MOÇAMBIQUE
NMP Advogados – PLMJ Colab Moçambique

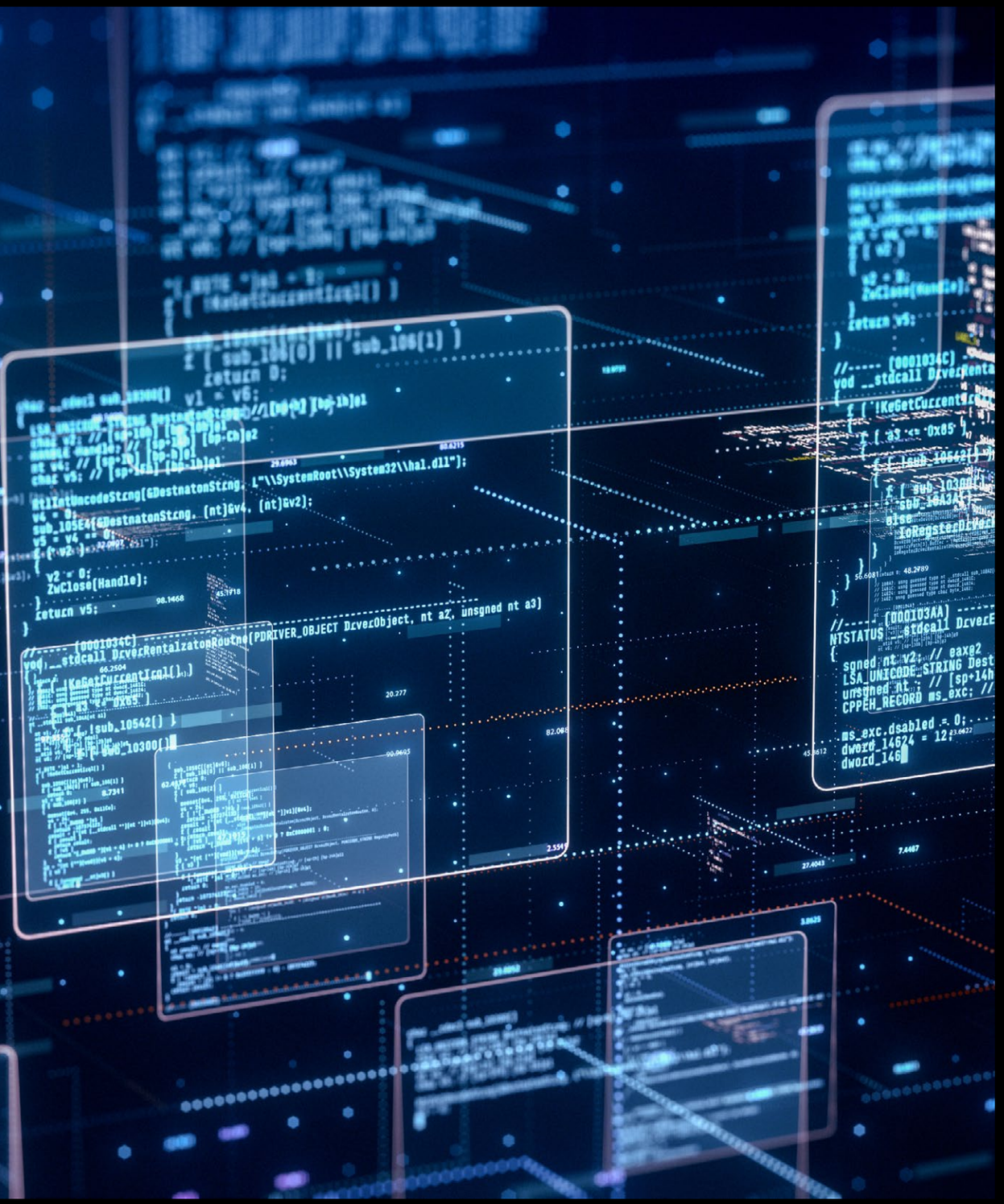
PORTUGAL
PLMJ Advogados

COLAB

Novo regime jurídico da segurança cibernética e dos crimes cibernéticos

Transformative Legal Experts

PLMJ



Índice

Foram publicadas, no Boletim da República, I Série, n.º 123, de 1 de julho de 2026, a Lei n.º 13/2026 de 1 de Julho, que aprova a Lei de Segurança Cibernética, e a Lei n.º 14/2026 de 1 de Julho, que aprova a Lei dos Crimes Cibernéticos. Esta última procede, ainda, à revogação de disposições do Código Penal e da Lei das Telecomunicações.

> Estes diplomas introduzem um quadro sancionatório próprio para a cibercriminalidade.

Tratam-se de dois diplomas com forte impacto transversal, na medida em que abrangem grande parte dos operadores económicos que dependem de redes e sistemas de informação, além de introduzirem, pela primeira vez no ordenamento jurídico moçambicano, um quadro sancionatório próprio para a cibercriminalidade.

O presente documento analisa os aspectos principais de cada um destes diplomas, com particular enfoque nas implicações práticas para as organizações.

Lei de Segurança Cibernética

Lei n.º 13/2026 de 1 de Julho

A Lei de Segurança Cibernética assume-se como o diploma-quadro do novo regime, definindo como objectivo central a protecção do Estado, das instituições e dos cidadãos no espaço cibernético, através da salvaguarda das redes de comunicação de dados, dos sistemas de informação e das infra-estruturas críticas.

O âmbito subjectivo de aplicação não se limita a operadores de infra-estruturas tradicionalmente sensíveis, estendendo-se, designadamente, aos seguintes sectores:

i) Administração Pública;

ii) Sector privado;

iii) Operadores de redes de infra-estruturas críticas;

iv) Prestadores intermediários de serviços;

v) Prestadores de serviços digitais;

vi) Operadores de redes de serviços essenciais;

vii) Prestadores de serviços de segurança cibernética;

viii) Prestadores de plataformas digitais;

ix) Operadores de comunicações electrónicas; e

x) De forma residual, a quaisquer pessoas singulares e entidades que utilizem redes de comunicação de dados e sistemas de informação.

Ficam, contudo, fora deste âmbito as entidades da Administração Pública em acções sobre redes, sistemas de informação e infra-estruturas críticas para fins de defesa nacional, segurança interna e de Estado, bem como as entidades que tratem informação classificada conforme a legislação aplicável. Quando uma entidade se enquadre simultaneamente em mais do que uma das categorias previstas, aplica-se o regime mais exigente para a segurança das redes e dos sistemas de informação.

A Lei rege-se por um conjunto alargado de princípios, entre os quais se destacam a colaboração e cooperação, a protecção dos direitos humanos, a transparência, a divulgação de vulnerabilidades, a integridade, a legalidade, a proporcionalidade, a necessidade e a privacidade.

ORGANIZAÇÃO DO SISTEMA NACIONAL DE SEGURANÇA CIBERNÉTICA

A Lei cria um ecossistema institucional para a governação da segurança cibernética, estruturado em torno de órgãos de coordenação política e técnica e de um conjunto alargado de entidades operacionais.

O Sistema Nacional de Segurança Cibernética é composto por órgãos e entidades organizados numa estrutura hierárquica.

No plano dos órgãos, destacam-se três pilares fundamentais:

i) O **Conselho Nacional de Segurança Cibernética (CNSC)** é o órgão multissectorial de coordenação e governação, presidido pelo Primeiro-Ministro, com competências de coordenação político-estratégica, monitorização da Estratégia Nacional de Segurança Cibernética e emissão de pareceres;

ii) A **Autoridade Nacional de Segurança Cibernética**, cujas funções são exercidas pela Autoridade Reguladora de Tecnologias de Informação e Comunicação, detém competências de regulação, supervisão, fiscalização, licenciamento, credenciação de profissionais e definição de padrões e normas na área da segurança cibernética;

iii) A **Equipa Nacional de Resposta a Incidentes de Segurança Cibernética (nCSIRT.MZ)** é o órgão de coordenação operacional para a prevenção e resposta a incidentes, funcionando na Entidade Reguladora de Tecnologias de Informação e Comunicação.

Em caso de estado de sítio ou de emergência, as funções da Autoridade Nacional de Segurança Cibernética são exercidas pelo Centro de Coordenação Cibernética das Forças de Defesa e Segurança.

No plano das entidades, o Sistema integra, nomeadamente, a Rede Nacional de CSIRTs, os Operadores de Infra-estruturas Críticas, os Provedores Intermediários de Serviços Electrónicos, os Operadores de Serviços Essenciais, os Provedores de Serviços Digitais, os Operadores de Plataformas Digitais, os Operadores de Centros de Dados, os Operadores de Plataformas de Computação em Nuvem, os Provedores de Serviços de Segurança Cibernética e os Operadores de Comunicações Digitais.

OBRIGAÇÕES DAS ENTIDADES

A Lei impõe obrigações específicas a cada categoria de entidade. Em termos gerais, todas as entidades abrangidas devem, entre outras obrigações:

i) registar-se junto da Autoridade Nacional de Segurança Cibernética;

ii) aplicar medidas de governação, identificação e protecção do risco cibernético, detecção, resposta e recuperação de ataques;

iii) manter o sigilo das comunicações dos seus utilizadores; e

iv) colaborar com as autoridades competentes.

A Administração Pública, o Sector Privado, os Operadores de Infra-estruturas Críticas, os Operadores de Serviços Essenciais, os Provedores de Serviços Digitais, os Operadores de Plataformas Digitais, os Operadores de Centros de Dados, os Operadores de Plataformas de Computação em Nuvem e os Operadores de Comunicações Digitais estão obrigados a estabelecer um CSIRT institucional.

SEGURANÇA DAS REDES, SISTEMAS DE INFORMAÇÃO E REQUISITOS DE SEGURANÇA

No que respeita à segurança das redes, a Lei impõe às entidades abrangidas o dever de assegurar a integridade, a confidencialidade e a privacidade das comunicações. Este dever é acompanhado de uma obrigação de conservação de dados de tráfego por um período mínimo de 1 ano, prazo que pode ser prorrogado mediante decisão judicial.

Nesse contexto, os provedores intermediários de serviços e os provedores de serviços digitais que armazenem dados de tráfego e de localização devem, sempre que tal lhes seja solicitado pelas autoridades competentes e nos termos da lei, disponibilizar-lhes o acesso a esses dados.

A Autoridade Nacional de Segurança Cibernética é responsável por estabelecer e actualizar os requisitos de segurança cibernética, de forma a permitir a utilização de padrões e normas internacionalmente aceites.

Os requisitos mínimos de segurança incluem, nomeadamente:

i) a existência de uma política de segurança de informação;

ii) uma metodologia de gestão do risco cibernético;

iii) procedimentos de notificação de incidentes;

iv) mecanismos de auditoria interna;

v) nomeação de um responsável pela segurança da informação; e

vi) criação de uma equipa especializada na detecção e resposta a incidentes.

As entidades da Administração Pública e do Sector Privado devem, adicionalmente, nomear um responsável e um auditor interno de segurança cibernética e criar uma Política de Segurança de Informação Institucional.

NOTIFICAÇÃO DE INCIDENTES E DIVULGAÇÃO RESPONSÁVEL DE VULNERABILIDADES

Quanto à notificação de incidentes, as entidades devem notificar ao respectivo CSIRT sectorial e ao CSIRT Nacional os **incidentes com impacto significativo**, dentro do prazo determinado pela Autoridade Nacional de Segurança Cibernética. A Lei consagra expressamente que a notificação não acarreta responsabilidades acrescidas para a parte notificante. A determinação do impacto significativo atende a parâmetros como o **número de utilizadores afectados**, a **duração do incidente** e a **distribuição geográfica da área afectada**.

Qualquer pessoa singular ou colectiva pode comunicar, publicar ou divulgar vulnerabilidades, desde que a divulgação seja baseada na boa-fé.

A Lei admite ainda a notificação voluntária de incidentes, que não pode dar origem à imposição de obrigações adicionais à entidade notificante.

Quanto à divulgação de vulnerabilidades, a Lei introduz um regime de divulgação responsável das mesmas, nos termos do qual qualquer pessoa singular ou colectiva pode comunicar, publicar ou divulgar vulnerabilidades, desde que a divulgação seja baseada na boa-fé, considerando-se de boa-fé a divulgação que, nomeadamente, não tenha sido feita sob coacção, tenha concedido um prazo razoável de pelo menos 90 dias para correcção da vulnerabilidade e tenha sido acompanhada de precauções para prevenir danos. Ficam excluídos do regime de boa-fé os métodos de identificação que envolvam negação de serviço, evidência física, uso de código malicioso, engenharia social ou alteração, remoção ou destruição de dados.

FUNDO DE SEGURANÇA CIBERNÉTICA

A Lei institui também um Fundo de Segurança Cibernética (FSC), gerido pela Autoridade Nacional de Segurança Cibernética, com o objectivo de assegurar recursos financeiros para promover e fortalecer a segurança cibernética. As entidades registadas e licenciadas para a prestação de serviços de segurança cibernética devem contribuir para o FSC com 1% da receita bruta do ano anterior.

> A Lei institui um Fundo de Segurança Cibernética, para assegurar recursos financeiros para promover e fortalecer a segurança cibernética.

REGIME SANCIONATÓRIO

A Lei estabelece um extenso elenco de contraordenações, que incluem, entre outras:

i) A omissão de notificação de incidentes;

ii) A obstrução de investigações ou auditorias;

iii) O incumprimento dos requisitos de segurança;

iv) A recusa de cumprimento de directivas da Autoridade; e

v) O exercício de actividades sem licença.

As sanções são calculadas em múltiplos do salário mínimo em vigor na Função Pública, variando conforme a gravidade da infracção. A título exemplificativo, o incumprimento dos requisitos de segurança é punível com multa de 90 a 160 salários mínimos; o incumprimento da obrigação de notificação de incidentes é punível com multa de 80 a 100 salários mínimos; e o exercício de actividades sem licença é punível com multa de 64 salários mínimos.

REGULAMENTAÇÃO E ENTRADA EM VIGOR

Compete ao Conselho de Ministros regulamentar a Lei no prazo de 180 dias a contar da data da sua publicação.

A Lei entra em vigor 90 dias após a sua publicação, ou seja, a 29 de Setembro de 2026.

▲ VOLTAR AO INÍCIO

Lei dos Crimes Cibernéticos

Lei n.º 14/2026 de 1 de Julho

OBJETO E ÂMBITO DE APLICAÇÃO

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

> O Capítulo II da Lei introduz catorze tipos criminais, cujas molduras penais escalam progressivamente em função da gravidade.

TIPOS CRIMINAIS

O Capítulo II da Lei introduz catorze tipos criminais, cujas molduras penais escalam progressivamente em função da gravidade da conduta e do bem jurídico afectado, culminando em ilícitos como a espionagem cibernética, punível com até 10 anos de prisão. Os ilícitos mais relevantes podem ser agrupados em quatro grandes categorias:

i) Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas;

ii) Crimes de natureza patrimonial e documental;

iii) Crimes contra a segurança do Estado e de infra-estruturas críticas; e

iv) Outros crimes de particular gravidade social.

No primeiro grupo, encontram-se os ilícitos típicos da criminalidade informática, dirigidos à protecção dos próprios sistemas e dados.

O acesso ilegítimo (artigo 4.º) pune quem, sem permissão legal ou autorização, se introduzir num dispositivo alheio com o fim de obter informação não pública, aceder a dados privados, segredos comerciais ou industriais, ou obter acesso remoto não autorizado, com pena de prisão de 1 a 2 anos e multa até 1 ano. Na mesma pena incorre quem produzir, vender, distribuir ou disseminar dispositivos ou programas destinados a produzir tais acções. Note-se que o procedimento criminal não depende de queixa, salvo quando estejam em causa dados relativos à vida privada.

Da mesma forma, a **intercepção ilegítima (artigo 5.º) de transmissões de dados informáticos** é punida com pena de prisão até 3 anos e multa até 2 anos.

Já a **interferência em dados (artigo 6.º)**, que pune a alteração, deterioração, inutilização, eliminação ou destruição ilícita de dados informáticos com pena de prisão de 1 a 2 anos e multa correspondente, sendo a pena agravada para 3 anos de prisão quando a conduta cause dano intencional a infra-estrutura crítica ou interrupção de serviços críticos.

A **interferência em sistemas (artigo 7.º)**, que pune quem entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, com pena de prisão até 2 anos e multa até 1 ano, partilham uma lógica agravatória comum: ambas preveem penas mais severas quando a conduta afecte infra-estruturas ou serviços críticos, podendo a interferência em sistemas ser punida com pena de prisão de 2 a 8 anos quando resulte em dano relevante, afectação de serviços essenciais ou prejuízo significativo para terceiros.

Ainda no primeiro grupo, o **uso abusivo de dispositivos (artigo 8.º)** criminaliza, autonomamente, a produção, venda, distribuição, importação ou disseminação de dispositivos, programas ou dados informáticos destinados à prática dos crimes de acesso ou intercepção ilegítimos, com pena de prisão de 1 a 2 anos.

No segundo grupo, de natureza patrimonial e documental, a **falsidade informática** (artigo 9.º) pune a introdução, modificação, eliminação ou supressão ilícita de dados informáticos com o intuito de produzir documentos falsos, com pena de prisão de 1 a 5 anos e multa até 1 ano. A pena é agravada para 2 a 8 anos de prisão quanto à importação, distribuição ou detenção para fins comerciais de dispositivos que permitam o acesso ilícito a sistemas de comunicação, aplicando-se ainda o mesmo artigo à manipulação, falsificação ou utilização indevida da identidade de outrem.

Numa lógica semelhante de protecção do património, a **burla informática e nas comunicações** (artigo 10.º) pune, com pena de prisão até 3 anos e multa correspondente, a interferência ilícita no tratamento de dados com intenção de enriquecimento ilegítimo que cause prejuízo patrimonial a outrem.

O terceiro grupo reúne os crimes com maior potencial lesivo para a segurança do Estado e das infra-estruturas críticas, reflectindo-se em molduras penais significativamente mais severas.

A **espionagem cibernética** (artigo 11.º) sanciona com pena de prisão de 3 a 10 anos o acesso ilícito a sistemas informáticos governamentais para obtenção de informações classificadas ou estratégicas, para fins de inteligência estrangeira, punindo ainda com 2 a 8 anos de prisão a invasão de redes corporativas para apropriação de segredos industriais.

No mesmo sentido, o crime de **terrorismo e extremismo violento cibernéticos** (artigo 12.º) pune com pena de prisão de 2 a 8 anos o ataque, invasão, destruição ou adulteração de dados ou sistemas de infra-estruturas críticas, bem como a mobilização, recrutamento ou difusão de conteúdos através de sistemas informáticos com motivações políticas, económicas ou religiosas, visando causar pânico, medo ou terror.

Por fim, destacam-se dois crimes de particular gravidade social.

A **extorsão cibernética** (artigo 13.º) pune com pena de prisão até 2 anos e multa correspondente a ameaça de divulgação de informações comprometedoras, ataques a sistemas informáticos ou exfiltração de dados pessoais em troca de pagamento, agravando-se a pena para até 3 anos quando a vítima seja titular de órgão de soberania, membro do governo ou titular de órgão público.

Já o crime de **conteúdo sexual infantil no ambiente digital** (artigo 15.º) pune, com pena de prisão de 6 meses a 1 ano e multa até 1 ano, a produção, oferta, troca, disponibilização, transmissão ou publicação de conteúdo sexual ou pornográfico envolvendo menores, por meio de sistema informático.

Em qualquer dos casos, a **tentativa de prática destes ilícitos é punível** nos termos gerais do Código Penal, e as pessoas colectivas e entidades equiparadas respondem penalmente pelos crimes previstos na Lei, nos termos e limites do regime de responsabilização do Código Penal.

> A tentativa de prática destes ilícitos é punível e as pessoas colectivas e entidades equiparadas respondem penalmente pelos crimes previstos na Lei.

DISPOSIÇÕES PROCESSUAIS

As disposições processuais aplicam-se à investigação dos crimes previstos na Lei, dos crimes cometidos por meio de sistema informático e daqueles que impliquem a recolha de prova em suporte digital.

Um primeiro conjunto de mecanismos visa assegurar que a prova digital não se perde antes de ser formalmente obtida pelas autoridades.

Assim, através da **preservação expedita de dados** (artigo 18.º), a autoridade judiciária competente pode ordenar a quem tenha disponibilidade ou controlo de dados informáticos, designadamente ao fornecedor de serviço, que preserve e proteja os dados em causa, por um prazo máximo de 3 meses, renovável até ao limite máximo de 1 ano, podendo esta ordem ser emitida também pelo órgão de investigação criminal mediante autorização prévia da autoridade judiciária ou, em caso de urgência, com comunicação posterior a esta.

Complementarmente, a **injunção para apresentação de dados** (artigo 20.º) permite à autoridade judiciária ordenar a efectiva apresentação de dados informáticos específicos (incluindo dados de clientes e assinantes de fornecedores de serviço, mesmo quando dirigida a prestadores estrangeiros no âmbito de tratados internacionais), sob pena de punição por desobediência; fica, no entanto, vedada a sua utilização contra suspeitos ou arguidos, bem como quanto a sistemas informáticos usados para o exercício da advocacia e das actividades médica e bancária.

▲VOLTAR AO INÍCIO

Um segundo conjunto de instrumentos diz respeito à obtenção material da prova já localizada.

A **pesquisa de dados informáticos** (artigo 21.º) carece, em regra, de despacho da autoridade judiciária competente, com prazo de validade máximo de 30 dias, podendo o órgão de investigação criminal actuar sem autorização prévia quando haja consentimento voluntário ou, em casos de terrorismo e criminalidade violenta ou altamente organizada, fundados indícios de prática iminente de crime que ponha em grave risco a vida ou integridade de pessoas.

Uma vez localizados os dados, a sua **apreensão** (artigo 22.º) pode ser autorizada pela autoridade judiciária, revestindo diversas formas, desde a apreensão do suporte físico até à simples cópia ou preservação tecnológica dos dados, ou ainda a eliminação ou bloqueio do acesso, sendo as apreensões efectuadas pelo órgão de investigação criminal sempre sujeitas a validação judicial no prazo máximo de 72 horas.

Por fim, a Lei remete para dois meios excepcionais de investigação já conhecidos do processo penal comum, adaptando-os à criminalidade cibernética.

A **intercepção de comunicações** (artigo 23.º) é admissível nos processos relativos aos crimes previstos na Lei, podendo destinar-se ao registo de dados de conteúdo ou apenas à recolha de dados de tráfego.

Já as **acções encobertas** (artigo 24.º) são admissíveis na investigação destes crimes, desde que puníveis com pena de prisão igual ou superior a 2 anos.

COOPERAÇÃO INTERNACIONAL

A Lei prevê um regime de cooperação internacional que contempla, nomeadamente, a troca de informação espontânea entre autoridades nacionais e estrangeiras, a manutenção de um ponto de contacto permanente para cooperação, assegurado pelo Ministério Público, disponível em regime de permanência, e a preservação e revelação expeditas de dados informáticos em contexto de cooperação internacional.

A cooperação pode ser recusada quando, designadamente, os dados respeitem a infracção de natureza política, atentem contra a soberania ou interesses constitucionais de Moçambique, ou o Estado requerente não ofereça garantias adequadas de protecção de dados pessoais.

As autoridades estrangeiras podem, sem necessidade de pedido prévio, aceder a dados informáticos armazenados em Moçambique quando publicamente disponíveis, ou receber dados mediante consentimento voluntário de pessoa legalmente autorizada.

NORMAS REVOGATÓRIAS

A Lei n.º 14/2026 revoga os artigos 256.º, 289.º, 336.º, 337.º, 338.º e 339.º 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.

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

REGIME SUBSIDIÁRIO E ENTRADA EM VIGOR

Em tudo o que não contrarie o disposto na Lei, aos crimes, medidas processuais e cooperação internacional 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 Internacional em Matéria Penal).

Compete ao Conselho de Ministros regulamentar a Lei no prazo de 180 dias. A Lei entra em vigor 90 dias após a sua publicação, ou seja, a 29 de Setembro de 2026.

Observações

Os dois diplomas representam um marco significativo no ordenamento jurídico moçambicano em matéria de segurança cibernética e cibercriminalidade. Do ponto de vista prático, destaca-se o impacto transversal da Lei de Segurança Cibernética, que impõe obrigações extensivas a um leque alargado de entidades públicas e privadas, incluindo a obrigação de registo junto da Autoridade Nacional de Segurança Cibernética, a criação de CSIRTs institucionais, o cumprimento de requisitos mínimos de segurança, a notificação obrigatória de incidentes e a contribuição financeira para o Fundo de Segurança Cibernética.

Os dois diplomas representam um marco significativo no ordenamento jurídico moçambicano em matéria de segurança cibernética e cibercriminalidade.

A Lei dos Crimes Cibernéticos, por seu turno, vem completar o quadro normativo com a tipificação autónoma de crimes cibernéticos, alguns dos quais com molduras penais significativas (como a espionagem cibernética, punível com pena de prisão até 10 anos), e com a regulação de meios de obtenção de prova digital, harmonizando o regime moçambicano com os padrões internacionais em matéria de cibercriminalidade.

Ambos os diplomas carecem de regulamentação pelo Conselho de Ministros, a ser aprovada no prazo de 180 dias, pelo que será relevante acompanhar a publicação da regulamentação complementar, a qual determinará em larga medida a operacionalização prática dos regimes agora instituídos.

Próximos passos

Tendo em conta o regime instituído pelos dois diplomas, recomenda-se que as organizações abrangidas iniciem, desde já, um processo de adequação, atendendo em particular aos seguintes aspectos.

- **Mapeamento do enquadramento legal**: As organizações devem identificar em que categoria(s) se enquadram para efeitos da Lei de Segurança Cibernética, uma vez que as obrigações variam consoante a qualificação aplicável. Caso se enquadrem em mais do que uma categoria, deve aplicar-se o regime mais exigente;

- **Registo junto da Autoridade Nacional de Segurança Cibernética**: A generalidade das entidades abrangidas deve registar-se junto da Autoridade Nacional de Segurança Cibernética como condição para o exercício da sua actividade;

- **Estabelecimento de CSIRT institucional**: As entidades sujeitas a esta obrigação devem preparar a criação e governance da respectiva equipa de resposta a incidentes.

- **Nomeação de responsáveis internos**: As entidades da Administração Pública, do sector privado e os Operadores de Infra-estruturas Críticas devem nomear um responsável e um auditor interno de segurança cibernética, com vista a assegurar a gestão de riscos cibernéticos;

- **Implementação de requisitos mínimos de segurança**: As organizações abrangidas devem rever e, se necessário, implementar uma política de segurança da informação, uma metodologia de gestão do risco cibernético, mecanismos de auditoria interna e um programa de capacitação dos colaboradores, em linha com os requisitos mínimos legalmente exigidos;

- **Preparação de procedimentos de notificação de incidentes**: Devem ser definidos procedimentos internos que permitam identificar, classificar e notificar tempestivamente incidentes de segurança cibernética com impacto significativo ao CSIRT sectorial e ao CSIRT Nacional, dentro dos prazos a fixar pela Autoridade Nacional de Segurança Cibernética;

- **Revisão de políticas de conservação e acesso a dados**: As organizações que armazenem dados de tráfego ou de localização devem assegurar a sua conservação pelo período mínimo de 1 ano e rever os procedimentos de resposta a pedidos judiciais de acesso, preservação ou apreensão de dados, tanto ao abrigo da Lei de Segurança Cibernética como da Lei dos Crimes Cibernéticos;

- **Revisão de protocolos de cooperação com autoridades de investigação criminal:** Face às novas disposições processuais da Lei dos Crimes Cibernéticos, as organizações, em particular os fornecedores de serviços, devem rever os seus procedimentos internos de resposta a ordens de preservação expedita de dados, injunções de apresentação de dados e pedidos de intercepção de comunicações; e

- **Acompanhamento da regulamentação**: Deve ser feito o acompanhamento próximo da regulamentação a aprovar pelo Conselho de Ministros, uma vez que essa regulamentação densificará aspectos essenciais dos regimes ora instituídos, incluindo os requisitos técnicos de segurança e os prazos de notificação de incidentes.

Sobre a PLMJ

→ Quem somos

Sobre NMP Advogados – PLMJ Colab Moçambique

→ Quem somos

"The firm puts together a multi-tiered team, from juniors to partners, and we receive great advice from every level. We always feel supported from a Mozambican law perspective."

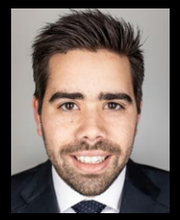
CLIENT REFERENCE FROM THE LEGAL 500

KEY CONTACTS

Pedro Lomba

Sócio e coordenador da área de Tecnologia, Media e Telecomunicações

(+351) 213 197 412
pedro.lomba@plmj.pt



Nuno Morgado Pereira

Sócio Fundador
NMP Advogados – PLMJ Colab Mozambique

(+258) 846 242 670
nuno.morgadopereira@nmpmozambique.com

Agosto 2026