IX GOVERNO CONSTITUCIONAL
MINISTÉRIO DA JUSTIÇA

Proposta de Lei n.º ...../2024

de.... de...

Cibercrime

EXPOSIÇÃO DE MOTIVOS

É inegável que a internet tornou parte das nossas vidas, uma revolução da informação que criou um verdadeiro mundo virtual, com redes sociais utilizadas para comunicação entre as pessoas, aquisição de bens e serviços realizadas através da internet, de tal modo que a utilização das redes e tecnologias de informação e comunicação tornou-se uma realidade omnipresente na vida quotidiana. Quase todas as atividades das sociedades modernas e das economias usam a Internet para seu apoio, e não só os cidadãos a usam para suas atividades da vida quotidiana, como também as funções tradicionais do Estado são realizadas e os seus serviços disponibilizados por intermédio da internet. Grande parte das atividades das sociedades modernas hoje dependem mesmo da Internet e outras ainda surgiram especificamente na e para a Internet, tornando-se numa realidade incontornável e em relação a qual as sociedades modernas já não podem prescindir no seu processo de desenvolvimento.

Naturalmente que a utilização quotidiana das tecnologias de informação e comunicação e dos meios informáticos para atividades dos cidadãos, empresas e do Estado comporta riscos e vulnerabilidades que podem ser usadas e exploradas de forma ilícita, tornado assim a cibercriminalidade numa verdadeira e real ameaça.

Para fazer face à utilização ilícita e abusiva das redes de comunicação, os Estados têm empreendido medidas legislativas com dimensão preventiva e repressiva, mediante aprovação de legislação específica que além de criminalizarem esse tipo de fenómenos, estabelecem normas específicas de investigação e recolha de prova e ainda incentivam a cooperação entre os Estados nestes casos.

A comunidade internacional ao longo dos anos tem empreendido medidas no sentido não só de fomentar a cooperação entre os Estados, mas também de harmonizar as legislações nacionais de forma a se poder combater com maior eficácia a cibercriminalidade. Nesse sentido, é de se referir esforços a Convenção sobre Cibercrime do Conselho da Europa, também conhecida como Convenção de Budapeste, aberto a assinatura em Budapeste desde 23 de Novembro de 2001. Trata-se do primeiro e mais importante instrumento internacional sobre crime no ciberespaço. É ainda o único instrumento normativo em vigor neste âmbito. Tem vocação universal e pretende vir a ser aceite pela generalidade dos países do mundo. O seu escopo precípuo é contribuir para a harmonização das legislações nacionais sobre a matéria do cibercrime, e também favorecer e facilitar a cooperação internacional, instituindo mecanismos processuais que confiram eficácia às investigações de natureza criminal. Incide sobre direito penal material (definindo crimes contra a confidencialidade, integridade e disponibilidade dos sistemas de computadores, crimes referentes aos conteúdos e crimes cometidos por via da informática) mas também contém medidas de natureza processual relativo à recolha e preservação de prova e igualmente de cooperação judiciária internacional.

Fazem parte da Convenção além dos Estados da União Europeia, países de todos os continentes, desde os Estados Unidos de América, Canadá, Argentina, Chile, Colômbia, Gana, Marrocos, Cabo Verde, Austrália, Japão, Sri Lanka e Filipinas.

A adesão à Convenção terá, quando a seu tempo vier a ser equacionada, a vantagem de pertença a um espaço global de cooperação policial e judiciária. Em concreto, trará a possibilidade de, em processos a decorrer, se poderem vir a utilizar novas formas de investigação e novas vias de cooperação, quando se tornar necessário recorrer à cooperação internacional. Estas novas formas de investigar e de cooperar podem ser utilizadas não só quanto aos crimes previstos na Convenção, mas também na investigação dos outros crimes, desde que cometidos por via de sistemas de computadores e ainda para qualquer tipo de crimes, desde que haja prova dos mesmos em formato digital.

Numa outra perspetiva, a Convenção de Budapeste tem sido utilizada como modelo de legislação para maioria dos países no mundo. A Convenção estabelece, desde logo, um catálogo de crimes que constituiu um verdadeiro mínimo denominador comum dos crimes desta área. Nenhum deles está consagrado no direito timorense, com exceção da burla informática, já prevista no artigo 268º do Código Penal. Nessa matéria, o ordenamento jurídico interno revela-se manifestamente lacunoso.

E o mesmo se pode dizer em matéria processual, porquanto no que respeita a normas de direito processual penal, a desadequação da ordem jurídica nacional à essa nova realidade é ainda maior: a legislação processual penal timorense não dispõe de quaisquer normas especificamente vocacionadas para a investigação eficaz dos fenómenos de cibercriminalidade, se estiver em causa prova digital.

A presente opção legislativa é de condensar num único diploma legislativo o conjunto de todas as normas respeitantes à cibercriminalidade e não de introduzir alterações das várias fontes legislativas sobre esta matéria, ou seja, do Código Penal, Código de Processo Penal, e ainda do regime geral da cooperação judiciária internacional em matéria penal (Lei n.º 15/2011, de 26 de Outubro).
Esta opção legislativa afigura-se ser mais vantajosa, por haver necessidade de adequar a legislação nacional a realidades cruzadas das áreas penal e processual penal. Por outro lado, uma vez que se introduzem regras processuais específicas, mostra-se desadequado introduzir em diplomas estruturantes do ordenamento penal (*máxime* no Código de Processo Penal), regras especiais, apenas aplicáveis a uma parcela restrita de tipos de ilícito. Por outro, viu-se neste modelo a conveniência prática, para os operadores judiciários, de ver sistematizados todos os normativos referentes a um sector específico da criminalidade.

No que respeita ao direito penal material, em linha com a Convenção de Budapeste, introduzem-se os crimes de falsidade informática (Artigo 3.º), dano relativo a programas ou outros dados informáticos (Artigo 4.º), sabotagem informática (Artigo 5.º), acesso ilegítimo (Artigo 6.º), interceção ilegítima (Artigo 7.º), e pornografia infantil (Artigo 9.º) e pornografia de vingança (artigo 10.º). Foi ainda introduzido o crime de utilização indevida de dispositivo (Artigo 8.º).

Relativamente à responsabilidade de pessoas coletivas, considerando que o código penal remete para legislação especial quando e em que condições são responsabilizadas e na esteira da recomendação da Convenção de Budapeste, entendeu-se estabelecer um regime especial de responsabilização criminal de pessoas coletivas, relativamente aos crimes tipificados na presente lei e ainda a todos os crimes cometidos por via de sistemas de computadores e ainda para qualquer tipo de crimes, desde que haja prova dos mesmos em formato digital.

A propósito de competência jurisdicional do direito penal timorense fizeram-se ajustamentos ao que já atualmente se prevê no Código Penal. Designadamente previu-se a possibilidade de, independentemente do local da prática dos factos, Timor-Leste se julgar competente para prosseguir criminalmente atos dos seus cidadãos nacionais, se aos mesmos não for aplicável a lei penal de nenhum outro Estado, o mesmo se passando com atos cometidos em benefício de pessoas coletivas com sede em território timorense. Por outro lado, Timor-Leste declara-se competente para julgar factos fisicamente praticados em território timorense, ainda que visem sistemas informáticos localizados fora desse território ou factos que visem "atacar" sistemas informáticos localizados em território timorense, independentemente do local onde esses factos forem fisicamente praticados.

No que se refere às disposições processuais, foram introduzidas a preservação expedita de dados armazenados num computador e a preservação expedita e revelação de dados de tráfego (clara inspiração dos Artigos 16.º e 17.º da Convenção de Budapeste) e foi introduzido o mecanismo da injunção (igualmente prevista no Artigo 18º da Convenção). Por outro lado, consagraram-se regimes específicos de adaptação das buscas e das apreensões clássicas, já previstas na existente legislação processual penal, às investigações de crimes cometidos no ambiente virtual. Na verdade, a essência destas medidas processuais coincide, no ambiente do ciberespaço, com as clássicas formas de busca e apreensão, do processo penal; porém, a forma como a busca e a apreensão estão descritas no Código de Processo Penal não se enquadra nestas novas realidades.

No que respeita ao regime da interceção de comunicações eletrónicas, já detalhadamente previsto no Código de Processo Penal, apenas se consagrou neste novo diploma ser aplicável aos crimes tipificados na presente lei e ainda a todos os crimes cometidos por via de sistemas de computadores – o que não resultaria da aplicação do regime geral. Na verdade, o Código de Processo Penal já prevê a aplicação do regime das interceções telefónicas a outras comunicações diversa do telefone, por exemplo eletrónicas. Porém, o catálogo de crimes em que é permitido

proceder a estas medidas processuais não inclui os crimes que agora se introduzem, por via da presente lei. E também não inclui outros tipos de crime, de diversa natureza, cometidos por via de sistemas de computadores. Ora, quer quanto a uns, quer quanto a outros, com frequência é essencial recorrer a interceção de comunicações como única ou essencial forma de os investigar. Previu-se e regulou-se a admissibilidade de ações encobertas enquanto mecanismo especial de investigação, dotando assim o sistema de formas especiais de investigação quer para os crimes previstos na presente lei, quer para os cometidos por meio de sistema informático quando lhes corresponda, em abstrato, pena de pisão máximo superior a cinco anos ou ainda que a pena seja inferior, quando se trata de crimes contra a liberdade e auto determinação sexual em que os ofendidos sejam menores ou incapazes e também em relação às infrações económico-financeiras.

Inevitavelmente que constitui uma compressão das liberdades dos cidadãos no ciberespaço a aprovação, no âmbito de investigação de crimes informáticos, de medidas processuais especiais.

É compreensível para todos a enorme vantagem da existência de um espaço livre e praticamente desregulado, onde cada um pode livremente comunicar, informar-se e informar, bem como – e talvez acima de tudo –, expressar-se e manifestar-se sem censura nem constrangimentos. O uso, para fins legais, das redes de comunicação, trouxe avanços incomensuráveis à sociedade moderna.

No entanto, ninguém também hoje ignora que no sentido oposto, as redes de comunicação, tem sido utilizado para prática de atividades ilícitas, beneficiando das vantagens de comunicação massiva, eficaz e de custo reduzidíssimo, escolhendo as suas vítimas de forma quase indiscriminada, situado em qualquer parte do mundo e, resguardando-se das autoridades por detrás da trans territorialidade, do anonimato e da complexidade técnica.

Se não deixa de ser exato dizer-se que a Internet não é propriedade de ninguém, também não deixa de ser correto dizer-se que ninguém é diretamente responsável por ela nem pelo que nela ocorre. Não tem sede nem local onde se possam localizar os seus responsáveis.

As leis modernas têm que tratar de forma adequada estas novas realidades criminógenas, incriminando-as e dotando as entidades competentes das ferramentas necessárias à sua investigação e julgamento.

No que tange à cooperação internacional, remete-se, como regra, para o regime legal já em vigor. Além disso, assume-se que as autoridades timorenses podem solicitar cooperação internacional – e também receber e executar pedidos de cooperação provenientes de autoridades estrangeiras-, nas mesmas condições e circunstâncias em que atuariam se os factos criminosos estivessem a ser investigados em Timor-Leste. Cria-se um ponto permanente de contacto 24 horas/7dias, no seio da Polícia Científica de Investigação Criminal, ao qual compete assegurar, quanto à matéria a que respeita esta proposta de projeto de lei, a cooperação internacional emergente.

Por mandato do povo, a Parlamento Nacional decreta, nos termos das alíneas *a*) e *b*) n.º 1 do artigo 96º da Constituição, o seguinte:

CAPÍTULO I
Objeto e definições

Artigo 1º
Objeto

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

Artigo 2º
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 factos, 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 fixados 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 materiais condutores, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função eletrónica.

h) «Dados relativo a assinantes», quaisquer informações que um prestador de serviços possua sobre os assinantes dos seus serviços, sobre a forma de dados informáticos ou sob qualquer outra forma, destinta dos dados de tráfego ou de conteúdo e que permitem determinar, o tipo de serviço de comunicação utilizado, as medidas técnicas adaptadas a esse respeito, a duração do serviço, a identidade, o endereço postal ou geográfico e o número de telefone do assinante e qualquer outro número de acesso, bem como de dados referentes à faturação e ao pagamento, disponíveis com base no contrato ou um acordo de serviços, ou qualquer outra informação sobre localização do equipamento de comunicação disponível com base num contracto ou num acordo de prestação de serviços.

CAPÍTULO II
Disposições penais materiais

Artigo 3º
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 de 1 a 5 anos.

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 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 4º

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 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 3 o procedimento penal depende de queixa.

Artigo 5º

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 6º

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 ações não autorizadas descritas no número anterior.

3 - No caso previsto no n.º 1, 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 e 3 o procedimento penal depende de queixa.

Artigo 7º

Interceção 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 proveniente, é punido com pena de prisão até 3 anos ou com pena de multa.

2 - 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 ações não autorizadas descritas no mesmo número.

3- A tentativa é punível.

Artigo 8º

Utilização indevida de dispositivos

1 - Quem ilegitimamente produzir, vender, adquirir ou detiver, para efeitos de utilização, importação ou distribuição para fins comercial quaisquer dispositivos que permita o acesso a sistema ou meio de pagamento, incluindo programa informático, concebido ou adaptado antes de mais para permitir o acesso a sistema de comunicações ou serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das infrações previstas nos artigos 4.º a 7.º, é punido com pena de prisão de 1 a 5 anos.

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

3 - A tentativa é punível.

Artigo 9º

Pornografia infantil

1 - Quem, além do previsto no artigo 176.º do Código Penal:

a) produzir, distribuir, importar, exportar, divulgar, exibir ou ceder, a qualquer título ou por qualquer meio, fotografia, filme ou gravação pornográficos de menor de 17 anos;

b) adquirir ou detiver materiais previstos na alínea a), com o propósito de os distribuir, importar, exportar, divulgar, exibir ou ceder; é punido com pena de prisão de 1 a 5 anos.

2 - Quem produzir, distribuir, importar, exportar, divulgar, exibir ou ceder, a qualquer título ou por qualquer meio fotografia, filme ou gravação utilizando material pornográfico com representação realista de menor de 17 anos é punido com pena de prisão até 2 anos.

3 - Quem praticar os atos descritos nos números anteriores profissionalmente ou com intenção lucrativa é punido com pena de prisão de 1 a 8 anos.

4 - Quem adquirir ou detiver os materiais previstos na alínea *a*) do n.º 1 e no n.º 2 é punido com pena de prisão até 1 ano.

5 - A tentativa é punível.

6 - As penas previstas nos números 1 a 4 são agravadas em um terço nos seus limites mínimo e máximo, se a vítima for ascendente ou descendente, ou se encontrar sob tutela do agente, desde que as circunstâncias do caso revelem um acentuado grau de ilicitude do facto ou da culpa do agente.

7 - As penas previstas nos números 1 a 4 são agravadas em metade, nos seus limites mínimo e máximo, se a vítima for menor de 14 anos.

8 - Se no mesmo comportamento concorrerem mais do que uma das circunstâncias referidas nos números anteriores, só é considerada para efeito de determinação da pena aplicável a que tiver efeito agravante mais forte, sendo a outra valorada na medida da pena.

9 - Quem for condenado por crime previsto no presente artigo pode, atenta a concreta gravidade do facto e a sua conexão com a função exercida pelo agente, ser inibido do exercício do poder paternal, da tutela ou curatela, ou proibido do exercício de profissão, função ou atividade que impliquem ter menores sob sua responsabilidade, educação, tratamento ou vigilância, por um período de 2 a 15 anos.

Artigo 10º

Pornografia de vingança

Quem sem permissão legal ou sem para tanto estar autorizado, divulgar ou ameaçar divulgar através de um sistema informático, fotos, vídeos ou qualquer outro material de conteúdo

sexualmente íntimo e privado, consentido ou não, de uma pessoa com a qual mantém ou manteve relação íntima, com propósito de causar danos morais e psicológicos à vítima, é punido com pena de prisão até 2 anos ou com pena de multa de 80 a 200 dias.

Artigo 11º

Responsabilidade penal das pessoas coletivas e entidades equiparadas

1 - As pessoas coletivas e entidades equiparadas, com exceção do Estado, de outras pessoas coletivas públicas e de organizações internacionais de direito público, são responsáveis pelos crimes tipificados na presente lei, pelos crimes cometidos por via de sistemas de computadores e ainda para qualquer tipo de crimes, desde que haja prova dos mesmos em formato digital, quando cometidos:

a) Em seu nome e no interesse coletivo por pessoas que nelas ocupem uma posição de liderança;

b) Por quem aja sob a autoridade das pessoas referidas na alínea anterior em virtude de uma violação dos deveres de vigilância ou controlo que lhes incumbem;

2 - Para efeito da presente lei a expressão pessoas coletivas públicas abrange:

a) Pessoas coletivas de direito público, nas quais se incluem as entidades públicas empresariais;

b) Entidades concessionárias de serviços públicos, independentemente da sua titularidade;

c) Demais pessoas coletivas que exerçam prerrogativas de poder público.

3 - Entende-se que ocupam uma posição de liderança os órgãos e representantes da pessoa coletiva a quem nela tiver autoridade para exercer o controlo das suas atividades.

4 - Para efeitos de responsabilidade criminal consideram-se entidades equiparadas a pessoas coletivas as sociedades civis e as associações de facto.

5 - A responsabilidade das pessoas coletivas e entidades equiparadas é excluída quando o agente tiver atuado contra ordens ou instruções expressas de quem de direito.

6 - A responsabilidade das pessoas coletivas e entidades equiparadas não exclui a responsabilidade individual dos respetivos agentes nem depende da responsabilização destes.

7 - A cisão ou fusão não determinam a extinção da responsabilidade criminal da pessoa coletiva ou entidade equiparada, respondendo pela prática do crime:

a) A pessoa coletiva ou entidade equiparada em que a fusão se tiver efetivado; e

b) As pessoas coletivas ou entidades equiparadas que resultarem da cisão.

8 - Sem prejuízo do direito de regresso, as pessoas que ocupam uma posição de liderança são subsidiariamente responsáveis pelo pagamento das multas e indemnizações em que a pessoa coletiva ou entidade equiparada for condenada, relativamente aos crimes:

a) Praticados no período de exercício do seu cargo, sem a sua oposição expressa;

b) Praticados anteriormente, quando tiver sido por culpa sua que o património da pessoa coletiva ou entidade equiparada se tornou insuficiente para o respetivo pagamento; ou

c) Praticados anteriormente, quando a decisão definitiva de as aplicar tiver sido notificada durante o período de exercício do seu cargo e lhes seja imputável a falta de pagamento.

9 - Sendo várias as pessoas responsáveis nos termos do número anterior, é solidaria a sua responsabilidade.

10 - Se a multa ou indemnização forem aplicadas a uma entidade sem personalidade jurídica, responde por elas o património comum e, na sua falta ou insuficiência, solidariamente, o património e cada um dos associados.

11 - Pelos crimes previstos no n.º 1 do presente artigo são aplicáveis às pessoas coletivas e entidades equiparadas as penas principais de multa ou de dissolução.

12 - Pelos mesmos crimes podem ser aplicados às pessoas coletivas e entidades equiparadas as seguintes penas acessórias:

a) Injunção judiciária;

b) Interdição de exercício de atividade;

c) Proibição de celebrar certos contratos ou contratos com determinadas entidades;

d) Privação do direito a subsídio, subvenções ou incentivos;

e) Encerramento de estabelecimento;

f) Publicidade da decisão condenatória às suas expensas.

Artigo 12º

Pena de multa

1- Os limites mínimos e máximos da pena de multa aplicáveis às pessoas coletivas e entidades equiparadas são determinadas tendo como referência a pena de prisão prevista para as pessoas singulares.

2- Um mês de prisão corresponde, para as pessoas coletivas e entidades equiparadas, a 10 dias de multa.

3- Sempre que a pena de aplicável às pessoas singulares estiver determinada exclusiva ou alternativamente em multa, são aplicáveis às pessoas coletivas ou entidades equiparadas os mesmos dias de multa.

4- A pena de multa é fixada em dias, de acordo com os critérios estabelecidos no n.º 1 do artigo 51.º do código penal.

5- Cada dia de multa corresponde a uma quantia entre 100 e 10.000 dólares norte-americano que o tribunal fixa em função da situação económica e financeira do condenado e dos seus encargos com trabalhadores, sendo aplicável o disposto no n.º 3 do artigo 75.º do código penal.

6- Findo o prazo de pagamento de multa ou de alguma das suas prestações sem que o pagamento seja efetuado, proceder-se à execução do património da pessoa coletiva ou entidade equiparada.

7- A multa que não for voluntaria ou coercivamente paga não pode ser convertida em prisão subsidiária.

Artigo 13º

Perda de bens relacionados com o crime

1 - Sem prejuízo da aplicação do regime geral, previsto no artigo 102.º e seguintes do Código Penal, o tribunal 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 – Os bens referidos no número 1 podem ser utilizados provisoriamente pelos órgãos de polícia criminal, através de declaração de utilidade operacional, desde a sua apreensão até a declaração de perda ou restituição, quando sejam suscetíveis de, findo o processo, virem a ser declarados perdidos a favor do Estado.

3 - Para efeitos do previsto no número anterior são notificados os interessados.

4 - Efetuada a apreensão e constatada a utilidade operacional do bem, será o mesmo registado, examinado e avaliado.

5 - O valor da avaliação determina a quantia a pagar ao proprietário a título de indemnização, caso o bem não venha, a final, a ser declarado perdido a favor do Estado.

6 - A avaliação do bem é efetuada por peritos nomeados pela autoridade judiciária a quem o compromisso de cumprimento da função lhe é cometido.

7 - A declaração de cessação de utilidade operacional cessam com a declaração de perda a favor do Estado ou a restituição ao dono ou legítimo titular.

CAPÍTULO III
Disposições processuais

Artigo 14º
Âmbito de aplicação das disposições processuais

Com exceção 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 eletrónico.

Artigo 15º
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, o Ministério Público ou o juíz, consoante a fase processual,

ordenam 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 do Ministério Público ou do juíz, consoante a fase processual, ou quando haja urgência ou perigo na demora, devendo neste último caso ser de imediato dada notícia do facto ao Ministério Público ou ao juíz, mediante a descrição dos factos 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 seis 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 ao Ministério Público ou ao juiz a sua obtenção, e fica obrigado a assegurar a confidencialidade da aplicação da medida processual.

5 - O Ministério Público ou o juiz podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do nº 3, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 16º

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 ao Ministério Público, ao juiz 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 17º

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, o Ministério Público ou o juiz, consoante a fase processual, ordenam 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 ao Ministério Públio ou ao juiz, 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 especificamente utilizados no exercício da atividade profissional das pessoas sujeitas ao dever de segredo, referidas no n.º 1 do Artigo 126º do Código de Processo Penal.

7 – O regime de segredo profissional ou de funcionário e de segredo de Estado previstos nos artigos 126.º, 127.º e 128.º do código de processo penal é aplicável com as necessárias adaptações.

Artigo 18º

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, o Ministério Público ou o juíz, consoante a fase processual, autorizam ou ordenam 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 do Ministério Público ou do juíz, 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 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 ao Ministério Público ou juiz, consoante a fase processual, e por esta apreciada em ordem à sua validação;
b) Em qualquer caso, é elaborado e remetido o Ministério Público ou juíz, consoante a fase processual, relatório na qual mencionam, de forma resumida, as investigações levadas a cabo, os resultados das mesmas, a descrição dos factos 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 do Ministério Público ou do juíz, nos termos dos números 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 19º

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, o Ministério Público ou o juíz, consoante a fase processual, autorizam ou ordenam 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 de dados relativas a sistemas informáticos utilizados para o exercício de profissões ou funções vinculadas a segredo, estão sujeitas, com as necessárias adaptações, às regras e formalidades previstas no artigo 226.º do Código de Processo Penal.

6 – As apreensões relativas a sistemas informáticos utilizados para exercício de atividades das pessoas indicadas nos artigos 126.º, 127.º e 128.º do código de processo penal estão sujeitas, com as necessárias adaptações, às regras e formalidade previstas no código de processo penal.

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 20º

Apreensão de correio eletrónico e registos de comunicações de natureza semelhante

1 – Se, 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, os mesmos são provisoriamente apreendidos pelo órgão de polícia criminal que proceder à pesquisa ou a outro acesso legítimo ao sistema.

2 - Vistos aqueles registos, os mesmos são levados ao juiz para que ordene a respetiva junção ao processo, se a apreensão se afigurar ser de grande interesse para a descoberta da verdade ou para a prova.

3 - Naquilo que não estiver previsto nos números anteriores, aplica-se subsidiariamente a esta apreensão o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 21º

Interceção de comunicações

1 – É admissível o recurso à interceção 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 á recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 177.º do código de processo penal.

2 – A interceção 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 competente e mediante requerimento do Ministério Público.

3 - A interceção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e o registo de dados de tráfico, devendo o despacho referido no número anterior especificar o respetivo âmbito, de acordo com as necessidades concretas da investigação.

4 – Em tudo que não for contrariado pelo presente artigo, à interceção e o registo de transmissões de dados informáticos é aplicável o regime da interceção e gravação de conversas ou comunicações telefónicas constantes dos artigos 177.º e 178.º do código de processo penal.

Artigo 22º

Ações encobertas

1 – É admissível o recurso às ações encobertas no decurso do inquérito relativo aos seguintes crimes:

a) Os previstos na presente lei;
b) Os cometidos por meio de um sistema informático, em abstrato, pena de prisão 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, burla qualificada, bula 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 interceção de comunicações.

3 - Consideram-se ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sobre o controlo da Polícia Científica de

Investigação Criminal, na investigação dos crimes indicados na presente lei, com ocultação da sua qualidade e identidade.

4 - A autorização para realização da ação encoberta é dada pelo juiz de turno, no prazo máximo de 48 horas, mediante proposta do Ministério Público, devendo constar da mesma os fundamentos, a descrição sumária da operação, e, sempre que possível, ser ponderada a necessidade e segurança da operação.

5 - A Polícia Científica de Investigação Criminal faz relatório da intervenção do agente encoberto ao Ministério Público, no prazo máximo de 48 horas após o termo daquela.

6 - Ninguém pode ser obrigado a participar em ação encoberta.

7 - Pode ser dispensada a presença em audiência de julgamento do funcionário de investigação criminal ou do terceiro que atuou com ocultação de identidade, nos termos da Lei n.º 2/2009, de 6 de Maio, que regula a aplicação de medidas de proteção de testemunhas e outros intervenientes no processo penal.

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 eletrónico, de um crime nos termos da presente lei e, naquilo que nela não se previr, nos termos do regime geral da cooperação judiciária internacional em matéria penal, previsto na Lei n.º 15/2011, de 26 de Outubro.

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 Procuradoria-Geral da República 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, sem prejuízo de delegação de competência na Polícia Científica de Investigação Criminal.

2 - Este ponto de contacto pode ser contactado por outros pontos de contacto, nos termos de acordos, tratados ou convenções a que Timor-Leste 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 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*) *d*o número anterior, a Polícia Científica de Investigação Criminal dá notícia imediata do facto 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 factos apurados e as provas recolhidas.

Artigo 25º

Preservação e revelação expeditas de dados informáticos em cooperação internacional

1 - Pode ser solicitada a Timor-Leste a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 14º, 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 factos relacionados;
c) Os dados informáticos a conservar e a sua relação com a infração;
d) Todas as informações disponíveis que permitam identificarem 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, o Ministério Público ou o juiz, consoante o caso, 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 Científica de Investigação Criminal mediante autorização do Ministério Público ou do juíz, 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 seis meses.

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

7 – O Ministério Público ou o juíz, consoante o caso, ou a Polícia Científica de Investigação Criminal mediante autorização daqueles, pode 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, o Ministério Público ou o juíz, consoante o caso, determinam a preservação dos dados até à adoção de uma decisão final sobre o pedido.

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

a) À autoridade judiciária estrangeira 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 16.º a 20.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 16.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 estrangeira 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 a autoridades estrangeiras.

Artigo 26º

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 conceções do direito timorense, ou
b) Atentar contra a soberania, segurança, ordem pública ou outros interesses da República de Timor-Leste, constitucionalmente definidos;
c) O Estado terceiro requisitante não oferecer garantias adequadas de proteção de 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 27º

Acesso a dados informáticos em cooperação internacional

1 - Em execução de pedido de autoridade estrangeira competente, o Ministério Público ou o juiz, consoante o caso, podem ordenar a pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Timor-Leste, relativos a crimes previstos no artigo 14.º, quando se trata de situação em que a pesquisa e apreensão seriam admissíveis em caso nacional semelhante.

2 - O Ministério Público ou o juiz ordenam a pesquisa e apreensão 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 timorenses a autoridades estrangeiras.

Artigo 28º

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

As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades timorense, no respeito pelas regras sobre transferência de dados pessoais, podem:

a) Aceder a dados informáticos armazenados em sistema informático localizado em Timor-Leste, quando publicamente disponíveis;
b) Receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Timor-Leste, mediante consentimento legal e voluntário de pessoa legalmente autorizada a divulga-los.

Artigo 29º

Interceção de comunicações em cooperação internacional

1 - Em execução de pedido da autoridade estrangeira competente, pode ser autorizada pelo juiz a interceção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Timor-Leste, desde que tal esteja previsto em acordo, tratado ou convenção

internacional e se trate de situação em que tal interceção seja admissível, nos termos do artigo 21.º, em caso nacional semelhante.

2 – É competente para receção dos pedidos de interceção a Polícia Científica de Investigação Criminal, que os apresentará ao Ministério Público, para que os apresente ao juiz competente no Tribunal Judicial da Primeira Instância para autorização.

3 - A autorização referida no número 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 timorenses a autoridades estrangeiras.

CAPÍTULO V
Disposições finais e transitórias

Artigo 30º
Aplicação no espaço da lei penal timorense e competência dos tribunais timorenses

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

a) Praticados por timorenses, se aos mesmos não for aplicável a lei penal de nenhum outro Estado;
b) Cometidos em benefício de pessoas coletivas com sede em território timorense;
c) Fisicamente praticados em território timorense, ainda que visem sistemas informáticos localizados fora desse território; ou
d) Que visem sistemas informáticos localizados em território timorense, independentemente do local onde esses factos forem fisicamente praticados; ou
e) Praticados por timorenses ou estrangeiro que se encontrar em território timorense ou para aqui se deslocar ou for encontrado.

2 - Se, em função da aplicabilidade da lei penal timorense, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente lei os tribunais timorenses e tribunais

estrangeiros, podendo em qualquer um deles ser validamente instaurado ou prosseguido o procedimento penal com base nos mesmos factos, a autoridade judiciária competente aos órgãos e mecanismos previstos na lei da 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 de procedimento é tomada pela autoridade judiciária competente, tendo em conta, sucessivamente, os seguintes elementos:

a) O local onde foi praticado a infração;
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 atuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos.

Artigo 31º

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 n.º 15/2011, de 26 de Outubro de 2011.

Artigo 32º

Competência da Polícia Científica de Investigação Criminal para cooperação internacional

A competência atribuída pela presente lei à Polícia Científica de Investigação Criminal para efeitos de cooperação internacional em matéria penal nela prevista é desempenhada pela unidade orgânica a quem se encontra cometida a investigação dos crimes previstos na presente lei.

Artigo 33º

Proteção de dados pessoais

O tratamento de dados pessoais ao abrigo da presente lei efetua-se de acordo com o disposto na legislação específica aprovada.

Artigo 34º

Entrada em vigor

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

Aprovada em dia ...

O Presidente do Parlamento Nacional,

Maria Fernanda Lay

Promulgada em dia ...

Publique -se.

O Presidente da República,

José Manuel Ramos Horta