

**República de Moçambique**

**Assembleia da República**

Lei n.º /2023

De de

Havendo necessidade de estabelecer o regime jurídico de Crimes Cibernéticos que visa responder de forma eficaz e eficiente aos desafios da Sociedade da Informação, combater a criminalidade cibernética, com vista a garantir a segurança do cidadão, das instituições, do Estado, a protecção dos sistemas de informação, dos dados electrónicos, das redes de computadores no espaço cibernético, ao abrigo do disposto no número 1, do artigo 178, da Constituição da República, a Assembleia da República determina:

**CAPÍTULO I**

**Disposições Gerais**

ARTIGO 1

**(Objecto)**

**A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico.**

**ARTIGO 2**

**(Âmbito)**

A presente Lei aplica-se à qualquer pessoa singular, colectiva pública ou privada que cometam infracções contra a confidencialidade, integridade e disponibilidade dos sistemas, dos dados e das redes de comunicação que possam causar danos às pessoas, ao Estado, às instituições no espaço cibernético.

ARTIGO 3

**(Definições)**

Para efeitos da presente Lei, as definições dos termos e acrónimos, constam do glossário em anexo, que dela é parte integrante.

**CAPÍTULO II**

**Disposições penais materiais**

**ARTIGO 4º**

**(Acesso ilegítimo)**

*(antigo artigo 256º do Código Penal)*

*1. Quem, sem permissão legal ou sem estar autorizado pelo proprietário, ou por outro titular do direito sobre o sistema ou de parte dele, invadir um dispositivo alheio, fixo ou móvel, ligado ou não à rede de computadores, com o fim de obter informação não pública de correio ou comunicações electrónicas privadas, acesso a dados privados, segredos comerciais ou industriais, informações sigilosas ou o acesso remoto não autorizado do dispositivo, é punido com prisão de 1 a 2 anos e multa até 1 ano.*

*2. Na mesma pena incorre quem, ilegitimamente, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.*

*3. O procedimento criminal depende de queixa.*

**ARTIGO 5**

**(Intercessão ilegítima)**

1. Quem, sem permissão legal ou sem estar autorizado pelo proprietário, por outro titular do direito sobre o sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.

2. Incorre na mesma pena quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número.

**ARTIGO 6**

**(Interferência em dados)**

*(antigo artigo 337º do Código Penal)*

*1. Quem alterar, deteriorar, inutilizar, apagar, suprimir, destruir ou, de qualquer forma, alterar dados informáticos, é punido com a pena de prisão de 1 a 2 anos e multa correspondente.*

*2. A mesma pena é aplicável a quem, mediante a introdução ou transmissão de dados informáticos ou, por qualquer outra forma, instalando vulnerabilidades, interferir no funcionamento de sistema informático, causando intencionalmente dano a alguém.*

**ARTIGO 7**

**(Interferência em sistemas)**

*(antigo artigo 338º do Código Penal)*

*Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 2 anos e multa até 1 ano.*

**ARTIGO 8**

**(Uso abusivo de dispositivos)**

*(antigo artigo 339º do Código Penal, corrigindo a gralha da última linha e estendendo o seu âmbito)*

*Incorre na pena de prisão de 1 a 2 anos, quem ilegitimamente produzir, vender, distribuir, importar ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas* ***descritas nos artigos 3º a 5º desta Lei.***

**ARTIGO 9**

**(Falsidade informática)**

*(antigo artigo 336º do Código Penal)*

*1. Quem introduzir, modificar, apagar ou suprimir de forma intencional e ilegítima dados informáticos, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se o fossem, é punido com a pena de prisão de 1 a 5 anos e multa até 1 ano.*

*2. Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.*

*3. Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções previstas nos números anteriores, é punido com a pena de prisão de 2 a 8 anos.*

**ARTIGO 10**

**(Burla informática e nas comunicações)**

*(antigo artigo 289º do Código Penal)*

*1. Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizado no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.*

*2. A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.*

**ARTIGO 11**

**(Punição da tentativa)**

A tentativa de prática dos ilícitos previstos nesta lei é punida.

**ARTIGO 12**

**(Responsabilidade penal das pessoas colectivas e entidades equiparadas)**

As pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente Lei nos termos e limites do respectivo regime de responsabilização previstos no Código Penal.

**CAPÍTULO III**

**Disposições processuais**

**ARTIGO 13**

**(Âmbito de aplicação das disposições processuais)**

As disposições processuais previstas no presente capítulo aplicam-se à investigação dos crimes:

a) previstos na presente Lei;

b) cometidos por meio de um sistema informático;

c) em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

**ARTIGO 14**

**(Preservação expedita de dados)**

1. Se no decurso do processo for necessária a prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos armazenados num sistema informático, incluindo dados de tráfego, em relacção aos quais haja receio de que possam perder-se, alterar-se ou deixar de estar disponíveis, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, que preserve os dados em causa.

2. A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária.

3. A ordem de preservação discrimina, sob pena de nulidade:

a) a natureza de 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 3 meses.

4. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tenha disponibilidade ou controlo sobre esses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa, protegendo e conservando a sua integridade pelo tempo fixado, de modo a permitir à autoridade judiciária competente a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

5. A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do nº 3 do presente artigo, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

**ARTIGO 15**

**(Revelação expedita de dados de tráfego)**

Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

**ARTIGO 16**

**(Injunção para apresentação ou concessão de acesso a dados)**

1. Se no decurso do processo se tornar necessária a obtenção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.

2. A ordem referida no número anterior identifica os dados em causa.

3. Em cumprimento da ordem descrita nos n.ºs 1 e 2, do presente artigo, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados.

4. O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo de dados relativos aos seus clientes ou assinantes ou qualquer outra informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:

a) o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

b) a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou

c) qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

5. A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo, nem a pessoa que validamente possa recusar-se a depor.

6. Não pode igualmente fazer-se uso da injunção prevista neste artigo quanto a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária.

**ARTIGO 17**

**(Pesquisa de dados informáticos)**

1. Quando no decurso do processo se tornar necessário para a prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

2. O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.

3. O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:

a) a mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) nos casos de terrorismo e criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

4. Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior do presente artigo, a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação.

5. Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.ºs 1 e 2

6. À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas.

**ARTIGO 18**

**(Apreensão de dados informáticos)**

1. Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontrados dados ou documentos informáticos necessários à prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a apreensão dos mesmos.

2. O órgão de polícia criminal pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

3. Caso sejam apreendidos dados ou documentos informáticos cujo conteúdo seja susceptível de revelar dados privados ou íntimos que possam pôr em causa a privacidade do respectivo titular ou de terceiro, sob pena de nulidade, esses dados ou documentos são apresentados ao juiz, que ponderará a sua junção aos autos tendo em conta os interesses do caso concreto.

4. As apreensões efectuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.

5. 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 de dados, em suporte autónomo, que será junto ao processo;

c) preservação, por meios tecnológicos, da integridade de dados, sem realização de cópia nem remoção dos mesmos;

d) eliminação não reversível ou bloqueio do acesso aos dados.

**ARTIGO 19**

**(Intercessão de comunicações)**

1. É admissível o recurso à intercessão de comunicações em processos relativos a crimes previstos na presente Lei, bem como quanto a crimes cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 222 do Código de Processo Penal.

2. A intercessão pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho judicial especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.

3. À intercessão e registo de transmissões de dados informáticos é aplicável o regime da intercessão e gravação de conversações ou comunicações telefónicas, previsto no Código de Processo Penal.

**ARTIGO 20**

**(Acções encobertas)**

É admissível o recurso às acções encobertas previstas no artigo 227º do Código de Processo Penal na investigação dos crimes previstos na presente lei e de todos os restantes cometidos com recurso à tecnologia informática, desde que punidos com penas de prisão superior a 3 anos.

**CAPÍTULO IV**

**Cooperação internacional**

**ARTIGO 21**

**(Âmbito da cooperação internacional)**

As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte electrónico, de um crime.

**ARTIGO 22**

**(Informação espontânea)**

1. Quando, no decurso de um processo, se obtiverem informações que possam ser úteis ao início de uma investigação criminal, ou a uma investigação criminal já existente, noutro Estado, a autoridade judiciária competente comunica tais informações à Autoridade Central, que por sua vez as comunica à Autoridade Central desse outro Estado.

2. Se as exigências do caso pendente na República de Moçambique assim o determinarem, tal comunicação pode ser acompanhada de solicitação de que as mesmas permaneçam confidenciais ou apenas sejam utilizadas em determinadas condições.

3.A Autoridade Central certifica-se, previamente, junto da Autoridade Central do outro Estado, que este pode satisfazer esta solicitação, apenas sendo as informações efectivamente remetidas neste caso.

**ARTIGO 23**

**(Ponto de contacto permanente para a cooperação internacional)**

1. Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata a investigações e procedimentos respeitantes a infracções penais previstas no artigo 13.º da presente Lei, é assegurada pelo **Serviço** Nacional de Investigação Criminal- Ministério Público, a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana.

2. Este ponto de contacto pode ser contactado por outros pontos, nos termos de acordos, tratados ou convenções a que Moçambique se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciários ou policiais.

3. A assistência imediata prestada por este ponto de contacto permanente inclui:

a) a prestação de aconselhamento técnico a outros pontos de contacto;

b) a preservação expedita de dados nos casos de urgência ou perigo na demora;

c) a recolha de prova para a qual seja competente nos termos da lei processual penal, nos casos de urgência ou perigo na demora;

d) a localização de suspeitos e a prestação de informações de carácter jurídico, nos casos de urgência ou perigo na demora.

**ARTIGO 24**

**(Preservação e revelação expeditas de dados informáticos em cooperação internacional)**

1. Pode ser solicitada à República de Moçambique a preservação expedita de dados informáticos armazenados em sistema informático localizado no seu território com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos.

2. A solicitação especifica:

a) a autoridade que pede a preservação;

b) a infracção que é objecto de investigação ou procedimento criminal, bem como uma breve exposição dos factos relacionados;

c) os dados informáticos a conservar e a sua relação com a infracção;

d) todas as informações disponíveis que permitam identificar o responsável pelos dados informáticos ou a localização do sistema informático;

e) a necessidade da medida de preservação;

f) a intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação de dados.

3. Em execução de solicitação de autoridade estrangeira competente nos termos dos números anteriores, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, que os preserve.

4 - A preservação pode também ser ordenada pela entidade policial competente mediante autorização da autoridade judiciária ou quando haja urgência ou perigo na demora.

5 - A ordem de preservação especifica, sob pena de nulidade:

a) a natureza de dados;

b) se forem conhecidos, a origem e o destino dos mesmos;

c) o período de tempo pelo qual os dados devem ser preservados, até um máximo de 3 meses.

6. Em cumprimento de ordem de preservação que lhe seja dirigida, quem tem disponibilidade ou controlo desses dados, designadamente o fornecedor de serviço, preserva de imediato os dados em causa pelo período de tempo especificado, protegendo e conservando a sua integridade.

7. A autoridade judiciária competente, ou a entidade policial, pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º5 do presente artigo, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de 1 ano.

8. Quando seja apresentado o pedido de auxílio referido no n.º 1 do presente artigo a autoridade judiciária competente determina a preservação de dados até à adopção de uma decisão final sobre o pedido.

9 - Os dados preservados ao abrigo do presente artigo apenas podem ser fornecidos:

a) à autoridade judiciária competente, em execução do pedido de auxílio referido no n.º 1, nos mesmos termos em que poderiam sê -lo, em caso nacional semelhante;

b) à autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante.

10. A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efectuada, comunica-os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos.

11. O disposto nos n.ºs 1 e 2, do presente artigo aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades moçambicanas.

**ARTIGO 25**

**(Motivos de recusa)**

1. A solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando:

a) os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concessões do direito moçambicano e

b) atentar contra a soberania, segurança, ordem pública ou outros interesses da República de Moçambique, constitucionalmente definidos.

2. A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação.

**ARTIGO 26**

**(Acesso a dados informáticos em cooperação internacional)**

1. Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Moçambique, nos mesmos termos e condições em que a pesquisa e apreensão sejam admissíveis em caso nacional semelhante.

2. A autoridade judiciária competente procede com a maior rapidez possível quando existam razões para crer que os dados informáticos em causa são especialmente vulneráveis à perda ou modificação ou quando a cooperação rápida se encontre prevista em instrumento internacional aplicável.

3. O disposto no n.º 1, do presente artigo aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias moçambicanas.

**ARTIGO 27º**

**(Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento)**

As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades moçambicanas, podem:

a) aceder a dados informáticos armazenados em sistema informático localizado em Moçambique, quando publicamente disponíveis;

b) receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Moçambique, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los.

**ARTIGO 28**

**(Intercessão de comunicações electrónicas em cooperação internacional)**

A realização de intercessão de comunicações solicitada pelas competentes autoridades estrangeiras, no contexto de investigações de crimes previstos na presente lei, é efectuada nos termos descritos no Artigo 157º da Lei n.º 21/2019, de 11 de Novembro (Lei da Cooperação Jurídica e Judiciária Internacional em Matéria Penal).

**CAPÍTULO V**

**Disposições finais**

**ARTIGO 29**

**(Regime geral aplicável)**

Em tudo o que não contrarie o disposto na presente Lei, aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, aplicam-se, respectivamente, as disposições da Lei n.ᵒ 24/2019 de 24 de Dezembro, Lei de Revisão do Código Penal, da Lei n.ᵒ 25/ 2019 de 26 de Dezembro, Lei de Revisão do Código de Processo Penal e da Lei n.º 21/2019, de 11 de Novembro (Lei da Cooperação Jurídica e Judiciária em Matéria Penal).

**ARTIGO 30**

**(Revogação)**

1. São revogados os artigos 256º, 289º, 336º, 337º, 338º e 339º do Código Penal.

2. É revogado o artigo 57º da Lei n.º 4/2016, de 3 de Julho (Lei das Telecomunicações).

**ARTIGO 31º**

**(Entrada em vigor)**

A presente Lei entra em vigor 30 dias após a sua publicação.

Aprovada pela Assembleia da República, aos xx de xxxx de 2023

A Presidente da Assembleia da República, Esperança Laurinda Francisco Nhiuane Bias

XXXXX

Promulgada aos xx de xxxxxxxx de 2023

Publique-se.

O Presidente da República, Filipe Jacinto Nyusi.

XXXXX

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ANEXO

**Glossário**

A

***Sistema informático***- qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção.

***Dados informáticos*** - qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função.

***Dados de tráfego*** *-* os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.

***Crimes cibernéticos*** – qualquer actividade ilegal que envolva o uso de tecnologias de informação e comunicação, como computadores, redes de computadores, sistemas de informação, dados electrónicos, entre outros.

***Fornecedor de serviço***- qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores.