CONSELHO DE MINISTROS

PROPOSTA DE LEI N.º /IX/2016

DE DE

ASSUNTO: 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 eletrónico.

EXPOSIÇÃO DE MOTIVOS

Com a expansão célere das redes de comunicação eletrónicas, em especial, a Internet e a globalização das comunicações através da rede mundial de computadores, cada vez mais atividades das sociedades modernas e das economias dependem do uso dessas redes e das aplicações que nelas assentam, mudando a vida quotidiana dos cidadãos, das empresas e do sector público, criando um espaço virtual, que pode ser indevidamente aproveitado para o cometimento de atos que ofendem bens jurídicos essenciais à subsistência salutar da comunidade, através de crimes informáticos de diferentes tipologias.

Neste contexto, assumem crescente relevo, as atividades ilegais associadas às redes de comunicação, usando-as para efeitos criminosos e explorando as suas vulnerabilidades, o que torna a cibercriminalidade uma ameaça típica dos tempos modernos.

O número de investigações relacionadas a crimes cibernéticos é crescente, e é razoável supor que, à medida que novos usuários ingressem na rede, mais pessoas passem a ter o domínio das estruturas básicas do sistema, surgindo novas formas de criminalidade informática.

Cabo Verde manifestou interesse em aderir à Convenção de Budapeste sobre o Cibercrime e carece de transpor para a legislação nacional ditâmes importantes relativas ao combate ao cibercrime que decorrem das medidas previstas no capítulo II dessa Convenção.

Neste sentido, se propõe definir o quadro legislativo adequado que tenha em conta tanto as necessidades de segurança nacional e os direitos dos consumidores para a criminalização da falsidade informática, abrangendo condutas típicas de falsificação e burla, os danos relativos a programas informáticos, a sabotagem informática, o acesso, a intercepção e a reprodução ilegítimas de programas, assim como a produção, oferta ou disponibilização, difusão ou transmissão, obtenção e posse através de sistema informático de material de conteúdo pornográfico relativo a menor de 18 anos. A

previsão penal que ora se propõe ao abrigo da presente Proposta de Lei abrange pessoas singulares e coletivas ou equiparadas.

Propugna-se ainda, no presente Proposta de Lei, mecanismos especiais de investigação, incluindo pedidas urgentes e preventivas, assim como processos céleres de cooperação judiciária internacional, com a adotação de ponto de contacto permantente, de modo a tornar mais expedita a investigação e a recolha de provas essenciais, que de outro modo poderiam perder-se, em estreita observância ao direito à privacidade e à proteção de dados pessoais.

Foram ouvidos o Conselho Superior da Magistratura Judicial, a Procuradoria-geral da República e a Ordem dos Advogados de Cabo Verde.

Assim,

No uso da faculdade conferida pela alínea b) do n.º 1 do artigo 203.º da Constituição, o Governo submete à Assembleia Nacional a seguinte Proposta de Lei:

CAPÍTULO I
OBJETO E DEFINIÇÕES

Artigo 1.º
Objeto

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 eletrónico.

Artigo 2.º
Definições

Para efeitos da presente Lei, considera -se:

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, proteção e manutenção;

b) «Dados informáticos», qualquer representação de fatos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;

c) «Dados de tráfego», os dados informáticos relacionados com uma comunicação efetuada 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 trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;

d) «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 respetivos utilizadores;

e) «Interceção», o ato destinado a captar informações contidas num sistema informático, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros;

f) «Topografia», uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respetivo fabrico;

g) «Produto semicondutor», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função eletrónica.

CAPÍTULO II
DISPOSIÇÕES PENAIS MATERIAIS

Artigo 3.º
Falsidade informática

1. Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.

2. Quando as ações 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 ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3. Quem, atuando 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 objeto dos atos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.

4. Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de

comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das ações prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.

5. Se os fatos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos.

Artigo 4.º
Dano relativo a programas ou outros dados informáticos

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa até 200 dias.

2. A tentativa é punível.

3. Incorre na mesma pena do n.º 1 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 ações não autorizadas descritas nesse número.

4. Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.

5. Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.

6. Nos casos previstos nos n.ºs 1, 2 e 4 o procedimento penal depende de queixa.

Artigo 5.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, 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 5 anos ou com pena de multa até 600 dias.

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 ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.

3. Nos casos previstos no número anterior, a tentativa não é punível.

4. A pena é de prisão de 1 a 5 anos se o dano emergente da perturbação for de valor elevado.

5. A pena é de prisão de 1 a 10 anos se:

a) O dano emergente da perturbação for de valor consideravelmente elevado;

b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma atividade 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.

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 a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2. Na mesma pena referida no número anterior 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 ações não autorizadas descritas no número anterior.

3. A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.

4. A pena é de prisão de 1 a 5 anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

5. A tentativa é punível, salvo nos casos previstos no n.º 2.

6. Nos casos previstos nos n.ºs 1, 3 e 5 o procedimento penal depende de queixa.

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, intercetar 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 prevista no número anterior 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 ações não autorizadas descritas no número anterior.

3. A tentativa é punível.

Artigo 8.º

Reprodução ilegítima de programa protegido

1. Quem, ilegitimamente, reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.

2. Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.

3. A tentativa é punível.

Artigo 9.º

Pornografia infantil

1. Quem produzir pornografia infantil com o propósito de a divulgar através de um sistema informático é punído com pena de prisão de 2 a 8 anos.

2. Quem oferecer ou disponibilizar pornografia infantil através do sistema informático é punído com pena de prisão de 1 a 5 anos.

3. Quem difundir ou transmitir pornografia infantil através do sistema informático é punído com pena de prisão de 1 a 5 anos.

4. Quem obter para si ou para outra pessoa pornografia infantil através do sistema informático é punído com pena de prisão de 1 a 4 anos.

5. Quem detiver ou por qualquer forma tiver a posse de pornografia infantil através do sistema informático é punído compena de prisão de 1 a 4 anos.

6. Para efeitos previstos nos números anteriores, pornografia infantil abrange todo o material pornografico que represente visualmente:

a) Uma pessoa menor de 18 anos de idade envolvido em comportamentos sexualmente explícitos;

b) Uma pessoa com aspeto de menor de de 18 anos de idade envolvida em comportamentos sexualmente explícitos;

c) Imagens realistas de uma pessoa menor de 18 anos envolvido em comportamentos sexualmente explícitos.

Artigo 10.º

Responsabilidade penal das pessoas coletivas e entidades equiparadas

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

Artigo 11.º
Perda de bens

1. O tribunal pode decretar a perda a favor do Estado dos objetos, materiais, equipamentos ou dispositivos que tiverem servido para a prática dos crimes previstos na presente lei e pertencerem a pessoa que tenha sido condenada pela sua prática.

2. À avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia criminal que sejam suscetíveis de vir a ser declarados perdidos a favor do Estado é aplicável o disposto na Lei n.º 18/VIII/2012, de 13 de setembro.

CAPÍTULO III
DISPOSIÇÕES PROCESSUAIS

Artigo 12.º
Âmbito de aplicação das disposições processuais

Com exceção do disposto nos artigos 19.º e 20.º, as disposições processuais previstas no presente capítulo aplicam -se a processos relativos a crimes:

a) Previstos na presente Lei;

b) Cometidos por meio de um sistema informático; ou

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

Artigo 13.º
Preservação expedita de dados

1. Se no decurso do processo for necessário à produção de 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 a 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 fato à autoridade judiciária e transmitir-lhe o relatório no qual mencionam, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos fatos apurados e as provas recolhidas

3. 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.

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 n.º 3, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 14.º
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 efetuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efetuada.

Artigo 15.º
Injunção para apresentação ou concessão do 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 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, 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 dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer 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 faturação 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.

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

7. O regime de segredo profissional, de função e de segredo de Estado previsto no artigo 247.º do Código de Processo Penal é aplicável com as necessárias adaptações.

Artigo 16.º
Pesquisa de dados informáticos

1. Quando no decurso do processo se tornar necessário à produção de 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, 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:

a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;

b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório no qual mencionam, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos fatos apurados e as provas recolhidas

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 previstas no Código de Processo Penal.

Artigo 17.º
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 produção de 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 efetuar 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 suscetível de revelar dados pessoais ou íntimos, que possam pôr em causa a privacidade do respetivo 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 efetuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.

5. As apreensões relativas a sistemas informáticos utilizados para o exercício da advocacia, e das atividades médica, jornalista e bancária e de órgãos de comunicação social estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Código de Processo Penal.

6. O regime de segredo profissional, de função e de segredo de Estado previsto no artigo 247.º do Código de Processo Penal é aplicável com as necessárias adaptações.

7. 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 respetiva 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; ou

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

8. No caso da apreensão efetuada nos termos da alínea b) do número anterior, a cópia é efetuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial 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.

Artigo 18.º

Apreensão de correio eletrónico e registos de comunicações de natureza semelhante

Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 19.º

Intercepção de comunicações

1. É admissível o recurso à intercepção de comunicações em processos relativos a crimes:

a) Previstos na presente Lei; ou

b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 255.º do Código de Processo Penal.

2. A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante a instrução, 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 fundamentado do juiz competente e mediante requerimento do Ministério Público.

3. 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 referido no número anterior especificar o respetivo âmbito, de acordo com as necessidades concretas da investigação.

4. Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constantes dos artigos 255.º, 256.º, 258.º do Código de Processo Penal.

Artigo 20.º

Ações encobertas

1. É admissível o recurso às ações encobertas previstas na Lei n.º 30/VII/2008, de 21 de julho, nos termos aí previstos, no decurso de instrução relativo aos seguintes crimes:

a) Os previstos na presente Lei;

b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual

nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras.

2. Sendo necessário o recurso a meios e dispositivos informáticos observam -se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.

CAPÍTULO IV
COOPERAÇÃO INTERNACIONAL

Artigo 21.º
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 eletrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 133/V/2001, de 22 de janeiro, alterada pela Lei n.º 41/VIII/2013, de 17 de setembro.

Artigo 22.º
Ponto de contacto permanente para a cooperação internacional

1. Para fins de cooperação internacional, tendo em vista a prestação de assistência imediata para os efeitos referidos no artigo anterior, a Polícia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto disponível em permanência, vinte e quatro horas por dia, sete dias por semana.

2. Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Cabo Verde 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, em conformidade com o disposto no artigo seguinte;

c) A recolha de prova para a qual seja competente nos casos de urgência ou perigo na demora;

d) A localização de suspeitos e a prestação de informações de caráter jurídico, nos casos de urgência ou perigo na demora;

e) A transmissão imediata ao Ministério Público de pedidos relativos às medidas referidas nas alíneas b) a d), fora dos casos aí previstos, tendo em vista a sua rápida execução.

4. Sempre que atue ao abrigo das alíneas b) a d) do número anterior, a Polícia Judiciária dá notícia imediata do fato ao Ministério Público e remete-lhe o relatório no qual mencionam, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos fatos apurados e as provas recolhidas

Artigo 23.º

Preservação e revelação expeditas de dados informáticos em cooperação internacional

1. Pode ser solicitada a Cabo Verde a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 12.º, 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 infração que é objeto de investigação ou procedimento criminal, bem como uma breve exposição dos fatos relacionados;

c) Os dados informáticos a conservar e a sua relação com a infração;

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

e) A necessidade da medida de preservação; e

f) A intenção de apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos 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 a fornecedor de serviço, que os preserve.

4. A preservação pode também ser ordenada pela Polícia Judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, sendo aplicável, neste último caso, o disposto no n.º 4 do artigo anterior.

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; e

c) O período de tempo pelo qual os dados devem ser preservados, até um máximo de três 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 Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea c) do n.º 5, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano.

8. Quando seja apresentado o pedido de auxílio referido no n.º 1, 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 n.º 1, nos mesmos termos em que poderiam sê-lo, em caso nacional semelhante, ao abrigo dos artigos 14.º a 18.º;

b) À autoridade nacional que emitiu a ordem de preservação, nos mesmos termos em que poderiam sê -lo, em caso nacional semelhante, ao abrigo do artigo 14.º.

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 efetuada, 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 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades cabo-verdianas.

Artigo 24.º
Motivos de recusa

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

a) Os dados informáticos em causa respeitarem a infração de natureza política ou infração conexa segundo as concepções do direito cabo-verdiano

b) Atentar contra a soberania, segurança, ordem pública ou outros interesses da República Cabo-verdiana, constitucionalmente definidos;

c) O Estado terceiro requisitante não oferecer garantias adequadas de proteção 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 será recusado por ausência de verificação do requisito da dupla incriminação.

Artigo 25.º
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 Cabo Verde, relativos a crimes previstos no artigo 12.º, quando se trata de situação em que a pesquisa e apreensão são admissíveis em caso nacional semelhante.

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

3. O disposto no n.º 1 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias cabo-verdianas.

Artigo 26.º

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

As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades cabo-verdianas, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 133/V/2001 de 22 de janeiro, alterada pela Lei n.º 41/VIII/2013 de 17 de setembro, podem:

a) Aceder a dados informáticos armazenados em sistema informático localizado em Cabo Verde, quando publicamente disponíveis;

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

Artigo 27.º

Intercepção de comunicações em cooperação internacional

1. Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Cabo Verde, desde que tal esteja previsto em acordo, tratado ou convenção internacional e se trate de situação em que tal intercepção seja admissível, nos termos do artigo 19.º, em caso nacional semelhante.

2. É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresentará ao Ministério Público, para que os apresente ao juiz competente da comarca da Praia para autorização.

3. O despacho de autorização referido no artigo anterior permite também a transmissão imediata da comunicação para o Estado requerente, se tal procedimento estiver previsto no acordo, tratado ou convenção internacional com base no qual é feito o pedido.

4. O disposto no n.º 1 aplica -se, com as devidas adaptações, aos pedidos formulados pelas autoridades judiciárias cabo-verdianas.

CAPÍTULO V
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Artigo 28.º
Aplicação no espaço da lei penal cabo-verdiana e competência dos tribunais cabo-verdianos

1. Para além do disposto no Código Penal em matéria de aplicação no espaço da lei penal cabo-verdiana, e salvo tratado ou convenção internacional em contrário, para efeitos da presente lei, a lei penal cabo-verdiana é ainda aplicável a fatos:

a) Praticados por cabo-verdianos, se aos mesmos não for aplicável a lei penal de nenhum outro Estado;

b) Cometidos em benefício de pessoas coletivas com sede em território cabo-verdiano;

c) Fisicamente praticados em território cabo-verdiano, ainda que visem sistemas informáticos localizados fora desse território; ou

d) Que visem sistemas informáticos localizados em território cabo-verdiano, independentemente do local onde esses fatos forem fisicamente praticados.

e) Praticados por cabo-verdiano ou estrangeiro que se encontrar em território cabo-verdiano ou para aqui se deslocar ou for encontrado

2. Se, em função da aplicabilidade da lei penal cabo-verdiana, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente lei tribunais estrangeiros, podendo em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos fatos, a autoridade judiciária competente recorre aos órgãos e mecanismos previstos na lei de cooperação judiciária em matéria penal para facilitar a cooperação e a coordenação das respetivas ações, por forma a decidir quem instaura ou prossegue o procedimento contra os agentes da infração, tendo em vista a eficácia da ação penal.

3. A decisão de aceitação ou transmissão do procedimento é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos:

a) O local onde foi praticada a infração;

b) A nacionalidade do autor dos fatos; e

c) O local onde o autor dos fatos foi encontrado.

4. São aplicáveis aos crimes previstos na presente Lei as regras gerais de competência dos tribunais previstas no Código de Processo Penal.

5. Em caso de dúvida quanto ao tribunal territorialmente competente, designadamente por não coincidirem o local onde fisicamente o agente atuou e o local onde está fisicamente instalado o sistema informático visado com a sua atuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos fatos.

Artigo 29.º

Regime geral aplicável

Em tudo o que não contrarie o disposto na presente lei, aplicam-se aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, respetivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei da cooperação judiciária em matéria penal

Artigo 30º.

Competência da Polícia Judiciária para a cooperação internacional

A competência atribuída pela presente lei à Polícia Judiciária para efeitos de cooperação internacional é desempenhada pela unidade orgânica a quem se encontra cometida a investigação dos crimes previstos na presente lei.

Artigo 31.º

Proteção de dados pessoais

O tratamento de dados pessoais ao abrigo da presente lei efetua-se de acordo com o disposto na Lei n.º 133/V/2001, de 22 de janeiro, alterada pela Lei n.º 41/VIII/2013, de 17 de setembro.

Artigo 32.º

Entrada em vigor

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

Aprovada em Conselho de Ministros do dia 06 de outubro de 2016.

José Ulisses Correia e Silva

Fernando Elísio Leboucher Freire de Andrade