



SÃO TOMÉ E PRÍNCIPE

DIÁRIO DA REPÚBLICA

SUMÁRIO

ASSEMBLEIA NACIONAL

Lei n.º 15/2017

Lei sobre Cibercrime.

Lei n.º 16/2017

Lei de Segurança Interna.

GOVERNO

Decreto n.º 15/2017

Aprova as atribuições e estabelece a composição do Conselho Nacional de Proteção Social.

ASSEMBLEIA NACIONAL**Lei n.º 15/2017****Lei sobre Cibercrime****Preâmbulo**

A presente Lei busca abordar aspectos e conceitos da internet e também das ameaças surgidas com a chamada Revolução Tecnológica. A despeito de a internet ser um «mundo sem leis», os actos ilícitos praticados por esse meio acabam saindo da esfera virtual e penetrando na esfera jurídica, surgindo, desse modo, os chamados crimes virtuais, que podem ser praticados através da internet ou com o uso do computador ou qualquer outro dispositivo electrónico.

Cresce a cada dia que passa, o número de pessoas conectadas através da internet. Assim, torna-se necessária a intervenção do Estado de forma a coibir práticas que ultrapassem o limite da esfera de liberdade alheia.

Assim, a Assembleia Nacional decreta nos termos da alínea b) do artigo 97.º da Constituição, o seguinte:

Capítulo I
Objecto e definições**Artigo 1.º**
Objecto

1. A presente Lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, relativa a ataques contra sistemas de informação, e adaptando o direito interno às convenções internacionais sobre o Cibercrime.

2. Atribuir igualmente competência ao Ministério Público para iniciar, exercer e dirigir a acção penal relativamente a crimes sexuais praticados contra menores com recurso aos meios informáticos ou divulgados através destes, cuja notícia de crime seja adquirida através de comunicações provindas de quaisquer Estado e organizações internacionais diversas.

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, protecção e manutenção;
- b) «Dados informáticos», qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;
- c) «Dados de tráfego», os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;
- 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 respectivos utilizadores;
- e) «Intercepção», o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, 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 semiconductor e

na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semiconductor, independentemente da fase do respectivo fabrico;

- g) «Produto semiconductor», a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semiconductor 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 electrónica.

Artigo 3.º

Direito subsidiário

Aos crimes previstos na presente Lei são subsidiariamente aplicáveis as normas do Código Penal.

Capítulo II

Disposições penais materiais

Artigo 4.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 10 a 300 dias.

2. Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.

3. Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1 ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no

número anterior, é punido com as penas previstas num e noutro número, respectivamente.

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 acções prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.

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

Artigo 5.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 afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.

2. A tentativa é punível.

3. Incorre na mesma pena do n.º 1 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 nesse número.

4. Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 300 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 6.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, entrar, 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 300 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 acções 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 actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Artigo 7.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 incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

3. 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 8.º **Intercepção ilegítima**

1. Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar 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. A tentativa é punível.

3. Incorre na mesma pena prevista no 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 acções não autorizadas descritas no mesmo número.

Artigo 9.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 semiconductor 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 10.º

Inserção de dados falsos

1. Quem inserir ou facilitar a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para outrem ou para causar prejuízo, é punido com pena de prisão até 2 anos ou com pena de multa até 200 dias.

2. A pena é agravada para o dobro se da alteração referida no número anterior resultar «efectivo prejuízo para uma pessoa.»

3. As Instituições com plataforma nos espaços cibernéticos devem garantir através de meios tecnológico a fiabilidade da identidade e a confirmação de e-e-mail no processo de cadastro de usuários.

4. As instituições com plataforma no mundo cibernético são penalizadas com as penas previstas no n.º 1 e 2 caso permita cibernautas propositalmente inserir ou facilitar a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para outrem ou para causar prejuízo.

Artigo 11.º

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 regime de responsabilização previsto no Código Penal.

Artigo 12.º

Perda de bens

1. O tribunal pode decretar a perda a favor do Estado dos objectos, 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. A avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia judiciária que sejam susceptíveis de vir a ser declarados perdidos a favor do Estado, é regulado por decreto do governo.

Artigo 13.º

Agravação da pena

1. Se os crimes previstos na presente Lei envolverem dados ou sistemas informáticos dos órgãos executivo, legislativo ou judicial ou de outras entidades públicas da República Democrática de São Tomé e Príncipe, as penas previstas nos artigos 3.º a 11.º são agravadas de um terço nos seus limites mínimo e máximo.

2. O disposto no n.º 1 do artigo 188.º alínea c) e do artigo 204.º do Código Penal é aplicável aos crimes neles indicados, cometidos através da internet quando esta seja utilizada como meio de ampla difusão.

Capítulo III

Disposições processuais

Artigo 14.º

Âmbito de aplicação das disposições Processuais

1. Com excepção do disposto nos artigos 21.º e 22.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 electrónico.

2. As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 3/2016, de 10 de Maio, Lei de Protecção de Dados Pessoais.

Artigo 15.º

Preservação expedita de dados

1. Se no decurso do processo for necessário a 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 judiciária mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no n.º 6.

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 devem 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 respectivos requisitos de admissibilidade, até ao limite máximo de um ano.

6. Em cumprimento das diligências previstas no n.º 2, os órgãos de polícia criminal que procederem a diligências referidas nos artigos anteriores elaboraram um relatório onde mencionam, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas.

7. O relatório é remetido ao Ministério Público ou ao juiz de instrução conforme os casos.

Artigo 16.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 judiciária, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efectuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efectuada.

Artigo 17.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 facturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou
- c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

5. A injunção prevista no presente artigo não pode ser dirigida a suspeito ou arguido nesse processo.

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

7. O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 253.º do Código de Processo Penal é aplicável com as necessárias adaptações.

Artigo 18.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 judiciária 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 judiciária proceder à pesquisa nos termos do número anterior:

- a) No caso previsto na alínea b) do número anterior, 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) Os órgãos de polícia judiciária que procederem a diligências referidas nos termos da presente Lei, elaboram um relatório onde mencionam, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos apurados e as provas recolhidas, que deve ser remetido ao Ministério Público ou ao juiz de instrução, conforme os casos.

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 e no Estatuto do Jornalista.

Artigo 19.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 judiciária pode efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

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

4. As apreensões efectuadas por órgão de polícia judiciária 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, das actividades médica e bancária estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas nos n.ºs 6 e 7 do artigo 15.º e as relativas a sistemas informáticos utilizados para o exercício da profissão de jornalista estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no Estatuto do Jornalista. O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 253.º do Código de Processo Penal é aplicável com as necessárias adaptações.

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

7. No caso da apreensão efectuada nos termos da alínea b) do número anterior, a cópia é efectuada em duplicado, sendo uma das cópias selada e confiada ao 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 20.º

Apreensão de correio electrónico 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 noutra a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico 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 21.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 electrónico, quando tais crimes se encontrem previstos no artigo 258.º do Código de Processo Penal.

2. A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, 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 de instrução 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 respectivo 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 constante dos artigos 258.º, 259.º e 260.º do Código de Processo Penal.

Artigo 22.º
Acções encobertas

1. É admissível o recurso às acções encobertas que são aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro actuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta Lei, com ocultação da sua qualidade e identidade.

2. O recurso às acções encobertas são admissíveis, no decurso de inquérito relativo aos seguintes crimes:

- a) Os previstos na presente Lei;
- b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, 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 infracções económico-financeiras, bem como os crimes consagrados para a violação do Direito de Autor e dos Direitos Conexos.

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

4. O regime jurídico das acções encobertas, consta de diploma próprio.

Capítulo IV
Cooperação internacional

Artigo 23.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 electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 3/2016, de 10 de Maio, Lei de Protecção de Dados Pessoais.

Artigo 24.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 São Tomé e Príncipe se encontre vinculado, ou em cumprimento de protocolos de cooperação internacional com organismos judiciais 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 carácter 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 actue ao abrigo das alíneas b) a d) do número anterior, a Polícia judiciária dá notícia imediata do facto ao Ministério Público e remete-lhe o relatório previsto no artigo 18.º.

Artigo 25.º

Preservação e revelação expeditas de dados Informáticos em cooperação internacional

1. Pode ser solicitada a República Democrática de São Tomé e Príncipe a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 15.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 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; 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 respectivos 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 17.º a 21.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 15.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 efectuada, comunica-os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos.

11. O disposto nos n.ºs 1 e 2 aplica-se, com as devidas adaptações, aos pedidos formulados pelas autoridades são-tomenses.

Artigo 26.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 infracção de natureza política ou infracção conexa segundo as concepções do direito são-tomense;
- b) Atentar contra a soberania, segurança, ordem pública ou outros interesses da República, constitucionalmente definidos;
- c) O Estado terceiro requisitante 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 é recusado por ausência de verificação do requisito da dupla incriminação.

Artigo 27.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 na República Democrática de São Tomé e Príncipe, 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 São-tomense.

Artigo 28.º
Acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento

1. As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades são-tomenses, de acordo com as normas sobre transferência de dados pessoais previstas na Lei de Protecção de Dados Pessoais, podem:

- a) Aceder a dados informáticos armazenados em sistema informático localizado na República Democrática de São Tomé e Príncipe, quando publicamente disponíveis;
- b) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em São Tomé e Príncipe, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulgá-los.

Artigo 29.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 na República Democrática de São Tomé e Príncipe, 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 20.º, em caso nacional semelhante.

2. É competente para a recepção dos pedidos de intercepção a Polícia Judiciária, que os apresenta ao Ministério Público, para que os apresente ao juiz de instrução criminal 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 nacionais.

Capítulo V

Disposições finais e transitórias

Artigo 30.º

Aplicação no espaço da lei penal são-tomense e a competência dos tribunais nacionais

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

- a) Praticados por são-tomenses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado;
- b) Cometidos em benefício de pessoas colectivas com sede em território são-tomense;
- c) Fisicamente praticados em território são-tomense, ainda que visem sistemas informáticos localizados fora desse território; ou
- d) Que visem sistemas informáticos localizados em território são-tomense, independentemente do local onde esses factos forem fisicamente praticados.

2. Se, em função da aplicabilidade da Lei penal são-tomense, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente Lei, os tribunais são-tomense e os tribunais de outro Estado com o qual aquele tenha acordo ou tratado ou convenção, pode em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos, a autoridade judiciária competente recorre aos órgãos e mecanismos instituídos para facilitar a cooperação entre as autoridades judiciárias dos Estados e a coordenação das respectivas acções, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infracção, tendo em vista centralizá-lo num só deles.

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 infracção;
- b) A nacionalidade do autor dos factos; e

- c) O local onde o autor dos factos 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 actuou e o local onde está fisicamente instalado o sistema informático visado com a sua actuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos.

Artigo 31.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, respectivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei de Cooperação Internacional em Matéria Penal.

Artigo 32.º

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 33.º

Protecção de dados pessoais

O tratamento de dados pessoais ao abrigo da presente Lei efectua-se de acordo com o disposto na Lei n.º 3/2016, protecção de dados pessoais, sendo aplicável, em caso de violação, o disposto no Capítulo IV.

Artigo 34.º

Entrada em vigor

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

Assembleia Nacional, em São Tomé, aos 28 de Junho de 2017.- O Presidente da Assembleia Nacional, *José da Graça Diogo*.

Promulgado em 03 de Agosto de 2017

Publique-se.-

O Presidente da República, *Evaristo do Espírito Santo Carvalho*.

Lei n.º 16/2017

Lei de Segurança Interna

Preâmbulo

Atendendo à diversidade das Forças e Serviços de Segurança, a criação deste órgão de consulta permite assistir, de modo permanente, às entidades governamentais responsáveis pela execução da política de Segurança Interna e servir de centro aglutinador e difusor de deliberações ministeriais concertadas, em matéria de Segurança Interna. Finalmente, porque a Segurança Interna tem de ser entendida como tarefa fundamental do Estado a favor do bem-estar das pessoas;

A presente Lei procura definir as medidas de polícia, os seus fins e os seus limites, de forma que os direitos fundamentais só possam ser limitados nos casos de excepcional necessidade admitida por lei e define os objectivos, prioridades e orientações em matéria de prevenção da criminalidade, investigação criminal, acção penal e execução de penas e medidas de segurança.

Assim sendo, a Assembleia Nacional decreta nos termos da alínea b) do artigo 97.º da Constituição, o seguinte:

Capítulo I

Disposições e Princípios Gerais

Artigo 1.º

Conceito de segurança interna

1. A Segurança Interna é a actividade desenvolvida pelo Estado, para garantir a ordem, a segurança e a tranquilidade pública, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática.

2. A actividade de Segurança Interna deve ser exercida de harmonia com as leis, em rigoroso res-

peito pelos direitos, liberdades e garantias dos cidadãos e em obediência, nomeadamente às leis processuais penais, Lei Orgânica da Polícia, e às orgânicas dos demais Serviços de Segurança.

Artigo 2.º

Fins da Segurança Interna

As medidas previstas na presente Lei visam a contenção da actividade criminal, de forma a impedir os seus resultados ou diminuir os seus efeitos e, especialmente, a protecção da vida e da integridade física das pessoas, da tranquilidade pública e da ordem democrática, contra a criminalidade violenta ou altamente organizada, não devendo ser utilizadas para além do estritamente necessário e obedecendo a exigências de adequação e proporcionalidade.

Artigo 3.º

Princípios fundamentais

A actividade de Segurança Interna é desenvolvida no respeito das leis, na observância dos princípios do Estado de Direito Democrático, dos direitos, liberdades e garantias, pelos princípios da Administração Pública e pelas regras gerais.

Artigo 4.º

Política de Segurança Interna

A política de Segurança Interna consiste no conjunto de princípios, objectivos, prioridades, orientações e medidas tendentes à prossecução dos fins definidos nos artigos 1.º e 2.º.

Artigo 5.º

Âmbito territorial

1. A actividade de Segurança Interna desenvolve-se em todo Território Nacional e em qualquer outro espaço geográfico sujeito aos poderes de jurisdição do Estado São-tomense.

2. No quadro dos compromissos internacionais e das normas aplicáveis do Direito Internacional, as Forças e Serviços de Segurança podem actuar fora do espaço referido no número anterior, em cooperação com organismos e serviços de Estados estrangeiros ou com Organizações Internacionais de que São Tomé e Príncipe faz parte.