



BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

IMPrensa Nacional de Moçambique, E.P.

AVISO

A matéria a publicar no «Boletim da República» deve ser remetida em cópia devidamente autenticada, uma por cada assunto, donde conste, além das indicações necessárias para esse efeito, o averbamento seguinte, assinado e autenticado: **Para publicação no «Boletim da República».**

SUMÁRIO

Assembleia da República:

Lei n.º 13/2026:

Aprova a Lei de Segurança Cibernética.

Lei n.º 14/2026:

Aprova a Lei dos Crimes Cibernéticos.

ASSEMBLEIA DA REPÚBLICA

Lei n.º 13/2026

de 1 de Julho

Havendo necessidade de estabelecer o regime jurídico da Segurança Cibernética que visa responder de forma eficaz e eficiente aos desafios da Sociedade da Informação, bem como garantir a segurança do Estado, das instituições, do cidadão, e a protecção de sistemas de informação e Infra-estruturas Críticas 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 o regime jurídico aplicável à Segurança Cibernética, visando garantir a segurança do Estado, das instituições, do cidadão, bem como assegurar a protecção de redes de comunicação de dados, de sistemas de informação e de infra-estruturas críticas no espaço cibernético.

ARTIGO 2

(Âmbito de aplicação)

1. A presente Lei aplica-se a:

- Administração Pública;
- Sector Privado;

- Operador de Rede de Infra-estruturas críticas;
- Provedores Intermediários de Serviços;
- Provedores de Serviços Digitais;
- Operador de Rede de Serviços Essenciais;
- Provedores de Serviços de Segurança Cibernética;
- Operadores de Plataformas Digitais;
- Operadores de Comunicações Electrónicas;
- Pessoas singulares e outras entidades que utilizam redes de comunicação de dados e sistemas de informação.

2. Exceptuam-se do previsto no número 1 do presente artigo:

- as entidades da Administração Pública em acções sobre redes de comunicação de dados, sistemas de informação e infra-estruturas críticas para fins de defesa nacional, segurança interna e de Estado;
- as entidades da Administração Pública em acções sobre redes e sistemas de informação que processem informação classificada conforme a legislação aplicável.

3. Caso uma entidade se enquadre simultaneamente em mais de uma das alíneas constantes do número 1, do presente artigo, aplica-se o regime mais exigente para a segurança das redes e dos sistemas de informação.

ARTIGO 3

(Definições)

As definições dos termos e os acrónimos usados na presente Lei constam do Glossário em anexo I e II, que dela fazem parte integrante.

ARTIGO 4

(Princípios)

A presente Lei rege-se pelos seguintes princípios:

- Colaboração e cooperação – consiste no dever das partes de colaborar, cooperar e respeitar os mecanismos de funcionamento do Sistema Nacional de Segurança Cibernética, ao nível interno e internacional, de modo a garantir a transparência e eficácia na governação da Segurança Cibernética;
- Protecção dos direitos humanos – consiste na utilização segura das Tecnologias de Informação e Comunicação, de forma a garantir o pleno respeito pelos direitos humanos, incluindo o direito à liberdade de expressão e de privacidade;
- Cadeia de valor – consiste na adopção de medidas que permitam a integridade com vista a que o cidadão confie na segurança dos produtos e serviços disponibilizados com recurso a Tecnologias de Informação e Comunicação;

#	Sector	Subsector	Tipo de Entidade
3	Transportes	Transporte terrestres	Autoridades rodoviárias e ferroviárias.
			Transportadores, companhias, agentes e operadores
			Operadores de serviço de tráfego rodoviário e ferroviário
			Operadores de sistemas de transporte inteligentes.
4	Finanças	Banca	Instituições de crédito.
		Seguros	
		Bolsa e Valores	Operadores de plataformas de negociação.
5	Infra-estruturas do mercado financeiro		Contrapartes centrais.
6	Saúde	Instalações de prestação de cuidados de saúde	Prestadores de cuidados de saúde.
		Instalações de Controlo e Logística	Armazéns de Medicamentos Prestadores de serviços de distribuição de Medicamentos
7	Infra-estruturas de Telecomunicações		Operadoras de Telecomunicações
8	Infra-estruturas de Internet		Registos de nomes de domínio de topo
			Pontos de troca de tráfego (IXP).
			Prestadores de serviços de Sistema de Nomes de Domínio (Domínio .MZ)
			Provedores de Serviços de Internet
			Rede Tecnológica Privada do Estado

ASSEMBLEIA DA REPÚBLICA

Lei n.º 14/2026

de 1 de Julho

Havendo necessidade de estabelecer o regime jurídico dos crimes cibernéticos com vista a assegurar a protecção, a recolha de prova e a responsabilização criminal, visando garantir a cooperação internacional sobre a matéria, 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 no domínio dos crimes cibernéticos e da recolha de prova em suporte electrónico.

ARTIGO 2

(Âmbito de aplicação)

A presente Lei aplica-se a todas as pessoas singulares e colectivas, públicas ou privadas, que utilizam redes de comunicação de dados e sistemas de informação.

ARTIGO 3

(Definições)

As definições dos termos e expressões utilizadas na presente Lei, constam do Glossário em anexo que dela é parte integrante.

CAPÍTULO II

Disposições Penais Materiais

ARTIGO 4

(Acesso ilegítimo)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular do direito sobre o sistema ou de parte dele, se introduzir num 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 ao dispositivo é punido com pena de 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 1 do presente artigo.

3. Para efeitos do disposto nos números 1 e 2 do presente artigo, o procedimento criminal não depende de queixa, salvo quando estejam em causa dados relativos à vida privada.

ARTIGO 5

(Intercepção ilegítima)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou 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 de até 3 anos e multa de até dois anos.

2. Incorre na mesma pena quem ilegítimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos, dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número 1 do presente artigo.

ARTIGO 6

(Interferência em dados)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular sobre o sistema ou de parte dele, alterar, deteriorar, inutilizar, apagar, suprimir, destruir ou, de qualquer forma, alterar dados informáticos, é punido com pena de prisão de 1 a 2 anos e multa correspondente.

2. Quem, mediante a introdução ou transmissão de dados informáticos ou, por qualquer outra forma, instalar vulnerabilidades, interferir no funcionamento de sistema informático, causando intencionalmente dano à infra-estrutura crítica, ou interrupção de fornecimento de serviços críticos, é punido com pena de prisão de 3 anos e multa correspondente.

ARTIGO 7

(Interferência em sistemas)

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário ou por outro titular do direito sobre o sistema ou de parte dele, entrar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, eliminação, 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.

2. À mesma infracção é aplicada a pena de prisão de 3 anos e multa correspondente, se a acção for praticada contra infra-estruturas, ou serviços críticos.

3. Se da conduta resultar dano relevante, afectação de serviços essenciais ou prejuízo significativo para terceiros, o agente é punido com pena de prisão de 2 a 8 anos.

ARTIGO 8

(Uso abusivo de dispositivos)

Quem, ilegítimamente, 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 4 e 5, da presente Lei, é punido com pena de prisão de 1 a 2 anos.

ARTIGO 9

(Falsidade informática)

1. Quem introduzir, modificar, apagar ou suprimir de forma intencional e ilegítima dados informáticos, produzindo dados ou documentos falsos ou não genuínos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se o fossem, é punido com 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 número 1 do presente artigo, ou

cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número 1, do presente artigo, é punido com as penas previstas nos números 1 e 3, do presente artigo.

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 pena de prisão de 2 a 8 anos.

4. A pena referida no número 1, do presente artigo, é também aplicável a quem, com objectivo de tirar proveito, manipular, falsificar ou usar indevidamente a identidade de outrem.

5. A ocorrência de danos morais ou patrimoniais em qualquer dos casos previstos no presente artigo constitui circunstância agravante.

ARTIGO 10

(Burla informática e nas comunicações)

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

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

(Espionagem cibernética)

1. Quem aceder, ilicitamente ou sem autorização, ao sistema informático governamental para a obtenção de informações classificadas ou estratégicas, com motivações políticas, económicas ou militares, para fins de inteligência estrangeira, é punido com pena de prisão de 3 a 10 anos.

2. Quem invadir redes corporativas para apropriação de segredos industriais ou estratégias comerciais e comprometimento de infra-estruturas críticas e serviços críticos, é punido com a pena de 2 a 8 anos.

ARTIGO 12

(Terrorismo e extremismo violento cibernéticos)

1. Quem atacar ou ameaçar atacar, invadir ou ameaçar invadir, destruir ou adulterar dados ou sistemas informáticos de infra-estruturas críticas, perturbando total ou parcialmente o seu funcionamento ou o fornecimento de seus serviços, é punido com pena de prisão de 2 a 8 anos.

2. É punido com a mesma pena de prisão prevista no número 1 do presente artigo, quem mobilizar ou recrutar, produzir e difundir conteúdos, através do sistema informático, com motivações políticas, económicas e religiosas, visando causar pânico, medo ou terror.

ARTIGO 13

(Extorsão cibernética)

1. Quem ameaçar divulgar informações comprometedoras, ataques a sistemas informáticos, ou vazamento de dados pessoais no espaço digital em troca de pagamento, é punido com a pena de prisão até 2 anos e multa correspondente.

2. A infracção referida no número 1 do presente artigo é punida com a pena de prisão de até 3 anos e multa correspondente, quando a vítima se tratar de titular ou membro de órgão de soberania, membro do governo, titular de órgão público e titular de órgão de Administração da Justiça.

ARTIGO 14

(Punição da tentativa)

A tentativa de prática dos ilícitos previstos na presente Lei é punível nos termos do Código Penal.

ARTIGO 15

(Conteúdo sexual infantil no ambiente digital)

1. Quem produzir, oferecer, trocar, disponibilizar, transmitir ou publicar, por meio de sistema informático ou telemático, fotografia, vídeo ou outro registo que contenha conteúdo sexual ou pornográfico envolvendo menores de idade, é punido com uma pena de prisão de 6 meses a 1 ano e multa até 1 ano.

2. O disposto no número 1 do presente artigo, não se aplica à aquele que praticar o acto previsto, com a finalidade de comunicar às autoridades competentes sobre a ocorrência do facto.

ARTIGO 16

(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 17

(Âmbito de aplicação das disposições processuais)

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

- a) previstos na presente Lei;
- b) cometidos por meio de um sistema informático;
- c) que impliquem a recolha de prova em suporte digital.

ARTIGO 18

(Preservação expedita de dados)

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

2. A preservação pode também ser ordenada pelo órgão de investigação criminal mediante autorização prévia da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, comunicar imediatamente o facto à autoridade judiciária competente.

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

- a) a natureza dos dados;
- b) a sua origem e destino, se forem conhecidos;
- c) o prazo pelo qual os dados devem ser preservados até ao máximo de três meses.

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

5. A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c), do número 3 do presente artigo, desde que se verifiquem os respectivos requisitos de admissibilidade, até ao limite máximo de 1 ano.

ARTIGO 19

(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 18, da presente Lei, indica a autoridade judiciária ou o órgão de investigação criminal, assim que tiver conhecimento, 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 20

(Injunção para apresentação ou concessão do acesso a dados)

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

2. A ordem referida no número 1 do presente artigo deve identificar os dados em causa.

3. Em cumprimento da ordem descrita nos números 1 e 2 do presente artigo aquele que tiver disponibilidade ou controlo desses dados apresenta-os à autoridade judiciária competente ou permite, sob pena de prática do crime de 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 juntem ao processo 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 adoptadas 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;
- c) qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

5. Os pedidos referidos no número 4 do presente artigo podem ser dirigidos e enviados directamente a um prestador de serviços estrangeiro, no âmbito de tratados internacionais que vinculem Moçambique, sempre que os dados solicitados sejam necessários para a obtenção da prova de prática de crimes.

6. Do mesmo modo, a ordem descrita no presente artigo é aplicável a entidades que prestam serviços de registo de nomes de domínio a fim de identificar ou contactar o titular registado de um nome de domínio.

7. 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.

8. Não pode igualmente fazer-se uso da injunção prevista no presente artigo quanto a sistemas informáticos utilizados para o exercício da advocacia e das actividades médica e bancária.

ARTIGO 21

(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 1 do presente artigo tem um prazo de validade máximo de 30 dias, sob pena de nulidade.

3. O órgão de investigação criminal pode proceder à pesquisa, sem prévia autorização da competente 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 investigação criminal proceder à pesquisa nos termos do número 3 do presente artigo, a realização da diligência é, sob pena de nulidade, logo que seja possível comunicar à autoridade judiciária competente e por esta apreciada em ordem à sua validação.

5. Quando, no decurso da 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 judiciária competente, nos termos dos números 1 e 2, do presente artigo.

6. À pesquisa a que se refere o presente artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas, nos termos do Código de Processo Penal.

ARTIGO 22

(Apreensão de dados informáticos)

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

2. O órgão de investigação criminal pode efectuar apreensões, sem prévia autorização da competente autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 21 da presente Lei, 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 pelo órgão de investigação criminal são sempre sujeitas à validação pela autoridade judiciária competente, 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 dos dados, em suporte autónomo, que será junto ao processo;
- c) preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos;
- d) eliminação não reversível ou bloqueio do acesso aos dados.

ARTIGO 23

(Intercepção de comunicações)

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

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

3. À interceptação e registo de transmissões de dados informáticos aplica-se o regime da interceptação e gravação de conversações ou comunicações telefónicas, previsto no Código de Processo Penal.

ARTIGO 24

(Acções encobertas)

É admissível o recurso às acções encobertas previstas no artigo 227 do Código de Processo Penal na investigação dos crimes previstos na presente Lei e dos demais crimes cometidos com recurso à tecnologia informática, desde que puníveis com pena de prisão igual ou superior a 2 anos.

CAPÍTULO IV

Cooperação Internacional

ARTIGO 25

(Âmbito da cooperação internacional)

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

ARTIGO 26

(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 da solicitação de que as mesmas permaneçam confidenciais ou apenas sejam utilizadas em determinadas condições.

3. Para efeitos do número 2 do presente artigo, 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 27

(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 16 da presente Lei, é assegurada pelo Ministério Público a manutenção de uma estrutura que garante um ponto de contacto disponível em regime de permanência.

2. Este ponto de contacto pode ser contactado por outros pontos de contacto, 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;
- e) em caso de emergência, no quadro de tratados ou acordos internacionais que vinculem Moçambique, receber pedidos de um outro ponto de contacto, pelo qual se solicite assistência imediata para obter, de forma expedita e sem pedido formal de auxílio judiciário mútuo, dados informáticos específicos armazenados, na posse ou sob o controlo de um prestador de serviços em Moçambique.

4. Sempre que actue ao abrigo das alíneas b) e c), do número 3 do presente artigo, o órgão de investigação criminal comunica, de imediato, ao Ministério Público, remetendo o respectivo relatório nos termos do Código de Processo Penal.

ARTIGO 28

(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 específica:

- 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 dos dados.

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

4. A preservação pode também ser ordenada pelo órgão de investigação criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora.

5. A ordem de preservação específica, sob pena de nulidade:

- a) a natureza dos dados;
- b) se forem conhecidos, a origem e o destino dos mesmos;
- c) o período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses.

6. Em cumprimento da ordem de preservação que lhe seja dirigida, aquele que tiver 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 o órgão de investigação criminal, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c), do número 5, 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 número 1, do presente artigo, a autoridade judiciária competente para dele decidir, determina a preservação dos dados até à adopção de uma decisão final sobre o pedido.

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

- a) à autoridade judiciária competente, em execução do pedido de auxílio referido no número 1, do presente artigo, nos mesmos termos em que poderiam sê-lo, em caso de pedido 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 9 do presente artigo, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via, através dos quais a comunicação foi efectuada, comunica-os imediatamente 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 números 1 e 2 do presente artigo, aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades moçambicanas.

ARTIGO 29

(Motivos de recusa)

1. Para além dos motivos que em geral podem fundamentar a recusa de cooperação jurídica e judiciária internacional, a solicitação de preservação ou revelação expeditas de dados informáticos é recusada quando:

- a) os dados informáticos em causa respeitarem a infracção de natureza política ou infracção conexa segundo as concepções do Direito moçambicano;
- b) atentar contra a soberania, segurança, ordem pública ou outros interesses da República de Moçambique, constitucionalmente consagrados;
- c) o Estado requerente não oferecer garantias adequadas de protecção dos dados pessoais.

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 pode ser recusado por ausência de verificação do requisito da dupla incriminação.

ARTIGO 30

(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 de pedido 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 acordo internacional aplicável.

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

ARTIGO 31

(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 voluntário de pessoa legalmente autorizada a divulgar.

ARTIGO 32

(Intercepção de comunicações electrónicas em cooperação internacional)

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

CAPÍTULO V

Disposições Transitórias e Finais

ARTIGO 33

(Regime subsidiário)

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 do Código Penal, 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 34

(Revogação)

1. São revogados os artigos 256, 289, 336, 337, 338 e 339, do Código Penal, aprovado pela Lei n.º 24/2019, de 24 de Dezembro, alterada pela Lei n.º 17/2020, de 23 de Dezembro.

2. São revogados o artigo 57 e o número 2 do artigo 66, ambos da Lei n.º 4/2016, de 3 de Julho, Lei das Telecomunicações.

ARTIGO 35

(Regulamentação)

Sem prejuízo das competências conferidas a determinadas entidades, compete ao Conselho de Ministros regulamentar a presente Lei, no prazo de 180 dias, a contar da data da sua publicação.

ARTIGO 36

(Entrada em vigor)

A presente Lei entra em vigor 90 dias, após a sua publicação.
Aprovada pela Assembleia da República, aos 29 de Abril de 2026.

A Presidente da Assembleia da República, *Margarida Adamugi Talapa*.

Promulgada, aos 10 de Junho de 2026.

Publique se.

O Presidente da República, DANIEL FRANCISCO CHAPO.

Preço — 120,00MT