Ante-Projecto de Lei de Combate à Criminalidade no Domínio das Tecnologias de Informação e Comunicação e dos Serviços da Sociedade da Informação

REPÚBLICA DE ANGOLA

ASSEMBLEIA NACIONAL

Lei n.º _____/2011

de _____ de _____

Considerando que o crescente avanço das tecnologias de informação e comunicação, bem como da sociedade da informação, tem contribuído para o progresso social, económico e cultural das sociedades actuais, ao mesmo tempo que tem trazido o risco de utilização das redes informáticas e de comunicações electrónicas para a prática de infracções penais;

Tendo em conta que as tecnologias de informação e comunicação não são utilizadas somente como um novo instrumento para a prática de crimes previstos na lei, mas a sua evolução se tem traduzido também no surgimento de uma nova criminalidade caracterizada pelo ataque aos sistemas de informação e aos dados neles armazenados;

Considerando que o pleno aproveitamento pelo Estado Angolano de todos os benefícios da sociedade da informação exige concomitantemente que se criem as condições necessárias para que os agentes económicos e os consumidores tenham a confiança necessária para utilizarem em larga escala os novos recursos electrónicos, evitando que estes constituam uma fonte de insegurança em qualquer sector da sociedade;

Assim, torna-se imprescindível reprimir os actos praticados contra a confidencialidade, integridade e disponibilidade dos sistemas de informação e comunicação, bem como contra a sua utilização fraudulenta, mediante a criminalização destes comportamentos.

Considerando que a eficácia do combate à criminalidade no domínio das TICs exige a previsão de sanções proporcionadas e dissuasivas da prática de tais comportamentos e a consagração de regras específicas em matéria de prova e da recolha da prova para crimes praticados com recurso a um sistema de informação ou em relação aos quais seja necessário reco-

lher prova em suporte electrónico, sem prejuízo da garantia da manutenção de um equilíbrio adequado entre os interesses a que a presente lei visa responder e o respeito pelos direitos fundamentais consagrados constitucionalmente, nomeadamente o direito à privacidade e à liberdade de expressão;

Tendo em conta que a presente lei visa responder de forma eficaz aos novos desafios da sociedade da informação, traduzida no aumento da designada "cibercriminalidade" com todos os riscos a ela associados, incluindo em matéria de criminalidade organizada e de terrorismo.

A Assembleia Nacional aprova, por mandato do povo, nos termos do nº 2 do artigo 165º e da alínea d) do nº 2 do artigo 166º ambos da Constituição da República de Angola, o seguinte:

LEI DE COMBATE À CRIMINALIDADE NO DOMÍNIO DAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO E DOS SERVIÇOS DA SOCIEDADE DA INFORMAÇÃO

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º
(Objecto)

A presente lei estabelece as disposições penais, substantivas e adjectivas, relativas ao domínio da criminalidade no âmbito das tecnologias e da sociedade da informação e da recolha da prova em suporte electrónico.

(Âmbito de aplicação)

1. Sem prejuízo do n.º 2 seguinte, e para além do disposto nas normas penais vigentes, a presente lei é ainda aplicável a factos nela previstos que:
   a) Sejam cometidos por cidadão angolano ou pessoa colectiva de direito angolano com domicílio em território angolano;

b) Sejam fisicamente praticados, total ou parcialmente, em território angolano, ainda que visem sistemas de informação ou dados localizados fora desse território; ou

c) Visem sistemas de informação ou dados localizados em território angolano, independentemente do local onde esses factos forem fisicamente praticados.

2. O disposto na secção VII do Capítulo IV aplica-se aos operadores de comunicações electrónicas acessíveis ao público e aos prestadores de armazenagem principal estabelecidos em território nacional.

Artigo 2.º

(Exclusões)

O regime constante da presente lei não prejudica:

a) O disposto nas normas constantes dos tratados e das convenções internacionais vigentes na ordem jurídica nacional;

b) O disposto em legislação vigente que seja compatível com a mesma;

c) O disposto no regime jurídico de protecção de dados pessoais;

d) O disposto no regime jurídico das tecnologias e dos serviços da sociedade da informação.

Artigo 3.º

(Responsabilidade criminal das pessoas colectivas e equiparadas)

1. As pessoas colectivas e entidades equiparadas, com excepção do Estado, de outras pessoas colectivas públicas e de organizações internacionais de direito público, são responsáveis pelos crimes previstos na presente lei, quando cometidos:
   a) Em seu nome e no interesse colectivo por pessoas que nelas ocupem uma posição de liderança; ou
   b) Por quem aja sob a autoridade das pessoas referidas na alínea anterior, quando a falta de vigilância ou controlo por parte destas possibilite a prática de um dos crimes previstos na presente lei em benefício da referida pessoa colectiva.
2. Para efeitos da presente lei, a expressão pessoas colectivas públicas abrange:
   a) Pessoas colectivas de direito público, nas quais se incluem as entidades públicas empresariais;
   b) Entidades concessionárias de serviços públicos, independentemente da sua titularidade;
   c) Demais pessoas colectivas que exerçam prerrogativas de poder público.
3. Entende-se que ocupam uma posição de liderança os órgãos e representantes da pessoa colectiva e quem nela tiver autoridade

para exercer o controlo da sua actividade ou tomar decisões em seu nome.

4. Para efeitos da presente lei, consideram-se entidades equiparadas a pessoas colectivas as sociedades civis e as meras associações de facto.
5. A responsabilidade das pessoas colectivas e entidades equiparadas é excluída quando o agente tiver actuado contra ordens ou instruções expressas de quem de direito.
6. A responsabilidade das pessoas colectivas e entidades equiparadas não exclui a responsabilidade individual dos respectivos agentes nem depende da responsabilização destes.
7. A cisão e a fusão não determinam a extinção da responsabilidade criminal da pessoa colectiva ou entidade equiparada, respondendo pela prática do crime:
   a) A pessoa colectiva ou entidade equiparada em que a fusão se tiver efectivado; e
   b) As pessoas colectivas ou entidades equiparadas que resultaram da cisão.
8. Sem prejuízo do direito de regresso, as pessoas que ocupem uma posição de liderança são subsidiariamente responsáveis pelo pagamento das multas e indemnizações em que a pessoa colectiva ou entidade equiparada for condenada, relativamente aos crimes:

a) Praticados no período de exercício do seu cargo, sem a sua oposição expressa;
b) Praticados anteriormente, quando tiver sido por culpa sua que o património da pessoa colectiva ou entidade equiparada se tornou insuficiente para o respectivo pagamento; ou
c) Praticados anteriormente, quando a decisão definitiva de as aplicar tiver sido notificada durante o período de exercício do seu cargo e lhes seja imputável a falta de pagamento.

9. Sendo várias as pessoas responsáveis nos termos do número anterior, é solidária a sua responsabilidade.
10. Se as multas ou indemnizações forem aplicadas a uma entidade sem personalidade jurídica, responde por elas o património comum e, na sua falta ou insuficiência, solidariamente, o património de cada um dos associados.

Artigo 4.º

(Definições)

Para efeitos da presente lei, considera-se:

a) **Acesso condicional**: sujeição do acesso de um serviço a uma assinatura ou qualquer outra forma de autorização prévia individual;

b) **Assinante**: a pessoa singular ou colectiva que é parte num contrato com um operador de comunicações electrónicas acessíveis ao público;

c) **Autoridade Competente**: o juiz, ou qualquer oficial de justiça ou agente da autoridade por sua ordem, e o Ministério Público nos termos da lei processual penal;

d) **Base de dados**: as colectâneas de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e susceptíveis de acesso individual por meios electrónicos ou outros;

e) **Chamada telefónica falhada**: uma comunicação vocal em que a ligação telefónica foi estabelecida mas que não obteve resposta (isto é, não foi atendida pelo destinatário) ou em que houve uma intervenção do gestor da rede (incluindo os casos nos quais a chamada foi desviada para o atendedor de chamadas do destinatário);

f) **Código de acesso**: dado ou senha que permite aceder, no todo ou em parte e sob forma inteligível, a um sistema de informação;

g) **Código de identificação do utilizador (user ID)**: um código único atribuído às pessoas quando estas se tornam assinantes ou se registam num serviço de acesso à Internet, ou num serviço de comunicação pela Internet;

h) **Conteúdos discriminatórios**: qualquer palavra, imagem ou outro que defenda, promova ou incite ao ódio ou a actos de violência

contra uma pessoa ou grupo de pessoas por causa da sua raça, origem étnica, cor, nacionalidade, religião ou orientação sexual, com o propósito de os discriminar;

i) **Dados**: qualquer representação de factos, informações ou conceitos, incluindo de programas de computador, que é armazenada, transmitida ou processada num sistema de informação. Os dados incluem nomeadamente os dados de base, de tráfego, de localização e de conteúdo;

j) **Dados de base**: os dados que permitem identificar uma pessoa, como seja o nome, idade, morada, telefone e endereço de correio electrónico;

k) **Dados de conteúdo**: os dados relativos ao conteúdo de uma comunicação ou conversação;

l) **Dados de localização**: quaisquer dados tratados num sistema de informação que indiquem a posição geográfica do equipamento terminal ou de um utilizador de um serviço prestado através de um sistema de informação;

m) **Dados de tráfego**: quaisquer dados tratados para efeitos do envio de uma comunicação através de um sistema de informação ou para efeitos de facturação daquela, incluindo os dados que indicam a origem, destino, trajecto, hora, data, tamanho e duração da comunicação, ou o tipo de serviço subjacente;

n) **Dados informáticos**: qualquer dado susceptível de processamento por um sistema informático;

o) **Dispositivo**: qualquer equipamento, material (electromagnético, acústico, mecânico, técnico ou outro) ou programa de computador;

p) **DSL (digital subscriber line)**: tecnologia que permite aproveitar o conjunto de pares de cabo de cobre para fins de serviços de Internet de banda larga;

q) **Endereço do protocolo IP**: o conjunto de números que permitem a identificação e a comunicação consistente entre equipamentos (normalmente computadores) de uma rede privada ou pública, mediante uma plataforma de Internet;

r) **Identificador de célula (cell ID):** a identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

s) **IMEI**: ("international mobile equipment identity"): o código pré-gravado nos telefones móveis da tecnologia GSM, que permite a identificação do equipamento ou do terminal a nível internacional, ao ser transmitido ou ao interligar-se a uma rede de comunicações electrónicas acessíveis ao público. Caso a tecnologia usada não seja GSM considera-se o código equivalente para a tecnologia em questão;

t) **IMSI:** ("international mobile subcriber identity"): o código único de identificação para cada aparelho terminal de telefonia móvel cuja integração no cartão SIM do telemóvel, permite a sua identificação através das redes da tecnologia GSM e UMTS. Caso a tecnologia usada não seja GSM e UMTS considera-se o código equivalente para a tecnologia em questão;

u) **Intercepção**: o acto destinado a captar dados contidos ou transmitidos através de um sistema de informação mediante o recurso a dispositivos;

v) **Material pornográfico simulado**: imagens realistas representando um menor de 18 anos envolvido em comportamentos sexualmente explícitos;

w) **Medidas de carácter tecnológico**: toda a técnica, dispositivo ou componente que, no decurso do seu funcionamento normal, se destinem a impedir ou restringir actos relativos a obras, prestações e produções protegidas (incluindo bases de dados protegidas pelo direito *sui generis* e excluindo programas de computador), que não sejam autorizados pelo titular dos direitos de autor ou conexos ou não sejam permitidos por lei, não devendo considerar-se como tais:

   i. Um protocolo;

   ii. Um formato;

iii. Um algoritmo;

iv. Um método de criptografia, de codificação ou de transformação.

x) **Medidas eficazes de carácter tecnológico**: medidas de carácter tecnológico em que a utilização da obra, prestação ou produção protegidas é controlada pelos titulares de direitos mediante a aplicação de um controlo de acesso ou de um processo de protecção como, entre outros, a codificação, cifragem ou outra transformação da obra, prestação ou produção protegidas, ou um mecanismo de controlo da cópia, que garanta a realização do objectivo de protecção;

y) **Informação para a gestão electrónica dos direitos**: toda a informação prestada pelos titulares dos direitos de autor e conexos (incluindo os titulares das bases de dados protegidas pelo direito *sui generis* e excluindo os titulares de programas de computador), que identifique a obra, a prestação e a produção protegidas, a informação sobre as condições de utilização destes, bem como quaisquer números ou códigos que representem essa informação;

z) **Operadores de comunicações electrónicas**: os organismos, as pessoas colectivas de direito público, as pessoas singulares ou colectivas de direito privado ou misto, que oferecem redes ou serviços de comunicações electrónicas;

aa) **Operadores de comunicações electrónicas acessíveis ao público**: os operadores de redes de comunicações electrónicas públicas e os operadores de serviços de comunicações electrónicas públicos, conforme estes sejam definidos na legislação relevante;

bb) **Organização criminosa**: o agrupamento de duas ou mais pessoas que se mantém ao longo do tempo (i.e., que não é constituída de forma fortuita para a prática imediata de uma infracção) e actua de forma concertada, tendo em vista a prática de crime com o objectivo de obter, directa ou indirectamente, benefícios políticos, económico-financeiros ou sociais, entre outros.

cc) **Organização terrorista**: o agrupamento de duas ou mais pessoas que, actuando concertadamente, visem prejudicar a integridade e a independência do Estado angolano ou de outro Estado, impedir, alterar ou subverter o funcionamento das instituições do Estado, forçar as respectivas autoridades a praticar um acto, a abster-se de o praticar ou a tolerar que se pratique, ou ainda intimidar certas pessoas, grupos de pessoas ou populações, mediante acções:

i. Contra a vida, a integridade física ou a liberdade das pessoas;

ii. Contra a segurança dos transportes e das comunicações, incluindo as informáticas, electrónicas, telegráficas, telefónicas, de rádio ou de televisão;

iii. Dolosas de perigo comum, através de incêndio, explosão, libertação de substâncias radioactivas ou de gases tóxicos ou asfixiantes, de inundação ou avalancha, desmoronamento de construção, contaminação de alimentos e águas destinadas a consumo humano ou difusão de doença, praga, planta ou animal nocivos;

iv. Que destruam ou que impossibilitem o funcionamento ou desviem dos seus fins normais, definitiva ou temporariamente, total ou parcialmente, meios ou vias de comunicação, de transmissão ou de transporte, instalações portuárias, fábricas ou depósitos, instalações de serviços públicos ou destinadas ao abastecimento e satisfação de necessidades vitais da população;

v. De Investigação e desenvolvimento de armas biológicas ou químicas;

vi. Que impliquem o emprego de energia nuclear, armas de fogo, biológicas ou químicas, substâncias ou engenhos explosivos, meios incendiários de qualquer natureza, encomendas ou cartas armadilhadas;

dd) **Pornografia infantil**: qualquer material pornográfico que represente, de forma visual ou sonora, um menor de 18 anos, ou pessoa

aparentando ser menor de 18 anos, envolvidos em comportamentos sexualmente explícitos;

ee) **Prestador de serviço**: qualquer pessoa, singular ou colectiva, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema de informação, bem como qualquer outra entidade que trate ou armazene dados em nome e por conta daquela ou dos respectivos utilizadores, incluindo, mas não se limitando, a operadores de comunicações electrónicas e prestadores de serviços da sociedade da informação;

ff) **Produto semicondutor**: a forma final ou intermédia de qualquer produto que, cumulativamente:

i. Consista num corpo material que inclua uma camada de material semicondutor;

ii. Possua uma ou mais camadas compostas de material condutor, isolante ou semicondutor, estando as mesmas dispostas de acordo com um modelo tridimensional predeterminado;

iii. Seja destinado a desempenhar uma função electrónica, quer exclusivamente, quer em conjunto com outras funções.

gg) **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;

hh) **Rede**: grupo de sistemas de informação interligados entre si que permite o envio e a recepção de dados;

ii) **Rede de comunicações electrónicas:** os 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, meios ópticos, ou por outros meios electro-magnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a Internet) e móveis, os sistemas de cabos de electricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes utilizadas para a radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informação transmitida;

jj) **Rede telefónica pública**: a rede de comunicações electrónicas utilizada para prestar serviços telefónicos acessíveis ao público;

kk) **Serviço da sociedade da informação**: serviço prestado à distância por via electrónica, no âmbito de uma actividade económica na sequência de pedido individual do destinatário, considerando-se, para efeitos da presente definição:

   i. Serviço: a disponibilização de conteúdos, bens (materiais e imateriais) e serviços, independentemente de a sua entrega ou prestação ser efectuada por via electrónica;

ii. À distância: sem que as partes estejam simultaneamente presentes;

iii. Por via electrónica: enviado da origem e recebido no destino através de meios electrónicos de processamento e de armazenamento de dados, incluindo a via informática, o cabo, rádio, meios ópticos e meios electromagnéticos, excluindo o telefone, telecópia, telex e teletexto televisivo.

iv. Pedido individual do destinatário: a solicitação do destinatário para que lhe seja prestado um serviço da sociedade da informação, incluindo o mero acesso ao sítio/página do prestador do serviço da sociedade da informação.

v. Não são serviços da sociedade da informação:

i) Serviços de radiodifusão televisiva e sonora;

ii) Distribuição automática de notas e bilhetes;

iii) Acesso às redes rodoviárias, parques de estacionamento, etc., mediante pagamento, mesmo que existam dispositivos electrónicos à entrada e ou à saída para controlar o acesso ou garantir o correcto pagamento.

ll) **Serviço de comunicações electrónicas**: o serviço oferecido em geral mediante remuneração que consiste total ou principalmente no envio de sinais através de sistemas de comunicações electrónicas,

incluindo os serviços de telecomunicações e os serviços de transmissão em redes utilizadas para a radiodifusão;

mm) **Serviço protegido**: qualquer serviço de radiodifusão ou da sociedade da informação, desde que prestado mediante remuneração e com base em acesso condicional, ou o fornecimento de acesso condicional aos referidos serviços considerado como um serviço em si mesmo;

nn) **Serviço telefónico**: qualquer um dos seguintes serviços:

i. Os serviços de chamada, incluindo as chamadas vocais, o correio vocal, a teleconferência ou a transmissão de dados;

ii. Os serviços suplementares, incluindo o reencaminhamento e a transferência de chamadas; e

iii. Os serviços de mensagens e multimédia, incluindo os serviços de mensagens curtas (SMS), os serviços de mensagens melhoradas (EMS) e os serviços multimédia (MMS).

oo) **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. Esta definição inclui mas não se limita a sistemas informáticos, de comunicações electrónicas, de radiodifusão e telemáticos;

pp) **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;

qq) **Sistema de comunicações electrónicas**: a rede de comunicações electrónicas e qualquer dispositivo ou conjunto de dispositivos que permitem a transmissão de sinais por meio óptico, celular, radioeléctrico, electromagnético ou através de qualquer outra plataforma;

rr) **Sistema telemático**: a combinação de sistemas informáticos e de comunicações electrónicas;

ss) **Topografia de um produto semicondutor**: conjunto de imagens relacionadas, quer fixas quer codificadas, que representem a disposição tridimensional das camadas de que o produto se compõe, em que cada imagem possua a disposição, ou parte da disposição, de uma superfície do mesmo produto, em qualquer fase do seu fabrico;

tt) **Valor elevado**: o que exceda o equivalente em moeda nacional à USD 10.000,00 avaliados no momento da prática do facto;

uu) **Valor consideravelmente elevado**: o que exceda o equivalente em moeda nacional à USD 40.000 avaliados no momento da prática do facto.

Artigo 5.º

(Direito subsidiário)

Em tudo o que não contrarie o disposto na presente lei, aplicam-se aos crimes e às medidas processuais nela previstos, respectivamente, o disposto no Código Penal e no Código de Processo Penal e respectiva legislação complementar.

CAPÍTULO II

DOS CRIMES

Secção I

Crimes praticados contra sistemas de informação

Artigo 6.º

(Acesso ilegítimo)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder à totalidade ou a parte de um sistema de informação, é punido com pena de prisão de três dias a dois anos ou com pena de multa correspondente.
2. A pena é de prisão de dois a oito anos ou multa correspondente se o acesso for conseguido através de violação de regras de segurança ou se o acesso tiver sido efectuado a um serviço protegido.

3. Aplica-se também a pena referida no número anterior quando:
   a) Através do acesso, o agente tomar conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou
   b) O benefício ou vantagem patrimonial obtidos forem de valor elevado.
4. A tentativa é punível.
5. Nos casos previstos nos números 1, 2 e 3 o procedimento penal depende de queixa, salvo se os crimes forem praticados no âmbito de uma organização criminosa ou terrorista.

Artigo 7.º

(Intercepção ilegítima)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar ou registar transmissões não públicas de dados que se processam no interior de um sistema de informação, a ele destinadas ou dele provenientes, é punido com pena de prisão de três meses à dois anos ou com pena de multa correspondente.
2. O disposto no nº anterior aplica-se igualmente a quem, sem consentimento, abrir mensagem de correio electrónico que não lhe

seja dirigida ou tomar conhecimento, por processos técnicos, do seu conteúdo ou, por qualquer modo, impedir que seja recebido pelo destinatário.

3. A pena é de prisão de dois a oito anos ou multa correspondente se a intercepção for efectuada através de violação de regras de segurança ou a um serviço protegido.
4. É punido com pena de prisão de oito a doze anos o agente que, sem consentimento e com intenção de devassar ou perturbar a paz e o sossego ou a vida pessoal, familiar ou sexual de outra pessoa:
   a) Tome conhecimento de informação privada ou confidencial interceptada ou registada; ou
   b) Transmite ou divulgue os dados interceptados.
5. As penas previstas nos números anteriores são agravadas em um terço nos seus limites mínimo e máximo, se o facto for praticado com intenção de obter recompensa para o agente ou para outra pessoa ou de prejudicar alguém.
6. A pena é agravada em um terço nos seus limites mínimo e máximo, se o facto for praticado por funcionário público no exercício das suas funções.
7. A tentativa é punível.
8. O procedimento penal depende de queixa, salvo se os crimes forem praticados no âmbito de uma organização criminosa ou terrorista.

Artigo 8.º

(Sabotagem informática)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, alterar, danificar, entravar, impedir, interromper, destruir, no todo ou em parte, perturbar gravemente o funcionamento de um sistema de informação ou lhe afectar a capacidade de uso, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de dados ou através de qualquer outra forma de interferência em sistema de informação, é punido com pena de prisão de 3 meses a dois anos ou com pena de multa correspondente.
2. No caso descrito no número anterior, a pena é de:
   a) Prisão de três meses a dois anos ou pena de multa correspondente agravada ao triplo nos seus limites mínimo e máximo, se o valor do prejuízo for elevado;
   b) Prisão de dois a oito anos ou pena de multa correspondente agravada ao triplo nos seus limites mínimo e máximo, se o prejuízo for consideravelmente elevado;
   c) Prisão de oito a doze anos ou pena de multa correspondente agravada ao triplo nos seus limites mínimo e máximo, se a per-

turbação causada atingir de forma grave ou duradoura um sistema de informação que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos, como sejam os serviços de água, energia eléctrica e as comunicações electrónicas.

3. A tentativa é punível.

Artigo 9.º

(Burla informática e nas comunicações)

1. Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial:
   a) Interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa de computador, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento;
   b) Usando programas, dispositivos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou

impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de comunicações electrónicas;

É punido com pena de prisão três meses a dois anos ou com pena de multa de correspondente.

2. No caso previsto no número anterior, a pena é de:
   a) Prisão de dois a oito anos ou com pena ou com multa correspondente, se o valor do prejuízo for elevado;
   b) Prisão de oito a doze anos ou com pena de multa correspondente, se o prejuízo for consideravelmente elevado.
3. O procedimento criminal depende de queixa, salvo se o crime for praticado no âmbito de uma organização criminosa ou terrorista ou contra uma instituição pública.
4. A tentativa é punível.

Secção II

Crimes praticados contra dados

Artigo 10.º

(Falsidade informática)

1. Quem, com intenção de enganar, introduzir, alterar, eliminar ou suprimir dados em sistema de informação ou por qualquer outra

forma interferir num tratamento de dados, produzindo dados falsos com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem verdadeiros, é punido com pena de prisão de dois a oito anos ou com pena de multa correspondente.

2. Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações electrónicas ou a serviço de acesso condicional, a pena é de oito a doze anos de prisão.
3. Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, utilizar os dados que foram objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no n.º 2, é punido com as penas previstas num e noutro número, respectivamente.
4. Se o autor dos factos descritos nos números anteriores for funcionário público no exercício das suas funções, a pena é de prisão de oito a doze anos ou com pena de multa correspondente.
5. A tentativa é punível.

Artigo 11.º

(Dano relativo a dados)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema de informação ou de parte dele, alterar, danificar, deteriorar, eliminar, suprimir ou destruir, no todo ou em parte, ou tornar não utilizáveis ou não acessíveis dados alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão de dois a oito anos ou pena de multa correspondente.
2. No caso descrito no número anterior, a pena é de:
   a) Prisão de dois a oito anos ou pena de multa correspondente, se o valor do prejuízo for elevado;
   b) Prisão de oito a doze anos ou pena de multa correspondente, se o prejuízo for consideravelmente elevado;
3. A tentativa é punível.
4. Nos casos previstos nos nºs 1, 2 a) e 3, o procedimento penal depende de queixa, salvo se os crimes forem praticados no âmbito de uma organização criminosa ou terrorista.

Secção III

Crimes praticados por intermédio de sistemas de informação

Artigo 12.º

(Pornografia infantil)

1. Quem:
   a) Produzir pornografia infantil para ser difundida através de um sistema de informação;
   b) Oferecer, transmitir ou disponibilizar pornografia infantil através de um sistema de informação; ou
   c) Difundir pornografia infantil através de um sistema de informação;

   É punido com pena de prisão de três meses a dois anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.

2. Se, no caso do número anterior, a vítima for menor de 14 anos, a pena é de prisão de dois a oito anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.
3. Quem praticar os actos descritos no n.º 1 utilizando material pornográfico simulado ou manipulado de menor não existente é puni-

do com pena de prisão de três meses a dois anos e multa correspondente.

4. Quem praticar os actos descritos no n.º 1 com intenção lucrativa é punido com pena de prisão de dois a oito anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.
5. Quem praticar os actos descritos no n.º 2 com intenção lucrativa é punido com pena de prisão de oito a doze anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.
6. Quem adquirir os materiais previstos no n.º 1 através de um sistema de informação ou tiver na sua posse os referidos materiais num sistema de informação ou num dispositivo de armazenamento de dados informáticos, é punido com pena de prisão de três dias a dois anos ou com pena de multa correspondente.
7. A tentativa é punível.

Artigo 13.º

(Fraude, assédio e exibicionismo sexual)

1. Quem:
   a) Se aproveitar do erro de outra pessoa sobre a sua identidade pessoal ou a induzir em erro, para praticar com ela acto sexual,

quando esse erro é facilitado pelo recurso a sistemas de informação; ou

b) Constranger outra pessoa a sofrer ou a praticar um acto sexual, consigo ou com outrem, por via de ordens, ameaças e coacções efectuadas através de um sistema de informação de tal forma que, atentas as circunstâncias do caso, a infracção não seria praticada ou é facilitada pelo recurso a sistemas de informação;

É punido com pena de prisão de três dias a dois anos ou com pena de multa correspondente.

2. Quem importunar outra pessoa através do envio ou disponibilização, em sistemas de informação, de conteúdos que representem actos de exibicionismo sexual, é punido com pena de prisão de dois a oito anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.
3. O procedimento criminal depende de queixa.
4. Se a vítima do crime for menor de 18 anos, as penas são agravadas em um terço nos seus limites mínimo e máximo.

Artigo 14.º

(Ameaça e coacção)

Quem praticar os crimes de ameaça e coacção através de um sistema de informação de tal forma que, atentas as circunstâncias do caso, a infracção não seria praticada ou é facilitada pelo recurso a sistemas de informação, é punido com pena de prisão de três dias a dois anos ou com pena de multa correspondente.

Artigo 15.º

(Difamação, injúria e calúnia)

Quem praticar os crimes de difamação, injúria ou calúnia através de um sistema de informação é punido com as penas previstas no Código Penal, elevadas de um terço dos seus limites, mínimos e máximos.

Artigo 16.º

(Gravações, fotografias e filmes ilícitos)

1. Quem, sem consentimento, oferecer, transmitir, disponibilizar ou difundir gravações, filmes e fotografias de outra pessoa, mesmo quando licitamente produzidos, através de um sistema de informação, é punido com pena de prisão de dois a oito anos ou com pena de multa correspondente.

2. A pena estabelecida no número anterior é agravada em um terço nos seus limites mínimo e máximo se o facto for praticado com intenção de obter recompensa para o agente ou para outra pessoa ou de prejudicar alguém, ou se as gravações, filmes ou fotografias respeitarem à vida pessoal, familiar ou sexual de uma pessoa.
3. O procedimento criminal depende de queixa.
4. A tentativa é punível.

Artigo 17.º

(Mensagens electrónicas)

1. Quem, sem consentimento e com a intenção de devassar ou perturbar a paz e o sossego ou a vida pessoal, familiar ou sexual de outra pessoa, enviar mensagens por vias de sistemas de informação, é punido com pena de prisão de dois a oito anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.
2. A pena é agravada em um terço nos seus limites mínimo e máximo se o facto for praticado com intenção de obter recompensa para o agente ou para outra pessoa ou de prejudicar alguém.

Artigo 18.º

(Atentado contra a segurança de serviços de utilidade pública)

Quem, mediante recurso a sistema de informação, atentar contra a segurança ou funcionamento de serviços destinados a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos, como sejam os serviços de água, energia eléctrica e as comunicações electrónicas, é punido com pena de prisão de oito a doze anos.

Artigo 19.º

(Instigação e apologia pública do crime)

1. Quem incitar directamente e de forma pública à prática de um crime determinado através de um sistema de informação é punido com pena de prisão de três dias a dois anos ou com pena de multa de correspondente.
2. Quem, publicamente e através de um sistema de informação, enaltecer, louvar ou recompensar o agente de determinado crime, criando o perigo de que outro crime da mesma espécie seja prati-

cado, é punido com pena de prisão de dois a oito anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.

3. Se das condutas descritas nos números anteriores resultar a prática do crime, o agente é punido como cúmplice do crime praticado.
4. A pena não pode em caso algum ser superior à cominada para o crime objecto da instigação.

Artigo 20.º

(Representação de violência)

1. Quem criar, produzir, distribuir, difundir, oferecer, mostrar ou tornar acessível, através de um sistema de informação, registos sonoros ou visuais, imagens ou outros que façam insistentemente a apologia de actos de violência ou crueldade, com a finalidade de promover os mesmos, é punido com pena de prisão de três dias a dois anos ou com pena de multa correspondente.
2. Se o agente actuar com propósito lucrativo, a pena é de prisão de dois a oito anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.

Artigo 21.º

(Incitamento à discriminação)

1. Quem:
   a) Produzir conteúdos discriminatórios para serem difundidos através de um sistema de informação;
   b) Oferecer, transmitir ou disponibilizar conteúdos discriminatórios através de um sistema de informação; ou
   c) Difundir conteúdos discriminatórios através de um sistema de informação;

   É punido com pena de prisão de 3 dias a dois anos ou com pena de multa correspondente.

2. Quem adquirir ou detiver os materiais previstos no n.º 1 é punido com pena de prisão de dois a oito anos ou com pena de multa correspondente.
3. A tentativa é punível.

Artigo 22.º

(Incitamento ao ódio e apologia da guerra)

1. Quem, reiterada e publicamente, recorrendo a sistemas de informação em circunstâncias tais que facilitem ou promovam a sua divulgação:
   a) Incitar ao ódio contra um povo, grupo nacional, étnico, racial ou religioso, com o propósito de desencadear uma guerra ou de o destruir, total ou parcialmente;
   b) Fizer apologia da guerra contra um Estado ou contra um povo,

   É punido com pena de prisão de dois a oito anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.
2. Se alguma guerra vier a ser desencadeada na sequência dos actos indicados no número anterior, a pena de prisão será de oito a doze anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.

Artigo 23.º

(Terrorismo)

1. Quem, por intermédio de sistema de informação, difundir informações com intenção de prejudicar a integridade ou a independência

nacional, de destruir, alterar ou subverter o funcionamento das instituições do Estado, de forçar as autoridades a praticar determinados actos, a abster-se de os praticar ou a tolerar que sejam praticados, cometer determinado acto ilícito, é punido com a pena de prisão de doze a dezasseis anos e multa até 360 dias.

2. A pena estabelecida no número anterior é ainda agravada de um terço, nos respectivos limites mínimo e máximo se o agente for dirigente de uma organização terrorista e de um quarto se apenas for seu membro ou colaborador.

Artigo 24.º

(Espionagem)

1. Quem, por intermédio de sistema de informação, procurar aceder à informação classificada no âmbito do regime do segredo de Estado para a revelar ou auxiliar outrem a fazê-lo é punido com a pena de prisão de oito a doze anos.
2. Se o facto for praticado em colaboração com governo, associação, organização, serviços de inteligência estrangeiros ou agente seu, a pena é de prisão de doze a dezasseis anos.

3. Se o agente praticar um dos factos descritos nos números anteriores, com violação de dever específico imposto pelo estatuto da sua função, serviço ou missão que lhe tenha sido legalmente confiado é punido com as mesmas penas, agravadas de um terço dos seus respectivos limites mínimo e máximo.
4. Se a actividade do agente não tiver por objecto o segredo do Estado, mas, ainda assim, a recolha de informação puser em perigo a segurança do Estado, a pena é de oito a doze anos.
5. Se o facto descrito no número anterior for praticado em colaboração com entidades referidas no nº2 ou em seu benefício a pena é de prisão de doze a dezasseis anos.

Secção IV

Outros crimes relacionados com a sociedade da informação

Artigo 25.º

(Tutela penal dos programas de computador)

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 de dois a oito anos e

multa correspondente agravada ao triplo nos seus limites mínimo e máximo.

2. Em caso de reprodução não autorizada, são apreendidas as cópias ilícitas de programas de computador, podendo igualmente ser apreendidos dispositivos em comercialização que tenham por finalidade exclusiva facilitar a supressão não autorizada ou a neutralização de qualquer salvaguarda técnica eventualmente colocada para proteger um programa de computador.
3. O destino dos objectos apreendidos é determinado na sentença final.
4. A tentativa é punível.

Artigo 26.º

(Tutela penal das topografias dos produtos semicondutores)

1. Quem ilegitimamente reproduzir, distribuir, comunicar ao público ou colocar à disposição do público uma topografia de um produto semicondutor ou um produto semicondutor fabricado a partir dessa topografia, é punido com pena de prisão de três dias a dois anos ou com pena de multa correspondente.
2. A tentativa é punível.

Artigo 27.º

(Tutela penal das bases de dados)

1. 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 de três dias a dois anos ou com pena de multa correspondente.
2. Quem, não estando para tanto autorizado, proceder à extracção ou reutilização de uma base de dados protegida pelo direito *sui generis* em violação do disposto no Regulamento das Tecnologias e dos Serviços da Sociedade da Informação, é punido com uma pena de dois a oito anos e multa correspondente agravada ao triplo nos seus limites mínimo e máximo.
3. Podem ser apreendidas, nos termos dos procedimentos cautelares, as cópias ilícitas de bases de dados.
4. Podem igualmente ser objecto de apreensão os dispositivos em comercialização que tenham por finalidade exclusiva facilitar a supressão não autorizada ou a neutralização de qualquer salvaguarda técnica eventualmente colocada para proteger uma base de dados.
5. O destino dos objectos apreendidos é determinado na sentença final.
6. A tentativa é punível.

Artigo 28.º

(Neutralização de medidas eficazes de carácter tecnológico)

1. Quem, não estando autorizado, neutralizar qualquer medida eficaz de carácter tecnológico, sabendo isso ou tendo motivos razoáveis para o saber, é punido com pena de prisão de três dias a dois anos ou com pena de multa correspondente.
2. A tentativa é punível.
3. Quem, não estando autorizado, proceder ao fabrico, importação, distribuição, venda, aluguer, publicidade para venda ou aluguer, ou tiver a posse para fins comerciais de dispositivos, produtos ou componentes ou ainda preste serviços que:
   a) Sejam promovidos, publicitados ou comercializados para neutralizar a protecção de uma medida eficaz de carácter tecnológico, ou
   b) Só tenham limitada finalidade comercial ou utilização para além da neutralização da protecção da medida eficaz de carácter tecnológico; ou
   c) Sejam essencialmente concebidos, produzidos, adaptados ou executados com o objectivo de permitir ou facilitar a neutralização da protecção de medidas de carácter tecnológico eficazes;

4. É punido com pena de prisão de dois a oito anos ou multa correspondente agravada ao triplo nos seus limites mínimo e máximo.

Artigo 29.º

(Informação para a gestão electrónica de direitos)

1. Quem, não estando autorizado, intencionalmente, sabendo ou tendo motivos razoáveis para o saber, pratique um dos seguintes actos:
   a) Suprima ou altere qualquer informação para a gestão electrónica de direitos;
   b) Distribua, importe para distribuição, emita por radiodifusão, comunique ou ponha à disposição do público obras, prestações ou produções protegidas, das quais tenha sido suprimida ou alterada, sem autorização, a informação para a gestão electrónica dos direitos, sabendo que em qualquer das situações indicadas está a provocar, permitir, facilitar ou dissimular a violação de direitos de propriedade intelectual;

   É punido com pena de prisão de três meses a dois anos ou com pena de multa correspondente.
2. A tentativa é punível.

Secção V

Dispositivos ilícitos e códigos de acesso

Artigo 30.º

(Dispositivos ilícitos e códigos de acesso)

1. Quem ilegitimamente produzir, importar, vender, distribuir, detiver para fins comerciais ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas de informação dispositivos ou códigos de acesso concebidos ou adaptados para permitir a prática das acções não autorizadas descritas nos artigos 6.º a 10.º é punido com as seguintes penas:
   a) Prisão de dois a oito anos ou de multa correspondente para os crimes previstos no artigo 6.º, sem prejuízo do número 2 seguinte;
   b) Prisão de dois a oito ou de multa correspondente agravada ao triplo nos seus limites mínimo e máximo para os crimes previstos no artigo 7.º;
   c) Prisão de oito a doze anos ou de multa corresponde para os crimes previstos no artigo 8.º;
   d) Prisão de dois a oito anos para os crimes previstos no artigo 9.º.

e) Prisão de dois a oito anos para os crimes previstos no artigo 10.º;

f) Prisão de dois a oito anos ou de multa correspondente para os crimes previstos no artigo 11.º.

2. É punido com pena de prisão até dois anos ou com pena de multa correspondente:

a) A utilização de comunicações comerciais para a promoção de dispositivos para a prática do crime constante do artigo 7.º;

b) A realização de acções ou quaisquer actividades com a finalidade de promover dispositivos concebidos ou adaptados para a prática do crime constante do artigo 7.º.

3. É punido com pena de prisão de oito a doze anos ou de multa correspondente a prática das seguintes actividades com o objectivo de permitir o acesso, sob forma inteligível, a um serviço protegido:

a) Fabrico, importação, distribuição, venda, locação ou detenção, para fins comerciais, de dispositivos ou códigos de acesso;

b) Instalação, manutenção ou substituição, para fins comerciais, de dispositivos ou códigos de acesso;

c) Utilização de comunicações comerciais para a promoção de dispositivos ou códigos de acesso;

d) Aquisição, utilização, propriedade ou mera detenção, a qualquer título, de dispositivos ou códigos de acesso para fins privados do

adquirente, do utilizador, do proprietário ou do detentor, bem como de terceiro.

4. A tentativa é punível.
5. O procedimento criminal depende de queixa, salvo se os crimes forem praticados no âmbito de uma organização criminosa ou terrorista.
6. A pena é agravada para o dobro dos seus respectivos limites quando o crime:
   e) For cometido através de violação de regras técnicas de segurança;
   f) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais;
   g) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.
7. Não é ilícita a produção, importação, venda, distribuição ou qualquer outra forma de disseminação de dispositivos ou códigos de acesso:
   a) Concebidos ou adaptados para efeitos de ensino, de investigação, de realização de testes autorizados ou de protecção de um sistema de informação, quando tal seja feito sem intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo;

b) Autorizada mediante acto próprio do titular do departamento ministerial que tutela as telecomunicações e tecnologias de informação, ouvido o Conselho das Telecomunicações e Tecnologias de Informação.

CAPÍTULO III

DAS PENAS

Secção I

Disposições comuns

Artigo 31.º

(Disposição geral)

São aplicáveis as penas e as medidas de segurança constantes do Código Penal, com as especificidades previstas nos artigos seguintes.

Secção II

Penas principais

Artigo 32.º

(Penas principais aplicáveis a pessoas singulares)

Pelos crimes previstos na presente lei são aplicáveis às pessoas singulares as penas principais de prisão ou de multa indicados nos artigos respectivos.

Artigo 33.º

(Penas principais aplicáveis a pessoas colectivas e equiparadas)

1. Pelos crimes previstos na presente lei são aplicáveis às pessoas colectivas e entidades equiparadas as penas principais de multa ou de dissolução.
2. Aplicam-se os seguintes princípios à pena de multa:
   a) Sempre que a pena aplicável às pessoas singulares for fixada em dias de prisão, a cada mês de prisão corresponde 90 dias de multa para as pessoas colectivas, calculando-se os limites mínimo e máximo da pena de multa tendo como referência a pena de prisão prevista para as pessoas singulares;
   b) Sempre que a pena aplicável às pessoas singulares estiver determinada exclusiva ou alternativamente em multa, são aplicáveis às pessoas colectivas ou entidades equiparadas os mesmos dias de multa, correspondendo a cada dia de multa uma quantia entre o equivalente, em moeda nacional, a USD 5,00 e a USD 5000,00, que o tribunal fixa em função da situação económica e financeira do condenado e dos seus encargos com os trabalhadores;
   c) Findo o prazo de pagamento da multa ou de alguma das suas prestações sem que o pagamento esteja efectuado, procede-se

à execução do património da pessoa colectiva ou entidade equiparada;

d) A multa que não for voluntária ou coercivamente paga não pode ser convertida em prisão subsidiária.

3. A pena de dissolução é decretada pelo tribunal quando a pessoa colectiva ou entidade equiparada tiver sido criada com a intenção exclusiva ou predominante de praticar os crimes indicados na presente lei ou quando a prática reiterada de tais crimes mostre que a pessoa colectiva ou entidade equiparada está a ser utilizada, exclusiva ou predominantemente, para esse efeito, por quem nela ocupe uma posição de liderança.

Artigo 34.º

(Admoestação)

1. Se ao agente, pessoa colectiva ou entidade equiparada, dever ser aplicada pena de multa em medida não superior a 120 dias, pode o tribunal limitar-se a proferir uma admoestação.
2. A admoestação só tem lugar se o dano tiver sido reparado e o tribunal concluir que, por aquele meio, se realizam de forma adequada e suficiente as finalidades da punição.

3. Em regra, a admoestação não é aplicada se o agente, pessoa colectiva ou entidade equiparada, nos três anos anteriores ao facto, tiver sido condenado em qualquer pena, incluída a de admoestação.
4. A admoestação consiste numa solene censura oral feita pelo tribunal em audiência ao agente, ou, no caso de pessoa colectiva ou entidade equiparada, ao representante legal da pessoa colectiva ou entidade equiparada ou, na sua falta, a outra pessoa que nela ocupe uma posição de liderança.

Artigo 35.º

(Caução de boa conduta)

1. Se à pessoa colectiva ou entidade equiparada dever ser aplicada pena de multa em medida não superior a cento e vinte dias, pode o tribunal substituí-la por caução de boa conduta, entre o equivalente, em moeda nacional, a USD 10.000,00 e USD 100.000,00, por um período entre seis meses e dois anos.

2. A caução é declarada perdida a favor do Estado se a pessoa colectiva ou entidade equiparada praticar novo crime pelo qual venha a ser condenada no decurso do prazo, sendo-lhe restituída no caso contrário.

3. A caução pode ser prestada por meio de depósito, penhor, hipoteca, fiança bancária ou fiança.
4. O tribunal revoga a pena de caução de boa conduta e ordena o cumprimento da pena de multa determinada na sentença se a pessoa colectiva ou entidade equiparada não prestar a caução no prazo fixado.

Artigo 36.º

(Vigilância judicial)

1. Se à pessoa colectiva ou entidade equiparada dever ser aplicada pena de multa em medida não superior a cento e vinte dias, pode o tribunal limitar-se a determinar o seu acompanhamento por um representante judicial, pelo prazo de três meses a dois anos, de modo que este proceda à fiscalização da actividade que determinou a condenação.
2. O representante judicial não tem poderes de gestão da pessoa colectiva ou entidade equiparada.
3. O representante judicial informa o tribunal da evolução da actividade da pessoa colectiva ou entidade equiparada semestralmente ou sempre que entender necessário.
4. O tribunal revoga a pena de vigilância judiciária e ordena o cumprimento da pena de multa determinada na sentença se a pessoa

colectiva ou entidade equiparada, após a condenação, cometer crime pelo qual venha a ser condenada e revelar que as finalidades da pena de vigilância judiciária não puderam, por meio dela, ser alcançadas.

Artigo 37.º

(Circunstâncias agravantes para organizações criminosas e terroristas)

1. As penas aplicáveis aos crimes indicados na presente lei são agravadas, no que diz respeito à pena de prisão, em um terço dos seus limites mínimo e máximo e, no que diz respeito à pena de multa, em triplo, quando sejam praticados no âmbito de uma organização criminosa.
2. As penas aplicáveis aos crimes indicados na presente lei são agravadas, no que diz respeito à pena de prisão, em um terço dos seus limites mínimo e máximo e, no que diz respeito à pena de multa, correspondente, quando sejam praticados no âmbito de uma organização terrorista.

Artigo 38.º

(Circunstâncias atenuantes para organizações criminosas e terroristas)

As penas previstas no artigo anterior podem ser reduzidas ou não haver lugar à punição caso o agente da infracção:

a) Renuncie voluntariamente às actividades criminosas; e
b) Afaste ou diminua consideravelmente o perigo provocado pela actividade criminosa ou forneça às autoridades competentes informações que essas autoridades não teriam podido obter de outro modo e que as ajudem a:
   i. Prevenir, fazer cessar ou limitar os efeitos da infracção;
   ii. Identificar ou levar a julgamento os demais autores da infracção;
   iii. Encontrar provas;
   iv. Privar a organização de recursos ilícitos ou do produto das suas actividades criminosas; ou
   v. Impedir a prática de outras infracções constantes da presente lei ou de outra legislação aplicável.

Artigo 39.º

(Outras circunstâncias agravantes)

1. As penas aplicáveis aos crimes indicados na presente lei são agravadas, no que diz respeito à pena de prisão, em um terço dos seus limites mínimo e máximo e, no que diz respeito à pena de multa correspondente, quando sejam praticados:
   a) Mediante a utilização de instrumentos destinados a lançar ataques que afectem um número significativo de sistemas de informação; ou

b) Mediante a dissimulação da identidade real do agente e causando prejuízo ao verdadeiro titular da identidade em causa.

2. As penas aplicáveis aos crimes indicados na presente lei são agravadas, no que diz respeito à pena de prisão, em um terço dos seus limites mínimo e máximo e, no que diz respeito à pena de multa correspondente, quando sejam praticados contra sistemas de informação ou dados dos órgãos do poder Executivo, Legislativo ou Judicial ou de outras entidades públicas da República de Angola.

Secção III

Penas acessórias

Artigo 40.º

(Penas acessórias aplicáveis a pessoas singulares)

Pelos crimes previstos na presente lei, podem ser aplicadas às pessoas singulares as seguintes penas acessórias:

a) Perda de bens;

b) Proibição do exercício de função;

c) Suspensão do exercício da função.

Artigo 41.º

(Penas acessórias aplicáveis a pessoas colectivas e equiparadas)

Pelos crimes previstos na presente lei, podem ser aplicadas às pessoas colectivas e entidades equiparadas as seguintes penas acessórias:

a) Perda de bens;
b) Injunção judiciária;
c) Interdição do exercício de actividade;
d) Proibição de celebrar certos contratos ou contratos com determinadas entidades;
e) Privação do direito a subsídios, subvenções ou incentivos;
f) Encerramento de estabelecimento;
g) Publicidade da sentença condenatória.

Artigo 42.º

(Perda de bens)

1. O tribunal pode decretar a perda a favor do Estado dos objectos, materiais, equipamentos e dispositivos que tiverem servido para a prática dos crimes previstos na presente lei e pertencerem à pessoa que tenha sido condenada pela sua prática.
2. Se o tribunal apurar que o agente adquiriu determinados bens empregando na sua aquisição dinheiro ou valores obtidos com a

prática do crime, são os mesmos também abrangidos pela decisão que decretar a perda.

Artigo 43.º

(Proibição do exercício de função)

1. O titular de cargo público, funcionário público ou agente da administração, que, no exercício da actividade para que foi eleito ou nomeado, cometer crime previsto na presente lei, pode ser também proibido do exercício daquelas funções por um período mínimo de dois meses e um máximo de dois anos quando o facto:
   a) For praticado com flagrante e grave abuso da função ou com manifesta e grave violação dos deveres que lhe são inerentes;
   b) Revelar indignidade no exercício do cargo; ou
   c) Implicar a perda da confiança necessária ao exercício da função.
2. O disposto no número anterior é correspondentemente aplicável às profissões ou actividades cujo exercício depender de título público ou de autorização ou homologação da autoridade pública.

Artigo 44.º

(Suspensão do exercício de função)

1. O titular de cargo público, funcionário público ou agente da administração, que, no exercício da actividade para que foi eleito ou

nomeado, cometer crime previsto na presente lei e for definitivamente condenado a pena de prisão, incorre na suspensão da função enquanto durar o cumprimento da pena se não for demitido disciplinarmente de função pública que desempenhe.

2. O disposto no número anterior é correspondentemente aplicável a profissões ou actividades cujo exercício depender de título público ou de autorização ou homologação da autoridade pública.

Artigo 45.º

(Efeitos da proibição e suspensão do exercício de função)

1. Salvo disposição em contrário, a proibição e a suspensão do exercício de função pública determinam a perda dos direitos e regalias atribuídos ao titular, funcionário ou agente, pelo tempo correspondente.
2. A proibição do exercício de função pública não impossibilita o titular, funcionário ou agente de ser nomeado para cargo ou para função que possam ser exercidos sem as condições de dignidade e confiança que o cargo ou a função de cujo exercício foi proibido exigem.
3. O disposto nos números anteriores é correspondentemente aplicável a profissões ou actividades cujo exercício depender de título público ou de autorização ou homologação da autoridade pública.

Artigo 46.º

(Injunção judiciária)

1. O tribunal pode ordenar à pessoa colectiva ou entidade equiparada que adopte certas providências, designadamente as que forem necessárias para cessar a actividade ilícita ou evitar as suas consequências.
2. O tribunal determina o prazo em que a injunção deve ser cumprida a partir do trânsito em julgado da sentença.

Artigo 47.º

(Proibição de celebrar contratos)

A proibição de celebrar certos contratos ou contratos com determinadas entidades é aplicável, pelo prazo mínimo de um mês e um máximo de um ano, a pessoa colectiva ou entidade equiparada.

Artigo 48.º

(Privação do direito a subsídios, subvenções ou incentivos)

A privação do direito a subsídios, subvenções ou incentivos outorgados pelo Estado e demais pessoas colectivas públicas é aplicável, pelo prazo de dois meses a dois anos, a pessoa colectiva ou entidade equiparada.

Artigo 49.º

(Interdição do exercício de actividade)

1. A interdição do exercício de certas actividades pode ser ordenada pelo tribunal, pelo prazo de seis meses a um ano, quando o crime tiver sido cometido no exercício dessas actividades.
2. Quando a pessoa colectiva ou entidade equiparada cometer crime punido com pena de multa superior a trinta dias, o tribunal pode determinar a interdição definitiva de certas actividades.
3. No caso previsto no número anterior, o tribunal pode reabilitar a pessoa colectiva ou entidade equiparada se esta se tiver conduzido, por um período de dois anos depois de cumprida a pena principal, de forma que torne razoável supor que não comete novos crimes.

Artigo 50.º

(Encerramento do estabelecimento)

1. O encerramento temporário do estabelecimento pode ser ordenado pelo tribunal, pelo prazo mínimo de um mês e o máximo de um ano, quando a infracção tiver sido cometida no âmbito da respectiva actividade.
2. Quando a pessoa colectiva ou entidade equiparada cometer crime punido com pena de multa superior a duzentos e quarenta dias, o

tribunal pode determinar o encerramento definitivo do estabelecimento.

3. No caso previsto no número anterior, o tribunal pode reabilitar a pessoa colectiva ou entidade equiparada e autorizar a reabertura do estabelecimento se esta se tiver conduzido, por um período de dois anos depois de cumprida a pena principal, de forma que torne razoável supor que não comete novos crimes.
4. Não obsta à aplicação da pena de encerramento a transmissão do estabelecimento ou a cedência de direitos de qualquer natureza, relacionadas com o exercício da actividade, efectuadas depois da instauração do processo ou depois da prática do crime, salvo se o adquirente se encontrar de boa fé.
5. O encerramento do estabelecimento não constitui justa causa para o despedimento dos trabalhadores nem fundamento para a suspensão ou redução do pagamento das respectivas remunerações.

Artigo 51.º

(Publicidade da decisão condenatória)

1. A decisão condenatória é sempre publicada nos casos em que sejam aplicadas as penas de admoestação, interdição do exercício da actividade e encerramento de estabelecimento, podendo sê-lo nos restantes casos.

2. Sempre que for aplicada a pena de publicidade da decisão condenatória, esta é efectivada, a expensas da condenada, em meio de comunicação social a determinar pelo tribunal, bem como através da afixação de edital, por período não inferior a trinta dias, no próprio estabelecimento comercial ou industrial ou no local de exercício da actividade, por forma bem visível ao público.
3. A publicidade da decisão condenatória é feita por extracto, de que constam os elementos da infracção e as sanções aplicadas, bem como a identificação das pessoas colectivas ou entidades equiparadas.

CAPÍTULO IV

DOS MEIOS DE PROVA E DE OBTENÇÃO DE PROVA

Secção I

Disposições comuns

Artigo 52.º

(Disposição geral)

São admitidos todos os meios de prova e de obtenção de prova que não sejam proibidos por lei, incluindo todos aqueles que se encontram regulados no Código de Processo Penal, com as especificidades previstas nos artigos seguintes.

Artigo 53.º

(Âmbito de aplicação)

O disposto no presente Capítulo aplica-se a processos relativos a crimes:

a) Previstos na presente lei;
b) Cometidos por intermédio de um sistema de informação; ou
c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

Secção II

Preservação de dados

Artigo 54.º

(Conservação expedita de dados)

1. Se no decurso do processo for necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados específicos armazenados num sistema de informação, incluindo dados de tráfego, em relação aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a Autoridade Competente ordena a quem tenha disponibilidade ou controlo desses dados, o que inclui mas não se limita ao prestador do serviço, que preserve os dados em causa.
2. A ordem de preservação discrimina, sob pena de nulidade:

a) A natureza dos dados;
b) A sua origem e destino, se forem conhecidos; e
c) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses.

3. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à Autoridade Competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.
4. A Autoridade Competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 2, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 55.º

(Conservação expedita de dados de tráfego)

Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de entidades que nela participaram, a entidade a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à Autoridade Competente ou ao órgão de investigação e instrução criminal, logo que o

souber, outras entidades através das quais aquela comunicação tenha sido efectuada, no sentido de permitir identificar todas elas e a via através da qual aquela comunicação foi efectuada.

Secção III

Transmissão de dados

Artigo 56.º

(Injunção para apresentação ou concessão de acesso a dados)

1. Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados específicos e determinados, armazenados num determinado sistema de informação, a Autoridade Competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso ao sistema de informação onde os mesmos estão armazenados sob pena de punição por desobediência qualificada.
2. A ordem referida no número anterior identifica tanto quanto possível os dados em causa.
3. A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido no processo.

4. Não se pode igualmente fazer uso da injunção prevista neste artigo quanto a sistemas de informação utilizados para o exercício da advocacia, das actividades médica e bancária e da profissão de jornalista.
5. As seguintes pessoas podem invocar, por escrito, segredo profissional ou de funcionário ou de Estado para se escusarem ao cumprimento da injunção:
   a) Os ministros de religião ou confissão religiosa e os advogados, médicos, jornalistas, membros de instituições de crédito e as demais pessoas a quem a lei permitir ou impuser que guardem segredo, bem como os funcionários sobre factos que constituam segredo e de que tiverem tido conhecimento no exercício das suas funções, salvo se, após as averiguações necessárias, se determinar que a recusa é ilegítima ou que é injustificada, segundo o princípio da prevalência do interesse preponderante, nomeadamente tendo em conta a imprescindibilidade dos dados para a descoberta da verdade, a gravidade do crime e a necessidade de protecção de bens jurídicos;
   b) As testemunhas sobre factos que constituam segredo de Estado, desde que a recusa sejam confirmada, no prazo de 10 dias, por intermédio do Ministro da Justiça. Decorrido este prazo sem a confirmação ter sido obtida, os dados devem ser entregues.

Artigo 57.º

(Localização celular)

1. As autoridades competentes e os órgãos de polícia criminal podem obter dados sobre a localização celular quando eles forem necessários para afastar perigo para a vida ou de ofensa à integridade física grave.
2. Se os dados sobre a localização celular previstos no número anterior se referirem a um processo em curso, a sua obtenção deve ser comunicada ao juiz no prazo máximo de quarenta e oito horas.
3. Se os dados sobre a localização celular previstos no n.º 1 não se referirem a nenhum processo em curso, a comunicação deve ser dirigida ao juiz da sede da entidade competente para a investigação criminal.
4. É nula a obtenção de dados sobre a localização celular com violação do disposto nos números anteriores.

Secção IV

Busca e apreensão de dados

Artigo 58.º

(Pesquisa de dados)

1. Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados especí-

ficos e determinados, armazenados num determinado sistema de informação, a Autoridade Competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema de informação, devendo, sempre que possível, presidir à diligência.

2. O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.
3. Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema de informação, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da Autoridade Competente, nos termos dos nºs 1 e 2.
4. Quem tiver a disponibilidade ou controlo dos dados deve prestar toda a sua colaboração, facultando o que for requisitado.
5. À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal.

Artigo 59.º

(Apreensão de dados)

1. Quando, no decurso de uma pesquisa ou de outro acesso legítimo a um sistema de informação, forem encontrados, armazenados nesse

sistema de informação ou noutro a que seja permitido o acesso legítimo a partir do primeiro, dados, incluindo mensagens de correio electrónico ou outros registos de comunicações, necessários à produção de prova ou para a descoberta da verdade, a Autoridade Competente autoriza ou ordena por despacho a apreensão dos mesmos.

2. Caso sejam apreendidos dados cujo conteúdo seja susceptível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular ou de terceiro, esses dados ou documentos são, sob pena de nulidade, apresentados ao juiz, que pondera a sua junção aos autos tendo em conta os interesses do caso concreto.
3. O disposto no nº 5 do artigo 57.º é aplicável.
4. A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:
   a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura;
   b) Realização de uma cópia dos dados, em suporte autónomo, que é junto ao processo;

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou
d) Eliminação não reversível ou bloqueio do acesso aos dados.

5. No caso da apreensão efectuada nos termos da alínea b) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao magistrado competente dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital.
6. Às apreensões a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras aplicáveis às apreensões previstas no Código de Processo Penal e legislação complementar em vigor.

Secção V

Intercepção de comunicações

Artigo 60.º

(Intercepção de dados)

1. A intercepção e registo, em tempo real, de dados relativos ao conteúdo das comunicações ou apenas de dados de tráfego, incluindo de quaisquer comunicações transmitidas através de qualquer sis-

tema de informação, como seja telefone, correio electrónico ou outro, bem como os efectuados presencialmente, só podem ser autorizadas durante a instrução preparatória dos processos-crime, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho da Autoridade Competente.

2. A obtenção e junção aos autos de dados de localização ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas por despacho da Autoridade Competente.
3. A autorização a que alude o n.º 1 pode ser solicitada ao magistrado dos lugares onde eventualmente se puder efectivar a conversação ou comunicação ou da sede da entidade competente para a investigação criminal.
4. Nos casos previstos no número anterior, a autorização é levada, no prazo máximo de 72 horas, ao conhecimento do magistrado do processo, a quem cabe praticar os actos jurisdicionais subsequentes.
5. A intercepção e o registo previstos nos números anteriores só podem ser autorizados, independentemente da titularidade do meio de comunicação utilizado, contra:

a) Suspeito ou arguido;
b) Pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou
c) Vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

6. É proibida a intercepção e o registo de dados de conteúdo relativos a conversações ou comunicações entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que elas constituem objecto ou elemento de crime.
7. A intercepção e o registo de dados são autorizados pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respectivos requisitos de admissibilidade.
8. O registo dos dados só pode ser utilizado em outro processo, em curso ou a instaurar, se tiver resultado de intercepção de meio de comunicação utilizado por pessoa referida no nº 5 e na medida em que for indispensável à prova de crime relativamente ao qual a intercepção de comunicações for admissível ao abrigo desta lei.
9. Nos casos previstos no número anterior, os suportes técnicos dos dados e os despachos que fundamentaram as respectivas intercepções são juntos, mediante despacho da Autoridade Competente, ao

processo em que devam ser usados como meio de prova, sendo extraídas, se necessário, cópias para o efeito.

Artigo 61.º

(Formalidades)

1. O órgão da polícia de investigação e instrução criminal que efectuar a intercepção e o registo a que se refere o artigo anterior lavra o correspondente auto e elabora relatório no qual indica os dados relevantes para a prova, descreve de modo sucinto o respectivo conteúdo e explica o seu alcance para a descoberta da verdade.
2. O disposto no número anterior não impede que o órgão da polícia de investigação e instrução criminal que proceder à investigação tome previamente conhecimento dos dados interceptados a fim de poder praticar os actos cautelares necessários e urgentes para assegurar os meios de prova.
3. O órgão da polícia de investigação e instrução criminal referido no nº 1 leva ao conhecimento do delegado do Ministério Público, de 15 em 15 dias a partir do início da primeira intercepção efectuada no processo, os correspondentes suportes técnicos, bem como os respectivos autos e relatórios.
4. O Ministério Público leva ao conhecimento do juiz os elementos referidos no número anterior no prazo máximo de 48 horas.

5. Para se inteirar dos dados, o juiz é coadjuvado, quando entender conveniente, pelo órgão da polícia de investigação e instrução criminal e nomeia, se necessário, intérprete.
6. Sem prejuízo do disposto no nº 7 do artigo anterior, o juiz determina a destruição imediata dos suportes técnicos e relatórios manifestamente estranhos ao processo:
   a) Que disserem respeito a dados de conteúdo em que não intervenham pessoas referidas no nº 5 do artigo anterior;
   b) Que abranjam matérias cobertas pelo segredo profissional, de funcionário ou de Estado; ou
   c) Cuja divulgação possa afectar gravemente direitos, liberdades e garantias;

Ficando todos os intervenientes vinculados ao dever de segredo relativamente às conversações de que tenham tomado conhecimento.

7. Durante a instrução preparatória, a Autoridade Competente determina a transcrição e junção aos autos dos dados indispensáveis para fundamentar a aplicação de medidas de coacção ou de garantia patrimonial, à excepção do termo de identidade e residência.
8. A partir do encerramento da instrução preparatória, o assistente e o arguido podem examinar os suportes técnicos dos dados e obter, à sua custa, cópia das partes que pretendam transcrever para jun-

tar ao processo, bem como dos relatórios previstos no nº1, até ao termo dos prazos previstos para requerer a abertura da instrução ou apresentar a contestação, respectivamente.

9. Só podem valer como prova os dados que:
   a) O Ministério Público mandar transcrever ao órgão da polícia de investigação e instrução criminal que tiver efectuado a intercepção e a gravação e indicar como meio de prova na acusação;
   b) O arguido transcrever a partir das cópias previstas no número anterior e juntar ao requerimento de abertura da instrução ou à contestação; ou
   c) O assistente transcrever a partir das cópias previstas no número anterior e juntar ao processo no prazo previsto para requerer a abertura da instrução, ainda que não a requeira ou não tenha legitimidade para o efeito.
10. O Juiz pode proceder à visualização ou audição dos registos para determinar a correcção das transcrições já efectuadas ou a junção aos autos de novas transcrições, sempre que o entender necessário à descoberta da verdade e à boa decisão da causa.
11. As pessoas cujas comunicações tiverem sido escutadas, visualizadas e transcritas podem examinar os respectivos suportes técnicos até ao encerramento da audiência de julgamento.

12. Os suportes técnicos referentes a dados que não forem transcritos para servirem como meio de prova são guardados em envelope lacrado, à ordem do tribunal, e destruídos nos termos do artigo 64.º.

Artigo 62.º

(Nulidade)

Os requisitos e condições referidos nos artigos anteriores desta Secção são estabelecidos sob pena de nulidade.

Secção VI

Destruição de dados

Artigo 63.º

(Destruição de dados)

1. A destruição dos dados na posse das autoridades competentes, bem como dos dados conservados nos termos dos artigos 55.º a 56.º, é determinada oficiosamente ou a requerimento de qualquer interessado, logo que os mesmos deixem de ser estritamente necessários para os fins a que se destinam.

2. Consideram-se que os dados deixam de ser estritamente necessários para o fim a que se destinam logo que ocorra uma das seguintes circunstâncias:
   a) Arquivamento definitivo do processo criminal;
   b) Absolvição, transitada em julgado;
   c) Condenação, transitada em julgado;
   d) Prescrição do procedimento penal;
   e) Amnistia.
3. Os dados conservados nos termos do artigo 55.º apenas podem ser destruídos quando as circunstâncias indicadas no n.º 2 acima se verifiquem relativamente a todos os processos que justificaram a conservação dos dados.

Secção VII

Regras específicas aplicáveis a operadores de comunicações electrónicas acessíveis ao público e a prestadores de armazenagem principal

Artigo 64.º

(Preservação de dados)

1. Os operadores de comunicações electrónicas acessíveis ao público e os prestadores de armazenagem principal devem conservar dados

de tráfego e de localização, bem como os dados conexos para identificar o assinante ou o utilizador de um serviço de comunicações electrónicas acessível ao público ou de um serviço de armazenagem principal, quando tais dados sejam por si gerados ou tratados no território nacional e no âmbito da sua actividade, exclusivamente para fins de investigação, detecção e repressão de crimes.

2. Para efeitos do número anterior, os operadores de comunicações electrónicas acessíveis ao público devem conservar, por um período de 6 meses a contar da data da conclusão da comunicação, as seguintes categorias de dados:
   a) Dados necessários para encontrar e identificar a fonte de uma comunicação;
   b) Dados necessários para encontrar e identificar o destino de uma comunicação;
   c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;
   d) Dados necessários para identificar o tipo de comunicação;
   e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores ou o que se considera ser o seu equipamento;
   f) Dados necessários para identificar a localização do equipamento de comunicação móvel.

3. Para os efeitos do disposto na alínea a) do número anterior, os dados necessários para encontrar e identificar a fonte de uma comunicação são os seguintes:
   a) No que diz respeito às comunicações telefónicas na rede fixa e na rede móvel:
      i. O número de telefone de origem;
      ii. O nome e endereço do assinante ou do utilizador registado;
   b) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:
      i. O código de identificação atribuídos ao utilizador;
      ii. O código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública;
      iii. O nome e o endereço do assinante ou do utilizador registado a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação.
4. Para os efeitos do disposto na alínea b) do n.º 1, os dados necessários para encontrar e identificar o destino de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas na rede fixa e na rede móvel:
   i. Os números marcados e, em casos que envolvam serviços suplementares como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada;
   ii. O nome e o endereço do assinante ou do utilizador registado;
b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:
   i. O código de identificação do utilizador ou o número de telefone do destinatário pretendido ou de uma comunicação telefónica através da Internet;
   ii. Os nomes e os endereços dos subscritores ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação.

5. Para os efeitos do disposto na alínea c) do n.º 1, os dados necessários para identificar a data, a hora e a duração de uma comunicação são os seguintes:
   a) No que diz respeito às comunicações telefónicas na rede fixa e na rede móvel, a data e a hora do início e do fim da comunicação;

b) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

i. A data e a hora do início e do fim da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado;

ii. A data e a hora do início e do fim da ligação ao serviço de correio electrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário.

6. Para efeitos do disposto na alínea d) do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas na rede fixa e na rede móvel, o serviço telefónico utilizado;

b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet, o serviço de Internet utilizado.

7. Para os efeitos do disposto na alínea e) do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, são os seguintes:
   a) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino;
   b) No que diz respeito às comunicações telefónicas na rede móvel:
      i. Os números de telefone de origem e de destino;
      ii. A Identidade Internacional de Assinante Móvel (IMSI) de quem telefona;
      iii. A Identidade Internacional do Equipamento Móvel (IMEI) de quem telefona;
      iv. A IMSI do destinatário do telefonema;
      v. A IMEI do destinatário do telefonema;
      vi. No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da activação inicial do serviço e o identificador da célula a partir da qual o serviço foi activado;
   c) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

i. O número de telefone que solicita o acesso por linha telefónica;

ii. A linha de assinante digital (DSL), ou qualquer outro identificador terminal do autor da comunicação.

8. Para os efeitos do disposto na alínea f) do n.º 1, os dados necessários para identificar a localização do equipamento de comunicação móvel são os seguintes:

   a) O identificador da célula no início da comunicação;

   b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respectivos identificadores de célula durante o período em que se procede à conservação de dados.

9. O disposto nos números anteriores aplica-se também nos casos em que a comunicação não seja iniciada ou concluída no território nacional.

10. Os dados telefónicos e da Internet relativos a chamadas telefónicas falhadas devem ser conservados quando sejam gerados ou tratados, e armazenados, pelos operadores de comunicações electrónicas acessíveis ao público no contexto da oferta de serviços de comunicação.

11. Os dados relativos a chamadas não estabelecidas não são conservados.

12. Para efeitos do números1, os prestadores de armazenagem principal devem conservar, por um período de 6 meses a contar da data da conclusão do alojamento, as seguintes categorias de dados:
    a) O país de origem dos dados armazenados;
    b) O nome e o endereço do fornecedor dos dados;
    c) O endereço do protocolo IP do fornecedor dos dados;
    d) A data do início e do fim do alojamento dos dados.
13. A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo das regras aplicáveis à intercepção e gravação legais de dados.
14. Os operadores de comunicações electrónicas acessíveis ao público, bem como os prestadores de armazenagem principal, na qualidade de responsáveis pelo tratamento dos dados pessoais que conservem ao abrigo deste artigo, devem assegurar o cumprimento das obrigações impostas ao responsável pelo tratamento constantes da legislação aplicável, nomeadamente o direito de acesso e de informação aos titulares dos dados.
15. Não carece de autorização da Agência de Protecção de Dados o tratamento dos dados nos termos e para os fins da presente Secção, o qual está sujeito a mera notificação.
16. O titular dos dados não pode opor-se ao respectivo tratamento, nem à sua transmissão nos termos do artigo 67.º.

Artigo 65.º

(Condições de conservação dos dados)

1. Os operadores de comunicações electrónicas acessíveis ao público e os prestadores de armazenagem principal devem:
   a) Garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos pelo menos à mesma protecção e segurança que os dados na rede;
   b) Tomar as medidas técnicas e organizativas adequadas à protecção dos dados previstos no artigo 65.º contra a destruição acidental ou ilícita, a perda ou a alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;
   c) Tomar as medidas técnicas e organizativas adequadas para garantir que apenas os trabalhadores ou colaboradores (incluindo subcontratados) especialmente autorizados por si tenham acesso aos dados referentes às categorias previstas no artigo 65.º;
2. Verificando-se que mais do que um operador de comunicações electrónicas acessíveis ao público conserva os mesmos dados relativos à mesma comunicação, como sucede nos casos de selecção e

de pré-selecção, os referidos operadores podem definir contratualmente a quem incumbe a obrigação de conservação dos dados, devendo dar conhecimento por escrito do mesmo à Autoridade das Comunicações Electrónicas, ficando o outro operador isento da obrigação referida.

3. Os dados referentes às categorias previstas no artigo 65.º, com excepção dos dados de base, devem permanecer bloqueados desde o início da sua conservação, só sendo alvo de desbloqueio para efeitos de transmissão, nos termos da presente lei, às autoridades competentes.
4. O disposto nos números anteriores não prejudica a observação dos princípios nem o cumprimento das regras relativas à qualidade e à salvaguarda da confidencialidade e da segurança dos dados pessoais.
5. A autoridade pública competente para o controlo da aplicação do acima disposto é a Agência de Protecção de Dados.

Artigo 66.º

(Transmissão de dados)

1. A transmissão de dados conservados nos termos do artigo 65.º só pode ser autorizada por despacho fundamentado da autoridade competente, se houver razões para crer que a diligência é indispen-

sável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão da criminalidade.

2. Os operadores de comunicações electrónicas acessíveis ao público e os prestadores de armazenagem principal devem transmitir no prazo máximo de 5 dias após a recepção do despacho às autoridades competentes, os dados conservados nos termos do artigo 65.º.
3. Só pode ser autorizada a transmissão de dados relativos:
   a) Ao suspeito ou arguido;
   b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou
   c) A vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.
4. A transmissão dos dados deve ser efectuada por via electrónica e observar um grau de codificação e protecção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados.
5. As condições de transmissão dos dados por via electrónica são fixadas em diploma autónomo, podendo incluir nomeadamente a criação de plataformas web através das quais as autoridades compe-

tentes possam aceder directamente aos dados de tráfego e de localização, bem como aos dados conexos relacionados.

6. Aplica-se o disposto neste artigo à transmissão de dados de tráfego e de localização, e dos respectivos dados conexos, que sejam validamente conservados por um prazo adicional ao período de conservação, nos termos do artigo 69.º ou de acordo com outra legislação aplicável.
7. A autoridade pública competente para o controlo da aplicação do disposto no n.º 4 é a Agência de Protecção de Dados.
8. Em tudo o que não estiver regulado no presente artigo, é aplicável o disposto no artigo 57.º.
9. O disposto nos números anteriores apenas se aplica à transmissão de dados de tráfego e de localização, bem como à transmissão de dados de base que deva ser efectuada conjuntamente com aqueles dados, sendo suficiente, para a transmissão isolada de dados de base, ordem dos órgãos de polícia criminal.
10. O disposto neste artigo não prejudica a obtenção de dados sobre a localização celular nos termos e para os fins constantes do artigo 58.º.

Artigo 67.º

(Obrigação de intercepção)

1. Os operadores de comunicações electrónicas acessíveis ao público são obrigados a instalar, a expensas próprias, e a disponibilizar às Autoridades Competentes, sistemas de intercepção legal.
2. Os operadores de comunicações electrónicas acessíveis ao público devem proceder à intercepção e registo de dados quando solicitados, por despacho fundamentado da Autoridade Competente, e apenas nos casos em que a intercepção e registo sejam admissíveis nos termos dos artigos anteriores.

Artigo 68.º

(Destruição dos dados)

1. Sem prejuízo do disposto no artigo 64.º, os operadores de comunicações electrónicas acessíveis ao público devem:
   a) Destruir os dados indicados no artigo 65.º no final do período de conservação, excepto os dados que devam ser preservados por ordem das autoridades competentes;
   b) Destruir os dados que tenham sido preservados após o decurso do período de conservação, quando tal lhe seja determinado por ordem das autoridades competentes e desde que os dados em

causa não tenham sido também preservados ao abrigo de outra ordem das autoridades competentes.

2. A autoridade pública competente para o controlo da aplicação do acima disposto é a Agência de Protecção de Dados.
3. A destruição dos dados nos termos indicados no n.º 1 não prejudica a sua conservação para outros fins desde que cumpridos os requisitos constantes da lei aplicável.

Artigo 69.º

(Contravenções e multas)

1. Sem prejuízo de outras sanções que se mostrem aplicáveis, constitui contravenção punível com multa a seguir indicada, a prática dos seguintes actos:
   a) Multa de valores, em moeda nacional, equivalente de USD 75.000,00 a USD 150.000,00, em caso de não conservação das categorias dos dados previstas nas alíneas a), b) e c) do n.º 2 do artigo 65.º;
   b) Multa de valores, em moeda nacional, equivalente de USD 30.000,00 a USD 75.000,00, em caso de não conservação das categorias dos dados previstas nas alíneas d), e) e f) do n.º 2 do artigo 65.º;

c) Multa de valores, em moeda nacional, equivalente de USD 10.000,00 a USD 30.000,00 em caso de não conservação das categorias dos dados previstas no n.º 12 do artigo 65.º;

d) Multa de valores, em moeda nacional, equivalente de USD 50.000,00 a USD 200.000,00:

   i. A não transmissão dos dados às autoridades competentes, quando autorizada nos termos do disposto no artigo 67º;

   ii. O incumprimento do disposto no artigo 66º;

   iii. O incumprimento das medidas de destruição dos dados, nos termos do disposto nos artigos 64.º e 69.º.

2. Tratando-se de pessoas colectivas, as contravenções previstas no número anterior são agravadas ao triplo dos respectivos limites.

3. A determinação da medida da multa é feita em função da ilicitude concreta do facto, da culpa do agente e dos benefícios obtidos com a prática da contravenção e das exigências de prevenção.

4. Na determinação da ilicitude concreta do facto e da culpa deve atender-se, entre outras, às seguintes circunstâncias:

   a) Ao perigo ou ao dano causados;

   b) Ao carácter ocasional ou reiterado da infracção;

   c) A existência de actos de ocultação tendentes a dificultar a descoberta da infracção;

d) A existência de actos do agente destinados a, por sua livre iniciativa, a reparar os danos ou obviar os perigos causados pela infracção;

e) A intenção do agente de obter, para si ou para outrem, um benefício ilegítimo ou de causar danos.

5. Na determinação da multa aplicável são ainda ponderadas a situação económica do infractor e o volume de negócios consolidado no ano civil anterior.

6. Se o mesmo facto constituir, simultaneamente, crime e contravenção, o agente é punido sempre a título de crime.

7. As sanções aplicadas às contravenções em concurso são sempre cumuladas materialmente.

Artigo 70.º

(Aplicação das multas)

1. Compete à Agência de Protecção de Dados a instrução dos processos de contravenção.

2. A aplicação das multas previstas na presente lei compete ao Presidente da Agência de Protecção de Dados, sob prévia deliberação da Agência.

3. A deliberação da Agência de Protecção de Dados, depois de homologada pelo Presidente, constitui título executivo, no caso de não ser impugnada no prazo legal.

Artigo 71.º

(Destino das receitas cobradas)

O montante das importâncias cobradas, em resultado da aplicação das multas é distribuído da seguinte forma:

a) 30% para o Estado;

b) 30 % para o órgão regulador das comunicações electrónicas;

c) 40 % para a Agência de Protecção de Dados.

Artigo 72.º

(Direito subsidiário)

Em tudo o que não contrarie o disposto nesta Secção, é aplicável a legislação aplicável à protecção de dados pessoais.

Secção VIII

Preservação da Soberania e Integridade Nacional, Segurança do Estado e Ordem Pública

Artigo 73.º
(Preservação, busca e apreensão de dados)

1. Os órgãos de defesa e segurança, no exercício das funções de protecção da integridade territorial, da soberania nacional e da segurança do Estado angolano podem ordenar a preservação, busca e apreensão de dados, sem prévia autorização da Autoridade Competente.
2. A preservação de dados pode também ser ordenada pelos órgãos de investigação e instrução criminal mediante prévia autorização da Autoridade Competente ou quando haja urgência ou perigo de demora, devendo os mesmos, neste último caso, dar notícia imediata do facto à Autoridade Competente e transmitir-lhe um relatório no qual mencione as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas.
3. Aplica-se o disposto nos números 2 e 4 do artigo 55.º à ordem de preservação indicada, no número anterior devendo a preservação dos dados ser efectuada em cumprimento do disposto no n.º 3 do mesmo artigo.

4. Aplica-se igualmente o disposto no artigo 56.º à preservação de dados efectuada nos termos dos números 1 e 2 deste artigo.
5. Os órgãos da polícia de investigação e instrução criminal podem proceder à pesquisa de dados armazenados num determinado sistema de informação, sem prévia autorização da Autoridade Competente, quando:
   a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;
   b) Nos casos de terrorismo ou de crime organizado, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.
6. Quando o órgão da policia de investigação e instrução criminal proceder à pesquisa nos termos do número anterior:
   a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à Autoridade Competente e por esta apreciada em ordem à sua validação;
   b) Em qualquer caso, é elaborado e remetido à Autoridade Competente um relatório no qual se mencione as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas.

7. Aplica-se à busca de dados efectuados nos termos do n.º 5 anterior o disposto nos números 4 e 5 do artigo 59.º
8. Os órgãos da polícia de investigação e instrução criminal podem efectuar apreensões de dados, sem prévia autorização da Autoridade Competente, no decurso de pesquisa legitimamente ordenada e executada nos termos do artigo 60.º, n.º 1, bem como quando haja urgência ou perigo na demora.
9. As apreensões efectuadas pelo órgão de investigação e instrução criminal são sempre sujeitas a validação pela Autoridade Competente, no prazo máximo de 72 horas.
10. Aplica-se à apreensão de dados efectuada nos termos do n.º 8 acima o disposto nos números 2, 3, 4, 5 e 6 do artigo 60.º

Artigo 74.º

(Intercepção de dados)

1. Os órgãos de defesa e segurança, no exercício das funções de prevenção e repressão dos crimes contra a integridade territorial, a soberania nacional e a segurança do Estado angolano, estão isentos da autorização prévia da Autoridade Competente em matéria de intercepção de comunicações, ficando contudo vinculados ao dever de segredo relativamente aos dados de que tomem conhecimento.

2. Sem prejuízo do disposto no n.º anterior, aplica-se à intercepção de dados constante do presente artigo o disposto nos números 1 e 6 do artigo 61.º.
3. A intercepção prevista no n.º 1 deste artigo apenas pode ser efectuado contra as pessoas indicadas no n.º 5 do artigo 61.º.

Artigo 75.º

(Admissibilidade como meio de prova)

1. Os dados recolhidos ao abrigo do número 1 do artigo74.º e do número 1 do artigo75.º são admitidos como meio de prova somente mediante despacho favorável emitido para o efeito pela Autoridade Competente.
2. No caso previsto no n.º anterior, o órgão que tiver procedido à recolha dos dados deve elaborar relatório no qual indique os dados que entende relevantes para efeitos de prova, descreva de modo sucinto o respectivo conteúdo e explique o seu alcance para a descoberta da verdade, aplicando-se no caso de recolha de dados ao abrigo do artigo 75.º o disposto nos números 5 a 12 do artigo 62.º com as devidas adaptações.
3. Nos casos do artigo 75.º, aplica-se o disposto nos números 8 e 9 do artigo 61.º com as devidas adaptações, bem como o disposto no artigo 62.º.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Artigo 76.º

(Regulamentação)

A presente lei deve ser regulamentada pelo Executivo, no prazo de 120 dias contados a partir da data da sua publicação.

Artigo 77.º

(Dúvidas e omissões)

As dúvidas e omissões que resultarem da interpretação e aplicação da presente lei são resolvidas pela Assembleia Nacional.

Artigo 78.º

(Revogação)

É revogada toda a legislação que contrarie a presente lei.

Artigo 79.º

(Entrada em vigor)

A presente lei entra em vigor na data da sua publicação.

Vista e aprovada pela Assembleia Nacional, em Luanda, aos de ____ de _____ de 2011.

O Presidente da Assembleia Nacional, *António Paulo Kassoma*

Promulgado aos ____ de _____ de 2011.

Publique-se

O Presidente da República, JOSÉ EDUARDO DOS SANTOS