propriedade ou mera detenção, a qualquer titulo, de dispositivos ilicitos para fins privados do adquirente, do utilizador, do proprietário ou do detentor, bem como de terceiro.
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,	**CPA** (11 November 2020) LIVRO II Parte Especial, TÍTULO VIII Crimes Informáticos, CAPÍTULO III Crimes Contra as Comunicações e Sistemas Informáticos, ARTIGO 442.º (Falsidade informática)

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	1. Quem, com intenção de enganar ou prejudicar, 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.
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.	**CPA** (11 November 2020) LIVRO II Parte Especial, TÍTULO VIII Crimes Informáticos, CAPÍTULO III Crimes Contra as Comunicações e Sistemas Informáticos, ARTIGO 443.º (Burla informática e nas comunicações) É punido com as penas estabelecidas para o crime de furto qualificado no n.º 3 do artigo 393.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 na alínea d) do artigo 250.º, mediante estruturação incorrecta de programa de computador, utilização incorrecta ou incomplete 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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. 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.	**CPA** (11 November 2020) LIVRO II Parte Especial, TÍTULO I Crimes Contra as Pessoas, CAPÍTULO IV Crimes Sexuais, SECÇÃO III, Crimes Contra a Autodeterminação Sexual, ARTIGO 198.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. 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 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 250.º SECÇÃO IV Disposições Comuns, ARTIGO 199.º (Agravação)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	1. As penas previstas nos artigos 182.º a 184.º e 187.º a 198.º são agravadas em um terço nos seus limites mínimo e máximo, se a vítima for: a) Ascendente ou descendente, adoptante ou adoptado, parente ou afim até ao terceiro grau da linha colateral do agente ou se encontrar sob sua tutela ou curatela; b) Se encontrar numa relação de dependência hierárquica, económica ou de trabalho do agente e o crime for praticado com aproveitamento dessa relação. 2. As penas previstas nos artigos 182.º a 187.º, 192.º a 194.º e 197.º são agravadas de um quarto nos seus limites mínimos e máximos, sempre que o agente seja portador de doença sexualmente transmissível susceptível de criar perigo para a vida da vítima. 3. As penas previstas nos artigos 182.º a 187.º são agravadas de um quarto nos seus limites mínimos e máximos quando a vítima for idosa, nos termos da lei. 4. As penas previstas nos artigos 182.º a 188.º e 198.º são agravadas de metade nos seus limites mínimos e máximos quando a vítima for menor de 14. 5. As penas estabelecidas para os crimes referidos no número anterior e no artigo 197.º, são agravadas de metade nos seus limites mínimos e máximo, sempre que dos comportamentos comportamentos neles descritos resultar gravidez, suicídio ou morte da vítima, ofensa grave à sua integridade física ou transmissão de doença incurável portadora de perigo para a vida da vítima. 6. As penas descritas nos artigos 182.º a 188.º, 192.º e 194.º são agravadas de dois terços nos seus limites mínimos e máximos, sempre que a vítima seja menor de 14 anos e, simultaneamente, dos comportamentos neles descritos resultar gravidez, suicídio ou morte da vítima, ofensa grave à sua integridade física ou transmissão de doença incurável portadora de perigo para a vida da vítima. 7. Se no mesmo comportamento concorrerem mais do que uma das circunstâncias referidas nos números anteriores, só é considerada para efeito de determinação da pena aplicável a que tiver um efeito agravante mais forte, sendo as demais valoradas na medida da pena. ARTIGO 201.º (Pena acessória) Quando o agente for condenado pelos crimes previstos no presente capítulo, pode ser inibido, atenta a gravidade do facto e a sua conexão com a função por ele exercida, do exercício da autoridade paternal, da tutela ou da curatela por um período de 3 a 15 anos.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**Constituição Da República De Angola (Constitution, 2010)** CAPÍTULO II DIREITOS, LIBERDADES E GARANTIAS FUNDAMENTAIS, SECÇÃO I DIREITOS E LIBERDADES INDIVIDUAIS E COLECTIVAS, Artigo 42.º (Propriedade intelectual) 1. É livre a expressão da actividade intelectual, artística, política, científica e de comunicação, independentemente de censura ou licença. 2. Aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar. 3. São assegurados, nos termos da lei: a) A protecção às participações individuais em obras colectivas e à reprodução da imagem e voz humanas, incluindo nas actividades culturais, educacionais, políticas e desportivas; b) O direito aos criadores, aos intérpretes e às respectivas representações sindicais e associativas de fiscalização do aproveitamento económico das obras que criem ou de que participem. 4. A lei assegura aos autores de inventos industriais, patentes de invenções e processos tecnológicos o privilégio temporário para a sua utilização, bem como a protecção às criações industriais, à propriedade das marcas, aos nomes de empresas e a outros signos distintivos, tendo em vista o interesse social e o desenvolvimento tecnológico e económico do País. **Lei n.º 15/14, dos Direitos de Autor e Conexos** (Law No. 15/14, on Copyright and Related Rights, 31 July 2014) **CPA** (11 November 2020) LIVRO II Parte Especial, TÍTULO VIII Crimes Informáticos, CAPÍTULO III Crimes Contra as Comunicações e Sistemas Informáticos, ARTIGO 444.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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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. 4. A pena do n.º 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
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.	**CPA** (11 November 2020) LIVRO I Parte Geral, TÍTULO II Facto Punível, CAPÍTULO II Formas Especiais do Facto Punível, 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. ARTIGO 25.º (Cumplicidade)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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.	**CPA** (11 November 2020) LIVRO I Parte Geral, TÍTULO II Facto Punível, CAPÍTULO I Pressupostos da Punição, 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 equiparadas, ainda que irregularmente constituídas, 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. As pessoas colectivas referidas no número anterior são ainda responsáveis por crimes cometidos 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 pessoas colectivas enquanto tais, deve entender-se que se trata de pessoas colectivas ou de meras associações de facto. 5. A responsabilidade penal das pessoas colectivas e equiparadas não exclui a responsabilidade individual dos respectivos agentes nem depende da responsabilização destes. 6. A responsabilidade penal das pessoas colectivas e equiparadas é excluída quando o agente tiver actuado contra ordens ou instruções expressas da entidade competente para o efeito. 7. A transmissão, a cisão e a fusão não determinam a extinção da responsabilidade penal das pessoas colectivas, respondendo pela prática do crime: a) A pessoa colectiva ou equiparada em que a transmissão ou a fusão tiver sido efectivada; b) As pessoas colectivas ou 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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Constituição Da República De Angola (Constitution, 2010)** TÍTULO II DIREITOS E DEVERES FUNDAMENTAIS, CAPÍTULO I PRINCÍPIOS GERAIS, 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. CAPÍTULO II DIREITOS, LIBERDADES E GARANTIAS FUNDAMENTAIS, SECÇÃO I DIREITOS E LIBERDADES INDIVIDUAIS E COLECTIVAS, 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. Artigo 34.º (Inviolabilidade da correspondência e das comunicações) 1. É inviolável o sigilo da correspondência e dos demais meios de comunicação

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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. Artigo 40.º (Liberdade de expressão e de informação) 1. Todos têm o direito de exprimir, divulgar e compartilhar livremente os seus pensamentos, as suas ideias e opiniões, pela palavra, imagem ou qualquer outro meio, bem como o direito e a liberdade de informar, de se informar e de ser informado, sem impedimentos nem discriminações. 2. O exercício dos direitos e liberdades constantes do número anterior não pode ser impedido nem limitado por qualquer tipo ou forma de censura. 3. A liberdade de expressão e a liberdade de informação têm como limites os direitos de todos ao bom nome, à honra e à reputação, à imagem e à reserva da intimidade da vida privada e familiar, a protecção da infância e da juventude, o segredo de Estado, o segredo de justiça, o segredo profissional e demais garantias daqueles direitos, nos termos regulados pela lei. 4. As infracções cometidas no exercício da liberdade de expressão e de informação fazem incorrer o seu autor em responsabilidade disciplinar, civil e criminal, nos termos da lei. CAPÍTULO IV PODER JUDICIAL, SECÇÃO IV INSTITUIÇÕES ESSENCIAIS À JUSTIÇA, Artigo 196.º (Defesa Pública) 1. O Estado assegura, às pessoas com insuficiência de meios financeiros, mecanismos de defesa pública com vista à assistência jurídica e ao patrocínio forense oficioso, a todos os níveis. 2. A lei regula a organização e funcionamento da Defesa Pública. **Lei n.º 39/20, Código do Processo Penal Angolano** (Code of Criminal Procedure/ CPPA, 11 Nov 2020) PARTE I Disposições Gerais, TÍTULO II Sujeitos Processuais, CAPÍTULO I O Juiz e os Tribunais, SECÇÃO I Jurisdição, ARTIGO 9.º (Jurisdição penal) 1. Só os Tribunais Judiciais Criminais e respectivos juízes podem, sem prejuízo da jurisdição criminal especial concedida aos Tribunais Militares, conhecer de causas penais e aplicar penas e medidas de segurança.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2. Na Administração da Justiça Penal, os Tribunais e os juízes obedecem exclusivamente à Constituição, à Lei e aos princípios do Processo Penal. PARTE II Formas de Processo e Tramitação do Processo, TÍTULO II Tramitação do Processo Comum em Primeira Instância, CAPÍTULO I Fase da Instrução Preparatória, SECÇÃO II Actos de Instrução Preparatória, ARTIGO 313.º (Actos a praticar pelo juiz de garantias) 1. Durante a fase de instrução preparatória, cabe ao juiz de garantias do Tribunal territorialmente competente: a) Aplicar medidas de coacção; b) Apreciar as reclamações suscitadas dos actos do Ministério Público que apliquem medidas cautelares em instrução preparatória; c) Proceder ao primeiro interrogatório judicial de arguido detido; d) Ordenar buscas nos estabelecimentos referidos no n.º 2 do artigo 213.º; e) Admitir como assistente no processo as pessoas que, nos termos da lei, o requererem e tiverem legitimidade; f) Ordenar a apreensão dos objectos procesualmente relevantes encontrados nas buscas a que se refere a alínea d); g) Praticar os actos a que se refere o artigo 135.º que regula as faltas injustificadas dos participantes processuais; h) Ordenar e proceder à prestação antecipada de depoimentos ou declarações; i) Ordenar ou praticar qualquer outro acto que a lei determinar ou que, pela sua natureza, só possa ser ordenado ou praticado por quem for titular de poder jurisdicional. 2. É juiz de garantias, para efeitos do presente Código, o juiz nomeado ou designado para praticar os actos previstos no número anterior. 3. Nas comarcas em que não existir juiz de garantias ou quando o nomeado ou designado estiver impedido, os actos referidos no n.º 1 do presente artigo são praticados pelo juiz do Tribunal territorialmente competente para julgar o arguido, salvo os actos estabelecidos nas alíneas a), c) e d), que são deferidos ao juiz de garantias da Comarca mais próxima da mesma província judicial. 4. Para os efeitos das alíneas d) e f) do número anterior, os objectos encontrados durante as buscas, são presentes ao juiz que, depois de os examinar, ordena, conforme for o caso, a sua apreensão e junção ao processo ou a sua restituição.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	ARTIGO 314.º (Actos a autorizar pelo juiz de garantias) Compete ainda ao magistrado judicial competente, durante a fase de instrução preparatória, autorizar: a) Peritagens ou exames susceptíveis de ofender a integridade, a reserva da intimidade ou o pudor das pessoas; b) Escutas telefónicas e actos com eles relacionados, nos termos dos artigos 241.º e seguintes; c) c) Qualquer outro acto, nos casos em que a lei determinar que seja o juiz a conceder a autorização. **Lei nº. 7/17 Protecção das Redes e Sistemas Informáticos** (Law no. 7/17 Law for the Protection of IT Systems) CAPITULO III Medidas de Protecção aos Dados de Trafego e de Localização, SECCAO IV Medidas de Protecção dos Dados, ARTIGO 38.º (Destruição dos dados) 1. Sem prejuizo do proviso no artigo anterior, os operadores de comunicacoes electronicas acessiveis ao publico devem: a) Destruir os dados indicados no presente capitulo, no final do periodo de conservacao, excepto os dados que devam ser preservados por orden do Juiz competente; b) Destruir os dados ou copias dos dados que tenham sido preservados apos o decurso do periodo de conservacao, quando tal lhe seja determinado por orden das autoridades competentes e desde que os dados em causa nao tenham sido tambem preservados ao abrigo do orgao de investigacao criminal sob direccao do Ministerio Publico. 2. A autoridade publica competente para o controlo da aplicacao do previsto no numero anterior e a Agencia de Proteccao de Dados Pessoais.
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.	**Lei nº. 7/17 Protecção das Redes e Sistemas Informáticos** (Law no. 7/17 Law for the Protection of IT Systems) CAPITULO III Medidas de Protecção aos Dados de Trafego e de Localização, SECCAO I Preservação de Dados, ARTIGO 20.º (Conservaçõ 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
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.	2. Os dados referidos no número anterior devem ser preservados até 6 (seis) meses. 3. O responsável pelo tratamento dos dados deve 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.	**Lei nº. 7/17 Protecção das Redes e Sistemas Informáticos** (Law no. 7/17 Law for the Protection of IT Systems) CAPITULO III Medidas de Protecção aos Dados de Trafego e de Localização, SECCAO I Preservação de Dados, ARTIGO 21.º (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, deve 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	**CPPA** (Code of Criminal Procedure, 11 Nov 2020) PARTE I Disposições Gerais, TÍTULO V Meios de Obtenção de Prova, CAPÍTULO II Revistas e Buscas, ARTIGO 215.º (Auto de revista e de busca)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	1. Da revista ou da busca é sempre lavrado auto, que deve ser assinado pela entidade que presidiu à diligência, pelas pessoas que nela participaram e pelo funcionário que o redigiu. 2. Do auto devem constar a identificação da diligência, a do órgão ou entidade que presidiu à sua realização e a das pessoas que nela participaram, a indicação do lugar e da hora em que teve lugar e a descrição da forma como foi realizada, dos resultados obtidos e de tudo o mais considerado relevante que, durante ela, tiver ocorrido. CAPÍTULO III Apreensões, ARTIGO 225.º (Auto de apreensão) 1. Da apreensão é sempre lavrado um auto do qual deve constar a descrição da forma como decorreu a diligência, assim como o número, a qualidade, a quantidade, a natureza e as características dos objectos apreendidos. 2. O auto de apreensão é assinado pela entidade que presidiu à diligência e pelas demais pessoas que estiveram presentes que o puderem e quiserem fazer e elaborado em duplicado, para que uma das vias possa ser entregue ao arguido ou a pessoa que tenha assistido à apreensão. 3. Se não for possível mencionar, desde logo, o número, a qualidade, a quantidade e a natureza dos objectos apreendidos, devem ser embalados e as embalagens fechadas e seladas. 4. Tratando-se de documentos que devam ser imediatamente juntos ao processo, são rubricados pela entidade que presidiu à diligência e pelas demais pessoas presentes. 5. Se as rubricas forem susceptíveis de causar prejuízo aos documentos ou se estes tiverem de ser examinados, não se rubricam, tomando-se as precauções necessárias para que o exame e os resultados que dele se esperam não sejam prejudicados. ARTIGO 226.º (Apreensão em serviços de correios e telecomunicações) 1. A apreensão de cartas, encomendas, valores, telegramas ou qualquer outra espécie de correspondência, mesmo em instalação ou estação de correios e telecomunicações, é autorizada, na fase de instrução preparatória, ou ordenada, nas fases seguintes, pelo juiz, sempre que: a) A correspondência seja remetida pelo arguido ou a ele destinada. b) Tenha relação com crime a que corresponda pena de prisão, com máximo superior a 3 anos;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	c) A apreensão se revista de grande interesse para a prova do crime ou para a descoberta da verdade. 2. Não pode, sob pena de nulidade, ser interceptada e apreendida correspondência trocada entre o arguido e o seu defensor, salvo se disser respeito a crime de que este seja arguido. 3. O juiz que autorizou ou ordenou a apreensão é o primeiro a conhecer o conteúdo da correspondência encontrada validando-a, desde que não contenda com direitos e garantias do visado. TÍTULO V Meios de Obtenção de Prova, CAPÍTULO V Escutas Telefónicas, ARTIGO 241.º (Pressupostos e admissibilidade) 1. Durante a fase de instrução preparatória, são admissíveis a escuta e a gravação de conversas ou comunicações electrónicas, desde que se verifiquem os seguintes pressupostos: a) Serem a escuta e a gravação electrónica autorizadas pela autoridade judicial competente; b) Serem a escuta e a gravação indispensáveis para a descoberta da verdade ou tornar-se a prova, sem elas, impossível ou muito difícil de obter; c) Tratar-se de crimes de: i) Produção e tráfico ilícitos de estupefacientes; ii) Contrabando; iii) Lenocínio e tráfico sexual de pessoas, abuso sexual de menores e lenocínio de menores; iv) Sequestro, rapto e tomada de reféns; v) Falsificação de moeda, passagem de moeda falsa ou falsificada, circulação não autorizada de moeda, fabrico e falsificação de títulos de crédito e respectiva utilização; vi) Perigo comum, puníveis com pena de prisão superior, no seu limite máximo, a 5 anos; vii) Associação criminosa e organização terrorista; viii) Contra a paz e a comunidade internacional; ix) Contra a segurança do Estado, puníveis com pena de prisão superior, no seu limite máximo, a 5 anos; x) Injúria, ameaça, coacção, perturbação e devassa da vida privada, utilizando equipamentos de comunicação electrónica; xi) Tráfico de pessoas e órgãos; xii) Corrupção;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	xiii) Branqueamento de capitais; xiv) Natureza cibernética. 2. O disposto no número anterior é igualmente aplicável a todos os crimes puníveis com pena de prisão superior, no seu limite máximo, a 5 anos e à criminalidade transnacional organizada. 3. A gravação de conversas ou comunicações telefónicas pode ser utilizada em qualquer outro processo, já instaurado ou a instaurar, desde que ela seja indispensável à prova de qualquer dos crimes mencionados nos n.os 1 e 2 e se tratar de conversas ou comunicações entre pessoas referidas nos n.os 4 e 5 do artigo seguinte. 4. Os suportes técnicos das conversas ou comunicações electrónicas e os despachos que autorizam as escutas e gravações são, no caso do número anterior, juntos, por despacho do respectivo magistrado judicial competente, ao processo em que vão ser utilizados como meio de prova, extraindo-se, para tal efeito, quando for necessário, copias dos referidos suportes. ARTIGO 242.º (Autorização) 1. As escutas e gravações de conversas e comunicações electrónicas são autorizadas por despacho fundamentado do magistrado judicial competente, a requerimento do Ministério Público. 2. Pode, no entanto, a autorização ser requerida ao magistrado judicial competente do lugar onde a escuta e a gravação se pretendem efectuar ou ao magistrado judicial competente em que tem a sede a entidade encarregada da investigação criminal. 3. No caso do número anterior, a autorização concedida deve ser comunicada, no prazo máximo de 3 dias, ao magistrado judicial competente do processo. 4. Só podem ser submetidas a escuta e gravação as conversas e comunicações electrónicas que envolvam o suspeito ou arguido, seja qual for o equipamento electrónico utilizado, assim como as pessoas em relação às quais haja fortes razões para crer que recebem comunicações vindas de suspeitos ou arguidos, que a eles se destinem ou que utilizam os seus telefones. 5. Podem, do mesmo modo, ser submetidas a escuta e gravação as conversas ou comunicações feitas através equipamentos de comunicação electrónica utilizados pela vítima, se esta expressamente as autorizar. 6. Não podem ser autorizadas a escuta e a gravação das conversas ou comunicações telefónicas entre o arguido e o seu defensor, salvo se, no processo, existirem indícios de comparticipação criminosa do último.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	7. A proibição estabelecida no número anterior aplica-se às conversas ou comunicações electrónicas entre o arguido e pessoas obrigadas a segredo profissional. 8. A autorização a que se refere o presente artigo é válida por um período de 3 meses renovável por períodos com a mesma duração, por despacho do magistrado judicial competente e a requerimento do Ministério Público, enquanto se mantiverem os pressupostos exigidos pelo artigo anterior. ARTIGO 243.º (Modo de efectuar as escutas e gravações. Competência) 1. Compete ao Órgão de Polícia Criminal, sob a direcção do Ministério Público, efectuar as escutas e a gravação das conversas ou comunicações electrónicas a que se referem os artigos anteriores. 2. Da escuta e gravação são elaborados o respectivo auto e um relatório, no qual devem ser indicadas as passagens susceptíveis de servir como meio de prova, resumidamente descrito o respectivo conteúdo e justificada a sua importância para a descoberta da verdade. 3. Os autos e relatórios são elaborados de 15 em 15 dias, a partir do envio da primeira escuta e gravação, e levados ao conhecimento do Ministério Público, que os apresenta ao magistrado judicial competente, no prazo máximo de 48 horas, se não contender com direitos e garantias fundamentais do visado, além dos limites da autorização concedidas. 4. O Órgão de Polícia Criminal pode, logo que tome conhecimento do conteúdo das conversas ou comunicações telefónicas, praticar os actos urgentes necessários para acautelar e garantir os meios de prova. 5. O magistrado judicial competente pode requisitar a coadjuvação de elementos de Órgãos de Polícia Criminal para se certificar do conteúdo e sentido das conversas ou comunicações, assim como nomear intérprete, sendo caso disso. 6. Na fase de instrução preparatória, o Ministério Público pode requerer e o magistrado judicial competente ordenar que se transcrevem as conversas e comunicações relevantes capazes de fundamentar a aplicação de medidas de coacção e de garantia patrimonial, com ressalva do termo de identidade e residência. **Lei nº. 7/17 Protecção das Redes e Sistemas Informáticos** (Law no. 7/17 Law for the Protection of IT Systems)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	CAPITULO III Medidas de Protecção aos Dados de Trafego e de Localização, SECCAO I Preservação de Dados, ARTIGO 22.º (Preservação de provas) O operador de comunicações electrónicas acessiveis ao publico ou o prestador de servicios de sociedade da informação que tenha armazenado num determinado sistema de informação, dados de trafego e de localização necessarios a produção de provas, tendo em vista a descoberta da verdade, deve disponibilizer o controlo desses dados ou permitir o acesso ao sistema de informação onde os mesmos estao armazenados, aos Magistrados Judiciais ou do Ministerio Publico, nos termos da legislação Penal aplicavel e da presente Lei. Lei nº. 7/17 Protecção das Redes e Sistemas Informáticos, Artigo 36
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.	**CPPA** (Code of Criminal Procedure, 11 Nov 2020) PARTE I Disposições Gerais, TÍTULO V Meios de Obtenção de Prova, CAPÍTULO II Revistas e Buscas, ARTIGO 213.º (Quem ordena ou autoriza e preside às revistas e buscas) 1. Na fase da instrução preparatória, as revistas e as buscas são, sem prejuízo do disposto no artigo 214.º, ordenadas ou autorizadas por despacho do magistrado do Ministério Público competente e, nas restantes fases, pelo juiz que as dirigir. 2. As buscas em escritório de advogado, consultório médico e outros estabelecimentos de saúde, estações de correios e serviços de telecomunicações ou, ainda, em bancos e estabelecimentos bancários são sempre ordenadas ou autorizadas por despacho de um juiz, oficiosamente ou por promoção do Ministério Público ou a requerimento do assistente ou do arguido. 3. As autoridades judiciárias ordenam: a) Revistas em pessoas obrigadas ou autorizadas a participar em actos processuais ou a que possam e queiram, sendo o caso, assistir ou, ainda, em pessoas que, nos termos da lei, tenham de ser conduzidas a esquadras, postos ou instalações da polícia se, em qualquer um destes casos, houver razões para suspeitar que são portadoras de armas de fogo ou outras que possam ser usadas no cometimento de crimes; b) Revistas em pessoas suspeitas, em pessoas detidas fora de flagrante delito e em pessoas que se encontrarem no lugar em que se proceder a uma busca, em caso de receio de fuga eminente;

Back to the Table of Contents

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.	c) Buscas no lugar em que se encontrarem pessoas suspeitas, que não seja casa habitada ou suas dependências fechadas, no mesmo caso da alínea anterior. 4. As revistas e as buscas são, na fase de instrução preparatória e sem prejuízo do disposto no artigo 214.º, presididas pelo magistrado do Ministério Público competente, que pode delegar a direcção nos Órgãos de Polícia Criminal. 5. As buscas em escritório de advogado, consultório médico ou outros estabelecimentos de saúde são presididas pessoalmente pelo magistrado do Ministério Público, na fase de instrução preparatória e pelo juiz que as ordenar, nas fases subsequentes. 6. Nas fases posteriores à instrução preparatória, as revistas e as buscas são, sem prejuízo do disposto no número anterior, presididas pelo juiz ou por autoridade de polícia criminal em quem ele delegar. ARTIGO 214.º (Revistas e buscas urgentes) 1. As autoridades de polícia criminal podem, sem autorização, proceder a revistas e buscas, sempre que: a) Em caso de urgência, ocorrido em período em que os serviços públicos se encontrarem encerrados ou durante a ausência ou impedimento da autoridade judiciária competente ou, ainda, em altura em que for difícil contactá-la, se possa razoavelmente recear que a demora frustre as finalidades da diligência; b) Houver consentimento da pessoa que tem a disponibilidade do lugar objecto da busca; c) Se verifique iminência ou ocorrência de um crime, ou a pessoa submetida à revista tiver sido detida em flagrante delito. 2. Para os efeitos do disposto na alínea a) do número anterior, é razoável recear que a demora na realização da diligência frustre as suas finalidades, nos casos em que: a) Houver fortes indícios de eminente destruição ou perda da prova ou de fuga de pessoa que deva ser detida ou presa e ao crime corresponder pena de prisão superior, no seu limite máximo, a 3 anos; b) Se se tratar de crime violento ou organizado, punível com pena de prisão superior, no seu limite máximo, a 8 anos e existirem indícios de eminente cometimento de crime grave contra a liberdade, a vida ou integridade física de qualquer pessoa.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	3. Nos casos a que se referem os n.os 1 e 2, quem ordenar a diligência deve, no prazo de 24 horas, comunicar a sua realização à autoridade judiciária competente, a fim de que ela a valide. 4. Aplica-se às autoridades de polícia criminal o disposto do n.º 3 do artigo anterior. ARTIGO 217.º (Formalidades das buscas) 1. Antes de a busca se iniciar, é entregue à pessoa que tiver a posse do lugar onde vai realizar-se uma cópia do despacho que a ordenou. 2. Na cópia do despacho deve dizer-se expressamente que à busca pode assistir a pessoa que estiver na posse do lugar e que ela pode ainda fazer-se acompanhar de outra pessoa da sua confiança, que esteja no local ou possa apresentar- se sem demora. 3. Para os efeitos do disposto no número anterior, considera- se a apresentação demorada, sempre que seja de recear a possibilidade de ela frustrar as finalidades da diligência ou de causar outro prejuízo processual relevante. 4. Não se encontrando presente a pessoa que tiver a posse do lugar, a cópia do despacho que a ordenou pode, sempre que possível, ser entregue a um parente, vizinho, porteiro do prédio ou qualquer outra pessoa que seja encontrada no local e possa recebê-la, pessoas que, em tais casos, são autorizadas a assistir à diligência. 5. A autoridade que presidir à busca pode proibir que as pessoas que se encontrem no lugar onde a diligência se realiza, ou alguma delas, se afastem, recorrendo, se necessário, à força pública. 6. Quando a busca é presidida pelo juiz, além das pessoas referidas nos n.os 2 e 4, podem assistir à diligência o Ministério Público, o assistente, se o houver, o arguido e o seu defensor, para esse efeito devendo ser devidamente notificados. 7. O disposto na última parte do número anterior não se aplica às buscas a que se refere a alínea c) do n.º 3 do artigo 213.º 8. Deve proceder-se à busca de forma a preservar a integridade, a ordem e a disposição dos objectos encontrados no lugar e a deixar este, na medida do possível, num estado de arrumação semelhante ao que existia antes de a busca se ter iniciado.
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:	**CPPA** (Code of Criminal Procedure, 11 Nov 2020) PARTE I Disposições Gerais, TÍTULO V Meios de Obtenção de Prova, CAPÍTULO V Escutas Telefónicas, ARTIGO 247.º (Extensão do regime)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	O disposto no presente capítulo é correspondentemente aplicável às comunicações transmitidas à distância através de qualquer outro meio técnico análogo 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. **Lei nº. 7/17 Protecção das Redes e Sistemas Informáticos** (Law no. 7/17 Law for the Protection of IT Systems) CAPITULO III Medidas de Protecção aos Dados de Trafego e de Localização, SECCAO I Preservação de Dados, ARTIGO 21.º (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, deve indicar as otras entidades que nela participem, permitindo a indetificação das mesmas. ARTIGO 22.º (Preservação de provas) O operador de comunicações electrónicas acessiveis ao publico ou o prestador de servicios de sociedade da informação que tenha armazenado num determinado sistema de informação, dados de trafego e de localização necessarios a produção de provas, tendo em vista a descoberta da verdade, deve disponibilizer o controlo desses dados ou permitir o acesso ao sistema de informação onde os mesmos estao armazenados, aos Magistrados Judiciais ou do Ministerio Publico, nos termos da legislação Penal aplicavel e da presente Lei.
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	**CPPA** (Code of Criminal Procedure, 11 Nov 2020) PARTE I Disposições Gerais, TÍTULO V Meios de Obtenção de Prova, CAPÍTULO V Escutas Telefónicas, 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 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
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.	**Lei nº. 7/17 Protecção das Redes e Sistemas Informáticos** (Law no. 7/17 Law for the Protection of IT Systems) CAPITULO III Medidas de Protecção aos Dados de Trafego e de Localização, SECCAO IV Medidas de Protecção dos Dados, ARTIGO 37.º (Obrigação de intercepção) 1. Os operadores de comunicações electrónicas acessiveis ao publico sao obrigados a instalar, a expensas proprias e a disponibilizar a autoridade judiciaria competente, sistemas de intercepcao legal, mediante despacho fundamentado do Magistrado competente. 2. Os operadores de comunicações electrónicas acessiveis ao publico devem proceder a intercepcao e registo de dados, quando solicitados, por despacho fundamentado do Magistrado competente e apenas nos casos em que a intercepcao e registo sejam admissiveis. SECCAO V Preservacao da Soberanía, Seguranca do Estado e Ordem Publica, ARTIGO 39.º (Sistema de Intercepção de dados) Os operadores de comunicações electrónicas acessiveis ao publico devem asegurar o acesso aos orgaos de inteligencia e de seguranca do Estado mediante autorizacao previa do Magistrado competente, para proceder a intercepção de communicacoes, nos termos do artigo 212 da Constituição da República de Angola. [Constitution 2010]
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.	**CPA** (11 November 2020) LIVRO I Parte Geral, TÍTULO I Lei Criminal, CAPÍTULO ÚNICO Princípios Gerais, ARTIGO 4.º (Aplicação da lei no espaço) A Lei Penal Angolana é aplicável a factos total ou parcialmente praticados em território angolano ou a bordo de navios ou aeronaves de matrícula ou sob pavilhão angolanos, independentemente da nacionalidade do agente, salvo convenção ou tratado internacional em contrário. ARTIGO 5.º (Aplicação da Lei Penal Angolana a factos ocorridos fora do território nacional)

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.	1. Salvo convenção ou tratado internacional em contrário, a Lei Penal Angolana é aplicável a factos cometidos for a do território angolano, quando: a) Constituírem os crimes previstos nos artigos 256.º a 264.º, 296.º, 297.º, 310.º a 319.º, 329.º a 332.º, 336.º e 469.º; b) Constituírem os crimes previstos nos artigos 377.º a 382.º, 384.º a 389.º, desde que o agente seja encontrado em Angola e não possa ser extraditado; c) Forem cometidos contra pessoas colectivas ou cidadãos angolanos, desde que o agente viva habitualmente em Angola e aqui seja encontrado; d) Forem cometidos por angolanos ou pessoas colectivas angolanas, ou por estrangeiros ou pessoas colectivas estrangeiras contra pessoas colectivas ou cidadãos angolanos, desde que: i) Os factos sejam igualmente puníveis pela lei do lugar em que foram cometidos; ii) Constituam crime que segundo a lei angolana admita extradição, mas esta não possa ser concedida; iii) O agente seja encontrado ou tenha sede, filial ou sucursal em Angola. e) Constituírem crimes que, por convenção ou tratado internacional, o Estado Angolano se tenha obrigado a julgar. 2. O disposto no número anterior só tem aplicação quando o agente não tiver sido julgado no país em que cometeu o crime ou se, posteriormente, se tiver subtraído ao cumprimento, total ou parcial, da sanção em que tenha sido condenado. 3. Salvo tratado ou convenção internacional em contrário, a Lei Penal Angolana é aplicável a factos praticados no estrangeiro por funcionários das organizações internacionais de direito público de que Angola seja Parte, desde que o agente seja cidadão nacional e a extradição não possa ser concedida. 4. A Lei Penal Angolana é ainda aplicável a factos praticados fora do território nacional, nos termos previstos em tratado ou convenção internacional de que Angola seja Parte. **CPPA** (Code of Criminal Procedure, 11 Nov 2020) PARTE I Disposições Gerais, TÍTULO I Disposições Preliminares, ARTIGO 5.º (Aplicação da Lei Processual Penal no espaço) 1. A Lei Processual Penal é aplicável em todo o território nacional.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2. Fora do território nacional, a Lei Processual Penal só é aplicável nos limites definidos pelo direito internacional e pelos acordos, tratados e convenções internacionais de que Angola é Parte.
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 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	**Constituição Da República De Angola (Constitution, 2010)** TÍTULO II DIREITOS E DEVERES FUNDAMENTAIS, CAPÍTULO II DIREITOS, LIBERDADES E GARANTIAS FUNDAMENTAIS, SECÇÃO II GARANTIA DOS DIREITOS E LIBERDADES FUNDAMENTAIS, Artigo 70.º (Extradição e expulsão) 1. Não é permitida a expulsão nem a extradição de cidadãos angolanos do território nacional. 2. Não é permitida a extradição de cidadãos estrangeiros por motivos políticos ou por factos passíveis de condenação à pena de morte e sempre que se admita, com fundamento, que o extraditado possa vir a ser sujeito a tortura, tratamento desumano, cruel ou de que resulte lesão irreversível da integridade física, segundo o direito do Estado requisitante. 3. Os tribunais angolanos conhecem, nos termos da lei, os factos de que sejam acusados os cidadãos cuja extradição não seja permitida de acordo com o disposto nos números anteriores do presente artigo. 4. Só por decisão judicial pode ser determinada a expulsão do território nacional de cidadãos estrangeiros ou de apátridas autorizados a residir no país ou que tenham pedido asilo, salvo em caso de revogação do acto de autorização, nos termos da lei. 5. A lei regula os requisitos e as condições para a extradição e a expulsão de estrangeiros. **Lei N.º 13/15, Lei Da Cooperação Judiciária Internacional Em Matéria Penal** (19 June 2015), TÍTULO II EXTRADIÇÃO

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	**Lei N.º 13/15, Lei Da Cooperação Judiciária Internacional Em Matéria Penal** (19 June 2015) TÍTULO I DISPOSIÇÕES GERAIS, CAPÍTULO I OBJECTO E ÂMBITO DE APLICAÇÃO, Artigo 1.º (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

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	administrativas, bem como de infracções que constituam ilícito transgressional, cujos processos admitam recurso judicial. CAPÍTULO II PRINCÍPIOS GERAIS, Artigo 4.º (Prevalência de tratados internacionais) 1- A cooperação judiciária em matéria penal rege-se pelas normas constantes de tratados internacionais que, nos termos da Lei n.º 4/11, de 14 de Fevereiro Lei dos Tratados Internacionais, vinculem o Estado Angolano e, na sua falta ou insuficiência, pelas disposições desta lei. 2- São subsidiariamente aplicáveis as disposições da legislação processual penal. Artigo 5.º (Princípio da reciprocidade) 1- À cooperação internacional em matéria penal é aplicável o princípio da reciprocidade. 2- No âmbito das suas atribuições, a autoridade central solicita uma garantia de reciprocidade se as circunstâncias o exigirem e pode prestá-la a outros Estados, nos limites da presente lei. Artigo 7.º (Requisitos gerais negativos da cooperação internacional) 1 - O pedido de cooperação é recusado quando: a) O processo não satisfizer ou não respeitar as exigências dos tratados internacionais aplicáveis na República de Angola; b) Existirem fundadas razões para crer que a cooperação é solicitada com o fim de perseguir ou punir uma pessoa em virtude da sua nacionalidade, ascendência, raça, sexo, língua, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou pertença a um grupo social determinado; c) Existir risco de agravamento da situação processual de uma pessoa por qualquer das razões indicadas na alínea anterior; d) Puder conduzir a julgamento por um tribunal de excepção ou respeitar a execução de sentença proferida por um tribunal dessa natureza; e) Respeitar a facto punível com pena de morte ou sempre que se admita, com fundamento, que possa resultar a prática de tortura, tratamento desumano ou outra de que possa resultar lesão irreversível da integridade da pessoa; f) Respeitar a infracção a que corresponda pena de prisão ou medida de segurança com carácter perpétuo ou de duração indefinida.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	2- O pedido de cooperação é ainda recusado quando não estiver garantida a reciprocidade. 3- Quando for negada a extradição com base nas alíneas d), e) e f) do n.º 1, aplica-se o mecanismo de cooperação previsto no nº 2 do artigo 33.º Artigo 8.º (Recusa relativa à natureza da infracção) 1- O pedido é também recusado quando o processo respeitar a facto que constitua: a) Infracção de natureza política ou a ela conexa, segundo as concepções do direito angolano; b) Crime militar que não seja simultaneamente previsto na lei penal comum. 2- Não se consideram de natureza política: a) O genocídio, os crimes contra a Humanidade, os crimes de guerra e infracções graves segundo as Convenções de Genebra de 1949; b) Os actos referidos na Convenção contra a Tortura e Outras Penas ou Tratamentos Cruéis, Desumanos ou Degradantes, adoptada pela Assembleia das Nações Unidas em 17 de Dezembro de 1984; c) As infracções compreendidas no campo da aplicação da Convenção para a Repressão da Captura Ilícita de Aeronaves, assinada em Haia ao 16 de Dezembro de 1970; d) As infracções compreendidas no campo da aplicação da Convenção para a Repressão de Actos Ilícitos Dirigidos contra a Segurança da Aviação Civil, assinada em Montreal em 23 de Setembro de 1971; e) As infracções graves constituídas por um ataque contra a vida, a integridade física ou a liberdade das pessoas que gozem de protecção internacional, inclusive os agentes diplomáticos; f) As infracções que comportam o rapto, a detenção de reféns ou o sequestro; g) As infracções que comportam a utilização de bombas, granadas, foguetões, armas de fogo ou cartas ou embrulhos armadilhados, na medida em que essa utilização apresente perigo para quaisquer pessoas; h) A tentativa de cometimento de uma das infracções acima citadas ou a participação como co-autor ou cúmplice; i) Quaisquer outros crimes a que seja retirada natureza política por tratado, convenção ou acordo internacional de que a República de Angola seja parte. Artigo 9.º (Extinção do procedimento penal)

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	1- A cooperação não é admissível se, em Angola ou noutro Estado em que tenha sido instaurado procedimento pelo mesmo facto: a) O processo tiver terminado com sentença absolutória transitada em julgado ou com decisão de arquivamento; b) A sentença condenatória se encontrar cumprida ou não puder ser cumprida segundo o direito do Estado em que foi proferida; c) O procedimento se encontrar extinto por qualquer outro motivo, salvo se estiver previsto em convenção internacional, como não obstando à cooperação por parte do Estado requerido. 2- O disposto nas alíneas a) e b) do número anterior não se aplica se, a autoridade estrangeira que formular o pedido o justificar para fins de revisão de sentença e os fundamentos desta forem idênticos aos admitidos no direito angolano. 3- O disposto na alínea a) do n.º 1 não obsta à cooperação com fundamento na reabertura de processo arquivado previsto na lei. Artigo 10.º (Concurso de casos de admissibilidade e de inadmissibilidade da cooperação) 1- Se o facto imputado à pessoa contra quem é instaurado procedimento estiver previsto em várias disposições do direito penal angolano, o pedido de cooperação só é atendido na parte respeitante à infracção ou infracções relativamente às quais seja admissível o pedido e desde que o Estado requerente dê garantias de observar as condições fixadas para a cooperação. 2- A cooperação é, porém, excluída se o facto estiver previsto em varias disposições do direito penal angolano ou estrangeiro e o pedido não possa ser satisfeito por força de uma disposição legal que o abranja na sua totalidade e que constitua motivo de recusa da cooperação. Artigo 11.º (Relevância da infracção) 1- A cooperação pode ser recusada se a reduzida importância da infracção não a justificar. 2- Para efeitos do número anterior, consideram-se de reduzida importância: a) As infracções de natureza criminal puníveis com pena de prisão com limite máximo de até 3 anos; b) As infracções de natureza contravencional ou transgressional puníveis com pena de multa com o limite máximo de até Kz. 2.000.000.00 (dois milhões de Kwanzas).

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Artigo 12.º (Protecção do segredo) Na execução de um pedido de cooperação requerido à República de Angola observam-se as disposições do Código de Processo Penal e legislação complementar relativas à recusa de testemunhar, às apreensões, escutas telefónicas e ao segredo profissional ou de Estado e nos demais casos em que o segredo seja protegido nos termos da lei. Artigo 13.º (Direito aplicável) 1- Produzem efeitos na República de Angola: a) Os motivos de interrupção ou de suspensão da prescrição segundo o direito do Estado requerente; b) A queixa apresentada em tempo útil a uma autoridade estrangeira, quando for igualmente exigida pela lei angolana. 2- Se apenas o Direito angolano exigir queixa, nenhuma sanção criminal pode ser imposta ou executada em Angola na falta de queixa ou no caso de desistência do respectivo titular. Artigo 16.º (Concurso de pedidos) 1- Se a cooperação for solicitada por vários Estados, relativamente ao mesmo ou a diferentes factos, esta é concedida em favor do Estado que, tendo em conta as circunstâncias do caso, assegure melhor os interesses da realização da justiça e da reinserção social do suspeito, do arguido ou do condenado. 2- O disposto no número anterior: a) Cede perante a regra de prevalência da jurisdição internacional, nos casos a que se refere o n.º 2 do artigo 1.º; b) Não se aplica à forma de cooperação referida na alínea f) do n.º 1 do artigo 1.º Artigo 19.º (Denegação facultativa da cooperação internacional) 1- Pode ser negada a cooperação quando o facto que a motiva for objecto deprocesso pendente ou quando esse facto deva ou possa ser também objecto de procedimento da competência de uma autoridade judiciária angolana. 2- Pode ainda ser negada a cooperação quando, tendo em conta as circunstancias do facto, o deferimento do pedido possa implicar consequências graves para a pessoa visada, em razão da idade, estado de saúde ou de outros motivos de carácter pessoal.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Artigo 20.º (Non bis in idem) Quando for aceite um pedido de cooperação que implique a delegação do procedimento em favor de uma autoridade judiciária estrangeira, não pode instaurar-se nem continuar em Angola procedimento pelo mesmo facto que determinou o pedido nem executar-se sentença cuja execução é delegada numa autoridade estrangeira. TÍTULO VII COOPERAÇÃO NO ÂMBITO DO CIBERCRIME, CAPÍTULO II PRESERVAÇÃO E REVELAÇÃO EXPEDITAS DE DADOS INFORMÁTICOS, 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 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	

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.	**Lei N.º 13/15, Lei Da Cooperação Judiciária Internacional Em Matéria Penal** (19 June 2015) TÍTULO VII COOPERAÇÃO NO ÂMBITO DO CIBERCRIME, CAPÍTULO II PRESERVAÇÃO E REVELAÇÃO EXPEDITAS DE DADOS INFORMÁTICOS, 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 informático; e) A necessidade da medida de preservação; e

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. 7 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.	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 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 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	**Lei N.º 13/15, Lei Da Cooperação Judiciária Internacional Em Matéria Penal** (19 June 2015) TÍTULO VII COOPERAÇÃO NO ÂMBITO DO CIBERCRIME, CAPÍTULO II PRESERVAÇÃO E REVELAÇÃO EXPEDITAS DE DADOS INFORMÁTICOS, 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.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	2- O disposto nos nºs 1 e 2 do artigo 166.º aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades angolanas.
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.	**Lei N.º 13/15, Lei Da Cooperação Judiciária Internacional Em Matéria Penal** (19 June 2015) TÍTULO VII COOPERAÇÃO NO ÂMBITO DO CIBERCRIME, CAPÍTULO II PRESERVAÇÃO E REVELAÇÃO EXPEDITAS DE DADOS INFORMÁTICOS, 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 voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**Lei N.º 13/15, Lei Da Cooperação Judiciária Internacional Em Matéria Penal** (19 June 2015) TÍTULO VII COOPERAÇÃO NO ÂMBITO DO CIBERCRIME, CAPÍTULO II PRESERVAÇÃO E REVELAÇÃO EXPEDITAS DE DADOS INFORMÁTICOS, Artigo 174.º (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) b) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Angola, mediante

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 13/15, Lei Da Cooperação Judiciária Internacional Em Matéria Penal** (19 June 2015) TÍTULO VI AUXÍLIO JUDICIÁRIO MÚTUO EM MATÉRIA PENAL, CAPÍTULO III ACTOS PARTICULARES DE AUXÍLIO INTERNACIONAL, 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 proceso 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. TÍTULO VII COOPERAÇÃO NO ÂMBITO DO CIBERCRIME, CAPÍTULO II PRESERVAÇÃO E REVELAÇÃO EXPEDITAS DE DADOS INFORMÁTICOS, 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. 2- São competentes para a recepção dos pedidos de intercepção o Serviço de Investigação Criminal, que os apresentará ao magistrado do Ministério Público titular na respectiva Comarca para autorização. 3- O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 angolanas.
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 13/15, Lei Da Cooperação Judiciária Internacional Em Matéria Penal** (19 June 2015) TÍTULO VI AUXÍLIO JUDICIÁRIO MÚTUO EM MATÉRIA PENAL, CAPÍTULO III ACTOS PARTICULARES DE AUXÍLIO INTERNACIONAL, 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 proceso 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. TÍTULO VII COOPERAÇÃO NO ÂMBITO DO CIBERCRIME, CAPÍTULO II PRESERVAÇÃO E REVELAÇÃO EXPEDITAS DE DADOS INFORMÁTICOS, 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. 2- São competentes para a recepção dos pedidos de intercepção o Serviço de Investigação Criminal, que os apresentará ao magistrado do Ministério Público titular na respectiva Comarca para autorização.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	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 angolanas.
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 13/15, Lei Da Cooperação Judiciária Internacional Em Matéria Penal** (19 June 2015) TÍTULO VII COOPERAÇÃO NO ÂMBITO DO CIBERCRIME, CAPÍTULO II PRESERVAÇÃO E REVELAÇÃO EXPEDITAS DE DADOS INFORMÁTICOS, 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. a) 3- A assistência imediata prestada por este ponto de contacto permanente inclui: 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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