DECRETO N.º 167/XIV

Transpõe a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, alterando o Código Penal, o Código de Processo Penal, a Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, e outros atos legislativos

A Assembleia da República decreta, nos termos da alínea *c*) do artigo 161.º da Constituição, o seguinte:

Artigo 1.º
Objeto

A presente lei transpõe para a ordem jurídica interna a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho, procedendo à:

a) Sétima alteração à Lei n.º 5/2002, de 11 de janeiro, que estabelece medidas de combate à criminalidade organizada e económico-financeira;
b) Sexta alteração à Lei n.º 52/2003, de 22 de agosto, que aprova a lei de combate ao terrorismo;
c) Primeira alteração à Lei n.º 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações;
d) Primeira alteração à Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime;

e) Terceira alteração à Lei n.º 22/2013, de 26 de fevereiro, que estabelece o estatuto do administrador judicial;

f) Segunda alteração ao Estatuto da Ordem dos Advogados, aprovado em anexo à Lei n.º 145/2015, de 9 de setembro;

g) Primeira alteração ao Estatuto da Ordem dos Solicitadores e dos Agentes de Execução, aprovado pela Lei n.º 154/2015, de 14 de setembro;

h) Segunda alteração ao Estatuto da Ordem dos Notários, aprovado pela Lei n.º 155/2015, de 15 de setembro;

i) Primeira alteração à Lei n.º 6/2018, de 22 de fevereiro, que estabelece o estatuto do mediador de recuperação de empresas;

j) Alteração ao Código Penal, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro;

k) Sétima alteração ao Estatuto das Instituições Particulares de Solidariedade Social, aprovado pelo Decreto-Lei n.º 119/83, de 25 de fevereiro,

l) Alteração ao Código de Processo Penal, aprovado pelo Decreto Lei n.º 78/87, de 17 de fevereiro;

m) Primeira alteração ao Decreto-Lei n.º 12/2021, de 9 de fevereiro, que assegura a execução na ordem jurídica interna do Regulamento (UE) 910/2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno;

n) Quinta alteração ao Regulamento da Caixa de Previdência dos Advogados e Solicitadores, aprovado pelo Decreto-Lei n.º 119/2015, de 29 de junho;

o) Alteração ao Código das Associações Mutualistas, aprovado em anexo ao Decreto-Lei n.º 59/2018, de 2 de agosto;

p) Primeira alteração ao Decreto-Lei n.º 137/2019, de 13 de setembro, que aprova a nova estrutura organizacional da Polícia Judiciária.

Artigo 2.º

Alteração à Lei n.º 5/2002, de 11 de janeiro

O artigo 1.º da Lei n.º 5/2002, de 11 de janeiro, passa a ter a seguinte redação:

«Artigo 1.º

[…]

1 – […]:

a) […];

b) […];

c) […];

d) […];

e) […];

f) […];

g) […];

h) […];

i) […];

j) […];

l) […];

m) […];

n) […];

o) Contrafação, uso e aquisição de cartões ou outros dispositivos de pagamento contrafeitos e respetivos atos preparatórios, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, dano relativo a programas ou outros dados informáticos e sabotagem informática, nos termos dos artigos 3.º-A, 3.º-B, 3.º-C, 3.º-D, 3.º-E, 4.º e 5.º da Lei n.º 109/2009, de 15 de setembro, e ainda o acesso ilegítimo a sistema informático, se tiver produzido um dos resultados previstos nas alíneas *a*) e *b*) do n.º 5 do artigo 6.º daquela lei, for realizado com recurso a um dos instrumentos referidos no n.º 2 do mesmo artigo, ou integrar uma das condutas aí tipificadas;

p) […];

q) […];

r) […].

2 – […].

3 – […].

4 – […].»

Artigo 3.º

Alteração à Lei n.º 52/2003, de 22 de agosto

O artigo 4.º da Lei n.º 52/2003, de 22 de agosto, passa a ter a seguinte redação:

«Artigo 4.º

[…]

1 – […].

2 – Quem praticar crime de furto qualificado, roubo, extorsão, burla informática e nas comunicações, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, falsidade informática, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação ou falsificação de documento com vista ao cometimento dos factos previstos no n.º 1 do artigo 2.º, é punido com a pena correspondente ao crime praticado, agravada em um terço nos seus limites mínimo e máximo.

3 – […].

4 – […].

5 – […].

6 – […].

7 – […].

8 – […].

9 – […].

10 – […].

11 – […].

12 – […].

13 – […].»

Artigo 4.º

Alteração à Lei n.º 32/2008, de 17 de julho

O artigo 2.º da Lei n.º 32/2008, de 17 de julho, passa a ter a seguinte redação:

«Artigo 2.º

[…]

1 – […]:

a) […];

b) […];

c) […];

d) […];

e) […];

f) […];

g) «Crime grave», crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

2 – […].»

Artigo 5.º

Alteração à Lei n.º 109/2009, de 15 de setembro

Os artigos 3.º, 6.º, 17.º, 19.º, 20.º, 21.º, 25.º e 30.º da Lei n.º 109/2009, de 15 de setembro, passam a ter a seguinte redação:

«Artigo 3.º

[…]

1 – […].

2 – Quando as ações descritas no número anterior incidirem sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso 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 dispositivo no qual se encontrem registados, incorporados ou ao qual respeitem os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.

4 – Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos destinados à prática das ações previstas no n.º 2, é punido com pena de prisão de 1 a 5 anos.

5 – […].

Artigo 6.º

[…]

1 – […].

2 – […].

3 – A pena é de prisão até 2 anos ou multa até 240 dias se as ações descritas no número anterior se destinarem ao acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

4 – A pena é de prisão até 3 anos ou multa se:

a) O acesso for conseguido através de violação de regras de segurança; ou

b) Através do acesso, o agente obtiver dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

5 – (*Anterior n.º 4*).

6 – A tentativa é punível, salvo nos casos previstos nos n.os 2 e 3.

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

Artigo 17.º

Apreensão de mensagens de correio eletrónico ou de natureza semelhante

1 – Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontradas, armazenadas nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou de natureza semelhante que sejam necessárias à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a sua apreensão.

2 – O órgão de polícia criminal pode efetuar as apreensões referidas no número anterior, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, bem como quando haja urgência ou perigo na demora, devendo tal apreensão ser validada pela autoridade judiciária no prazo máximo de 72 horas.

3 – À apreensão de mensagens de correio eletrónico e de natureza semelhante aplica-se o disposto nos n.os 5 a 8 do artigo anterior.

4 – O Ministério Público apresenta ao juiz, sob pena de nulidade, as mensagens de correio eletrónico ou de natureza semelhante cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto.

5 – Os suportes técnicos que contenham as mensagens apreendidas cuja junção não tenha sido determinada pelo juiz são guardados em envelope lacrado, à ordem do tribunal, e destruídos após o trânsito em julgado da decisão que puser termo ao processo.

6 – No que não se encontrar previsto nos números anteriores, é aplicável, com as necessárias adaptações, o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 19.º

[…]

1 – […]:

a) […];

b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, o abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.

2 – […].

Artigo 20.º

[…]

As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 59/2019, de 8 de agosto.

Artigo 21.º

[…]

1 – […].

2 – […].

3 – […].

4 – […].

5 – O Ministério Público deve, de modo a responder prontamente a pedidos de assistência imediata, assegurar a disponibilidade de magistrados e meios técnicos para levar a cabo quaisquer intervenções processuais urgentes da sua competência.

Artigo 25.º

[…]

As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 59/2019, de 8 de agosto, podem:

a) […];

b) […].

Artigo 30.º

[…]

O tratamento de dados pessoais ao abrigo da presente lei efetua-se nos termos da Lei n.º 59/2019, de 8 de agosto, sendo aplicável, em caso de violação, o disposto no respetivo capítulo VII.»

Artigo 6.º

Aditamento à Lei n.º 109/2009, de 15 de setembro

São aditados à Lei n.º 109/2009, de 15 de setembro, os artigos 3.º-A, 3.º-B, 3.º-C, 3.º-D, 3.º-E, 3.º-F e 3.º-G, com a seguinte redação:

«Artigo 3.º-A

Contrafação de cartões ou outros dispositivos de pagamento

Quem, com intenção de provocar engano nas relações jurídicas, contrafizer cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, nomeadamente introduzindo, modificando, apagando, suprimindo ou interferindo, por qualquer outro modo, num tratamento informático de dados registados, incorporados ou respeitantes a estes cartões ou dispositivos, é punido com pena de prisão de 3 a 12 anos.

Artigo 3.º-B

Uso de cartões ou outros dispositivos de pagamento contrafeitos

1 – Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar cartão de pagamento contrafeito, ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos.

2 – As ações descritas no número anterior são punidas com pena de prisão de 2 a 8 anos se o prejuízo ou o benefício for de valor consideravelmente elevado.

3 – As ações descritas no n.º 1 são punidas com pena de prisão de 3 a 12 anos se o agente as praticar de concerto com o agente dos factos descritos no artigo 3.º-A.

Artigo 3.º-C

Aquisição de cartões ou outros dispositivos de pagamento contrafeitos

Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar cartão de pagamento contrafeito ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos.

Artigo 3.º-D

Atos preparatórios da contrafação

Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer cartão, dispositivo, programa ou outros dados informáticos, ou quaisquer outros instrumentos, informáticos ou não, destinados à prática das ações descritas no artigo 3.º-A, é punido com pena de prisão de 1 a 5 anos.

Artigo 3.º-E

Aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático

Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar:

a) Dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que hajam sido obtidos mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;
b) Cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que haja sido obtido mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;

é punido com pena de prisão de 1 a 5 anos.

Artigo 3.º-F

Agravação

Se os factos referidos nos artigos 3.º-A a 3.º-E forem praticados por funcionário no exercício das suas funções, o limite mínimo da pena de prisão aplicável é:

a) De 2 anos, tratando-se dos factos previstos no n.º 1 do artigo 3.º-B, no n.º 1 do artigo 3.º-C, no artigo 3.º-D e no artigo 3.º-E;

b) Agravado em um terço, nos restantes casos.

Artigo 3.º-G

Moeda virtual

Para efeitos da presente lei, considera-se também sistema ou meio de pagamento aquele que tenha por objeto moeda virtual.»

Artigo 7.º

Alteração à Lei n.º 22/2013, de 26 de fevereiro

O artigo 5.º da Lei n.º 22/2013, de 26 de fevereiro, passa a ter a seguinte redação:

«Artigo 5.º

[…]

1 – […].

2 – […]:

a) Condenada com trânsito em julgado, no país ou no estrangeiro, por crime de furto, roubo, burla, burla informática e nas comunicações, extorsão, abuso de confiança, recetação, infidelidade, falsificação, falsas declarações, insolvência dolosa, frustração de créditos, insolvência negligente, favorecimento de credores, emissão de cheques sem provisão, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, apropriação ilegítima de bens do sector público ou cooperativo, administração danosa em unidade económica do sector público ou cooperativo, usura, suborno, corrupção, tráfico de influência, peculato, receção não autorizada de depósitos ou outros fundos reembolsáveis, prática ilícita de atos ou operações inerentes à atividade seguradora ou dos fundos de pensões, fraude fiscal ou outro crime tributário, branqueamento de capitais, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, ou crime previsto no Código das Sociedades Comerciais ou no Código dos Valores Mobiliários;

b) […].

3 – […].

4 – […].»

Artigo 8.º

Alteração ao Estatuto da Ordem dos Advogados

O artigo 177.º do Estatuto da Ordem dos Advogados, aprovado em anexo à Lei n.º 145/2015, de 9 de setembro, passa a ter a seguinte redação:

«Artigo 177.º

[…]

1 – […].

2 – Para efeitos do disposto na alínea *a*) do número anterior, consideram–se crimes gravemente desonrosos para o exercício da profissão, designadamente, os crimes de furto, roubo, burla, burla informática e nas comunicações, extorsão, abuso de confiança, recetação, infidelidade, falsificação, falsas declarações, insolvência dolosa, frustração de créditos, insolvência negligente, favorecimento de credores, emissão de cheques sem provisão, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, apropriação ilegítima de bens do sector público ou cooperativo, administração danosa em unidade económica do sector público ou cooperativo, usura, suborno, corrupção, tráfico de influência, peculato, receção não autorizada de depósitos ou outros fundos reembolsáveis, prática ilícita de atos ou operações inerentes à atividade seguradora ou dos fundos de pensões, fraude fiscal ou outro crime tributário, branqueamento de capitais, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, ou crime previsto no Código das Sociedades Comerciais, no Código dos Valores Mobiliários ou na alínea *h)* do n.º 1 do artigo 55.º do Código dos Contratos Públicos.»

Artigo 9.º

Alteração ao Estatuto da Ordem dos Solicitadores e dos Agentes de Execução

O artigo 106.º do Estatuto da Ordem dos Solicitadores e dos Agentes de Execução, aprovado em anexo à Lei n.º 154/2015, de 14 de setembro, passa a ter a seguinte redação:

«Artigo 106.º

[…]

1 – […].

2 – […].

3 – […].

4 – Para efeitos do disposto na alínea *a*) do número anterior, consideram–se crimes desonrosos para o exercício da profissão, designadamente, os crimes de furto, roubo, burla, burla informática e nas comunicações, extorsão, abuso de confiança, recetação, infidelidade, falsificação, falsas declarações, insolvência dolosa, frustração de créditos, insolvência negligente, favorecimento de credores, emissão de cheques sem provisão, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, apropriação ilegítima de bens do sector público ou cooperativo, administração danosa em unidade económica do sector público ou cooperativo, usura, suborno, corrupção, tráfico de influência, peculato, receção não autorizada de depósitos ou outros fundos reembolsáveis, prática ilícita de atos ou operações inerentes à atividade seguradora ou dos fundos de pensões, fraude fiscal ou outro crime tributário, branqueamento de capitais, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, ou crime previsto no Código das Sociedades Comerciais, no Código dos Valores Mobiliários, ou na alínea *h*) do n.º 1 do artigo 55.º do Código dos Contratos Públicos.

5 – […].

6 – […].

7 – […].

8 – […].

9 – […].»

Artigo 10.º

Alteração ao Estatuto da Ordem dos Notários

O artigo 70.º do Estatuto da Ordem dos Notários, aprovado em anexo à Lei n.º 155/2015, de 15 de setembro, passa a ter a seguinte redação:

«Artigo 70.º

[…]

1 – […].

2 – […].

3 – Para efeitos do disposto na alínea *a*) do número anterior, presumem–se não idóneos para o exercício da profissão, designadamente, os condenados por qualquer crime gravemente desonroso para o exercício da profissão, considerando-se como tal os crimes de furto, roubo, burla, burla informática e nas comunicações, extorsão, abuso de confiança, recetação, infidelidade, falsificação, falsas declarações, insolvência dolosa, frustração de créditos, insolvência negligente, favorecimento de credores, emissão de cheques sem provisão, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, apropriação ilegítima de bens do sector público ou cooperativo, administração danosa em unidade económica do sector público ou cooperativo, usura, suborno, corrupção, tráfico de influência, peculato, receção não autorizada de depósitos ou outros fundos reembolsáveis, prática ilícita de atos ou operações inerentes à atividade seguradora ou dos fundos de pensões, fraude fiscal ou outro crime tributário, branqueamento de capitais, contrafação de cartões ou outros dispositivos de pagamento, uso de

cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, ou crime previsto no Código das Sociedades Comerciais, no Código dos Valores Mobiliários, ou na alínea *h)* do n.º 1 do artigo 55.º do Código dos Contratos Públicos.

4 – […].

5 – […].

6 – […].

7 – […].

8 – […].

9 – […].»

Artigo 11.º

Alteração à Lei n.º 6/2018, de 22 de fevereiro

O artigo 5.º da Lei n.º 6/2018, de 22 de fevereiro, passa a ter a seguinte redação:

«Artigo 5.º

[…]

1 – […].

2 – […].

3 – […].

4 – […]:

a) […];

b) […];

c) […];

d) […];

e) […];

f) […];

g) […];

h) Condenação, com trânsito em julgado, no país ou no estrangeiro, por crime de furto, roubo, burla, burla informática e nas comunicações, extorsão, abuso de confiança, recetação, infidelidade, falsificação, falsas declarações, insolvência dolosa, frustração de créditos, insolvência negligente, favorecimento de credores, emissão de cheques sem provisão, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, apropriação ilegítima de bens do sector público ou cooperativo, administração danosa em unidade económica do sector público ou cooperativo, usura, suborno, corrupção, tráfico de influência, peculato, receção não autorizada de depósitos ou outros fundos reembolsáveis, prática ilícita de atos ou operações inerentes à atividade seguradora ou dos fundos de pensões, fraude fiscal ou outro crime tributário, branqueamento de capitais, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, ou crime previsto no Código das Sociedades Comerciais ou no Código dos Valores Mobiliários.

i) […];

j) […].

5 – […].

6 – […].»

Artigo 12.º

Alteração ao Código Penal

Os artigos 11.º, 61.º, 74.º, 99.º, 221.º, 225.º, 267.º e 368.º-A do Código Penal, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro, passam a ter a seguinte redação:

«Artigo 11.º

[…]

1 – […].

2 – As pessoas coletivas e entidades equiparadas, com exceção do Estado, de pessoas coletivas no exercício de prerrogativas de poder público e de organizações de direito internacional público, são responsáveis pelos crimes previstos nos artigos 144.º-B, 152.º-A, 152.º-B, 159.º e 160.º, nos artigos 163.º a 166.º sendo a vítima menor, e nos artigos 168.º, 169.º, 171.º a 176.º, 203.º a 205.º, 209.º a 211.º, 217.º a 223.º, 225.º, 231.º, 232.º, 240.º, 256.º, 258.º, 262.º a 283.º, 285,º 299.º, 335.º, 348.º, 353.º, 363.º, 367.º, 368.º-A e 372.º a 376.º, quando cometidos:

a) […];

b) […].

3 – […].

4 – […].

5 – […].

6 – […].

7 – […].

8 – […].

9 – […].

10 – […].

11 – […].

Artigo 61.º

[…]

1 – […].

2 – […]:

a) […];

b) A libertação se revelar compatível com a defesa da ordem jurídica e da paz social.

3 – […].

4 – […].

5 – […].

6 – […].

Artigo 74.º

[…]

1 – Quando o crime for punível com pena de prisão não superior a 6 meses, ou só com multa não superior a 120 dias, pode o tribunal declarar o arguido culpado mas não aplicar qualquer pena se:

a) […];

b) […];

c) […].

2 – […].

3 – […].

Artigo 99.º

[…]

1 – […].

2 – […].

3 – […].

4 – […].

5 – É correspondentemente aplicável o disposto nos n.os 1 e 4 do artigo 61.º.

6 – […].

Artigo 221.º

[…]

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

2 – […].

3 – […].

4 – […].

5 – […].

6 – […].

Artigo 225.º

Abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento

1 – Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, usar:

a) Cartão de garantia;

b) Cartão de pagamento;

c) Qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento;

d) Dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou a meio de pagamento;

determinando o depósito, a transferência, o levantamento ou, por qualquer outra forma, o pagamento de moeda, incluindo a escritural, a eletrónica ou a virtual, e causar, desse modo, prejuízo patrimonial a outra pessoa, é punido com pena de prisão até 3 anos ou com pena de multa.

2 – […].

3 – […].

4 – […].

5 – […].

6 – […].

Artigo 267.º

[…]

1 – […]:

a) […];

b) […];

c) Os cartões de garantia.

2 – […].

Artigo 368.º-A

[…]

1 – […]:

a) […];

b) Burla informática e nas comunicações, extorsão, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, contrafação de moeda ou de títulos equiparados, depreciação do valor de moeda metálica ou de títulos equiparados, passagem de moeda falsa de concerto com o falsificador ou de títulos equiparados, passagem de moeda falsa ou de títulos equiparados, ou aquisição de moeda falsa para ser posta em circulação ou de títulos equiparados;

c) Falsidade informática, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo, interceção ilegítima ou reprodução ilegítima de programa protegido;

d) […];

e) […];

f) […];

g) […];

h) […];

i) […];

j) […];

k) […];

l) […];

m) […].

2 – […].

3 – […].

4 – […].

5 – […].

6 – […].

7 – […].

8 – […].

9 – […].

10 – […].

11 – […].

12 – […].»

Artigo 13.º

Alteração ao Estatuto das Instituições Particulares de Solidariedade Social

O artigo 21.º-A do Estatuto das Instituições Particulares de Solidariedade Social, aprovado em anexo ao Decreto-Lei n.º 119/83, de 25 de fevereiro, passa a ter a seguinte redação:

«Artigo 21.º-A

[…]

1 – Os titulares dos órgãos não podem ser reeleitos ou novamente designados se tiverem sido condenados em processo judicial por sentença transitada em julgado, em Portugal ou no estrangeiro, por crime doloso contra o património, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, usura, insolvência dolosa ou negligente, apropriação ilegítima de bens do setor público ou não lucrativo, falsificação, corrupção, branqueamento de capitais e contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação ou aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático salvo se, entretanto, tiver ocorrido a extinção da pena.

2 – […].»

Artigo 14.º

Alteração ao Código de Processo Penal

Os artigos 187.º, 202.º e 215.º do Código de Processo Penal, aprovado pelo Decreto–Lei n.º 78/87, de 17 de fevereiro, passam a ter a seguinte redação:

«Artigo 187.º

[…]

1 – […].

2 – […]:

a) […];

b) […];

c) […];

d) […];

e) Falsificação de moeda ou títulos equiparados a moeda prevista nos artigos 262.º, 264.º, na parte em que remete para o artigo 262.º, e 267.º, na parte em que remete para os artigos 262.º e 264.º do Código Penal, bem como contrafação de cartões ou outros dispositivos de pagamento e uso de cartões ou outros dispositivos de pagamento contrafeitos, previstos no artigo 3.º-A e no n.º 3 do artigo 3.º-B da Lei n.º 109/2009, de 15 de setembro;

f) […].

3 – […].

4 – […].

5 – […].

6 – […].

7 – […].

8 – […].

Artigo 202.º

[…]

1 – […]:

a) […];

b) […];

c) […];

d) Houver fortes indícios de prática de crime doloso de ofensa à integridade física qualificada, furto qualificado, dano qualificado, burla informática e nas comunicações, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, recetação, falsificação ou contrafação de documento, atentado à segurança de transporte rodoviário, puníveis com pena de prisão de máximo superior a 3 anos;

e) […];

f) […].

2 – […].

Artigo 215.º

[…]

1 – […].

2 – […]:

a) […];

b) […];

c) De falsificação de moeda, títulos de crédito, valores selados, selos e equipamentos ou da respetiva passagem, e de contrafação de cartões ou outros dispositivos de pagamento e uso de cartões ou outros dispositivos de pagamento contrafeitos, previstos nos artigos 3.º-A e 3.º-B da Lei n.º 109/2009, de 15 de setembro;

d) […];

e) […];

f) […];

g) […].

3 – […].

4 – […].

5 – […].

6 – […].

7 – […].

8 – […].»

Artigo 15.º

Alteração ao Decreto-Lei n.º 12/2021, de 9 de fevereiro

O artigo 19.º do Decreto-Lei n.º 12/2021, de 9 de fevereiro, passa a ter a seguinte redação:

«Artigo 19.º

[…]

1 – […].

2 – […]:

a) Condenada, no País ou no estrangeiro, por crime de furto, roubo, burla, burla informática e nas comunicações, extorsão, abuso de confiança, infidelidade, falsificação, falsas declarações, insolvência dolosa, insolvência negligente, favorecimento de credores, emissão de cheques sem provisão, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, apropriação ilegítima de bens do sector público ou cooperativo, administração danosa em unidade económica do sector público ou cooperativo, usura, suborno, corrupção, receção não autorizada de depósitos ou outros fundos reembolsáveis, prática ilícita de atos ou operações inerentes à atividade seguradora ou dos fundos de pensões, branqueamento de capitais, abuso de informação, manipulação do mercado de valores mobiliários, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, ou crime previsto no Código das Sociedades Comerciais;

b) […];

c) […];

d) […];

e) […];

f) […].

3 – […].»

Artigo 16.º

Alteração ao Regulamento da Caixa de Previdência dos Advogados e Solicitadores

O artigo 6.º do Regulamento da Caixa de Previdência dos Advogados e Solicitadores, aprovado em anexo ao Decreto-Lei n.º 119/2015, de 29 de junho, passa a ter a seguinte redação:

«Artigo 6.º

[…]

1 – […].

2 – […]:

a) […];

b) […];

c) Não tenham sido condenados, por sentença transitada em julgado, por furto, abuso de confiança, roubo, burla, extorsão, infidelidade, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, emissão de cheques sem provisão, usura, insolvência dolosa, insolvência negligente, frustração de créditos, favorecimento de credores, apropriação ilegítima de bens do setor público ou cooperativo, administração danosa em unidade económica do setor público ou cooperativo, falsificação, falsidade, suborno, corrupção, branqueamento de capitais, receção não autorizada de depósitos ou outros fundos não reembolsáveis, prática ilícita de atos ou operações de seguros, de resseguros ou de gestão de fundos de pensões, abuso de informação, manipulação do mercado de valores mobiliários, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, aquisição de cartões ou outros

dispositivos de pagamento obtidos mediante crime informático, ou pelos crimes previstos no Código das Sociedades Comerciais;

d) […];

e) […];

f) […];

g) […];

h) […];

i) […].»

Artigo 17.º

Alteração ao Código das Associações Mutualistas

O artigo 100.º do Código das Associações Mutualistas, aprovado em anexo ao Decreto-Lei n.º 59/2018, de 2 de agosto, passa a ter a seguinte redação:

«Artigo 100.º

[…]

1 – […]:

a) […];

b) […];

c) […];

d) […];

e) Sejam pessoas idóneas, nomeadamente por não terem sido condenados, em Portugal ou no estrangeiro, por crime doloso contra o património, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, usura, insolvência dolosa ou negligente, apropriação ilegítima de bens do setor público ou não lucrativo, falsificação, gestão danosa, corrupção, branqueamento de capitais, prática ilícita de gestão de fundos de pensões, abuso de informação e manipulação do mercado de valores mobiliários, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação, ou aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático, salvo se, entretanto, tiver ocorrido a extinção da pena;

f) […];

g) […].

2 – […].»

Artigo 18.º

Alteração ao Decreto-Lei n.º 137/2019, de 13 de setembro

O artigo 33.º do Decreto-Lei n.º 137/2019, de 13 de setembro, passa a ter a seguinte redação:

«Artigo 33.º

[…]

1 – […].

2 – […]:

a) […];

b) […];

c) […];

i) […];

ii) […];

iii) […];

iv) Relativos à interferência, utilização ou manipulação ilegítima de meios de pagamento eletrónicos e virtuais;

v) […];

vi) […].

3 – […].

4 – […].»

Artigo 19.º

Norma revogatória

São revogados o n.º 3 do artigo 265.º e o n.º 3 do artigo 278.º-A do Código Penal, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro.

Artigo 20.º

Republicação

É republicada em anexo à presente lei, da qual faz parte integrante, a Lei n.º 109/2009, de 15 de setembro.

Artigo 21.º

Entrada em vigor

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

Aprovado em 20 de julho de 2021

O PRESIDENTE DA ASSEMBLEIA DA REPÚBLICA,

(Eduardo Ferro Rodrigues)

ANEXO

(a que se refere o artigo 20.º)

Republicação da Lei n.º 109/2009, de 15 de setembro

CAPÍTULO I
Objeto e definições

Artigo 1.º
Objeto

A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa.

Artigo 2.º
Definições

Para efeitos da presente lei, considera-se.

a) «Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;

b) «Dados informáticos», qualquer representação de 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 fixadas ou codificadas, que representam a configuração tridimensional das camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respetivo fabrico;

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

CAPÍTULO II
Disposições penais materiais

Artigo 3.º
Falsidade informática

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

2 – Quando as ações descritas no número anterior incidirem sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso 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 dispositivo no qual se encontrem registados, incorporados ou ao qual respeitem os dados objeto dos atos referidos no número anterior, é punido com as penas previstas num e noutro número, respetivamente.

4 – Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos destinados à prática das ações previstas 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 3.º-A

Contrafação de cartões ou outros dispositivos de pagamento

Quem, com intenção de provocar engano nas relações jurídicas, contrafizer cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, nomeadamente introduzindo, modificando, apagando, suprimindo ou interferindo, por qualquer outro modo, num tratamento informático de dados registados, incorporados, ou respeitantes a estes cartões ou dispositivos, é punido com pena de prisão de 3 a 12 anos.

Artigo 3.º-B

Uso de cartões ou outros dispositivos de pagamento contrafeitos

1 – Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar cartão de pagamento contrafeito, ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos.

2 – As ações descritas no número anterior são punidas com pena de prisão de 2 a 8 anos se o prejuízo ou o benefício for de valor consideravelmente elevado.

3 – As ações descritas no n.º 1 são punidas com pena de prisão de 3 a 12 anos se o agente as praticar de concerto com o agente dos factos descritos no artigo 3.º-A.

Artigo 3.º-C

Aquisição de cartões ou outros dispositivos de pagamento contrafeitos

Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar cartão de pagamento contrafeito ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento contrafeito, é punido com pena de prisão de 1 a 5 anos.

Artigo 3.º-D

Atos preparatórios da contrafação

Quem produzir, adquirir, importar, distribuir, vender ou detiver qualquer cartão, dispositivo, programa ou outros dados informáticos, ou quaisquer outros instrumentos, informáticos ou não, destinados à prática das ações descritas no artigo 3.º–A, é punido com pena de prisão de 1 a 5 anos.

Artigo 3.º-E

Aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático

Quem, atuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, adquirir, detiver, exportar, importar, transportar, distribuir, vender ou por qualquer outra forma transmitir ou disponibilizar:

a) Dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que hajam sido obtidos mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;

b) Cartão de pagamento ou qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento, que haja sido obtido mediante facto ilícito típico previsto nos artigos 4.º, 5.º, 6.º e 7.º;

é punido com pena de prisão de 1 a 5 anos.

Artigo 3.º-F

Agravação

Se os factos referidos nos artigos 3.º-A a 3.º-E forem praticados por funcionário no exercício das suas funções, o limite mínimo da pena de prisão aplicável é:

a) De 2 anos, tratando-se dos factos previstos no n.º 1 do artigo 3.º-B, no n.º 1 do artigo 3.º-C, no artigo 3.º-D e no artigo 3.º-E;

b) Agravado em um terço, nos restantes casos.

Artigo 3.º-G

Moeda virtual

Para efeitos da presente lei, considera–se também sistema ou meio de pagamento aquele que tenha por objeto moeda virtual.

Artigo 4.º

Dano relativo a programas ou outros dados informáticos

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

2 – A tentativa é punível.

3 – Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas nesse número.

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

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

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

Artigo 5.º

Sabotagem informática

1 – Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

2 – Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.

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

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

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

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

b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Artigo 6.º

Acesso ilegítimo

1 – Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

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

3 – A pena é de prisão até 2 anos ou multa até 240 dias se as ações descritas no número anterior se destinarem ao acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

4 – A pena é de prisão até 3 anos ou multa se:

a) O acesso for conseguido através de violação de regras de segurança; ou

b) Através do acesso, o agente obtiver dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

5 – 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.

6 – A tentativa é punível, salvo nos casos previstos nos n.os 2 e 3.

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

Artigo 7.º

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, intercetar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.

2 – 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 ações não autorizadas descritas no mesmo número.

Artigo 8.º

Reprodução ilegítima de programa protegido

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

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

3 – A tentativa é punível.

Artigo 9.º

Responsabilidade penal das pessoas coletivas e entidades equiparadas

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

Artigo 10.º

Perda de bens

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

2 – À avaliação, utilização, alienação e indemnização de bens apreendidos pelos órgãos de polícia criminal que sejam suscetíveis de vir a ser declarados perdidos a favor do Estado é aplicável o disposto no Decreto–Lei n.º 11/2007, de 19 de janeiro.

CAPÍTULO III

Disposições processuais

Artigo 11.º

Âmbito de aplicação das disposições processuais

1 – Com exceção do disposto nos artigos 18.º e 19.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.

2 – As disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de julho.

Artigo 12.º

Preservação expedita de dados

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

2 – A preservação pode também ser ordenada pelo órgão de polícia criminal mediante autorização da autoridade judiciária competente ou quando haja urgência ou perigo na demora, devendo aquele, neste último caso, dar notícia imediata do facto à autoridade judiciária e transmitir-lhe o relatório previsto no artigo 253.º do Código de Processo Penal.

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

a) A natureza dos dados;

b) A sua origem e destino, se forem conhecidos; e

c) O período de tempo pelo qual deverão ser preservados, até um máximo de três meses.

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

5 – A autoridade judiciária competente pode ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do n.º 3, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano.

Artigo 13.º
Revelação expedita de dados de tráfego

Tendo em vista assegurar a preservação dos dados de tráfego relativos a uma determinada comunicação, independentemente do número de fornecedores de serviço que nela participaram, o fornecedor de serviço a quem essa preservação tenha sido ordenada nos termos do artigo anterior indica à autoridade judiciária ou ao órgão de polícia criminal, logo que o souber, outros fornecedores de serviço através dos quais aquela comunicação tenha sido efetuada, tendo em vista permitir identificar todos os fornecedores de serviço e a via através da qual aquela comunicação foi efetuada.

Artigo 14.º
Injunção para apresentação ou concessão do acesso a dados

1 – Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.
2 – A ordem referida no número anterior identifica os dados em causa.
3 – Em cumprimento da ordem descrita nos n.os 1 e 2, quem tenha disponibilidade ou controlo desses dados comunica esses dados à autoridade judiciária competente ou permite, sob pena de punição por desobediência, o acesso ao sistema informático onde os mesmos estão armazenados.

4 – O disposto no presente artigo é aplicável a fornecedores de serviço, a quem pode ser ordenado que comuniquem ao processo dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar:

a) O tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço;

b) A identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou

c) Qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços.

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

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

7 – O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

Artigo 15.º

Pesquisa de dados informáticos

1 – Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.

2 – O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.

3 – O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:

a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;

b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

4 – Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:

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

b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.

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 16.º

Apreensão de dados informáticos

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

2 – O órgão de polícia criminal pode efetuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo anterior, bem como quando haja urgência ou perigo na demora.

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

4 – As apreensões efetuadas por órgão de polícia criminal são sempre sujeitas a validação pela autoridade judiciária, no prazo máximo de 72 horas.

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

6 – O regime de segredo profissional ou de funcionário e de segredo de Estado previsto no artigo 182.º do Código de Processo Penal é aplicável com as necessárias adaptações.

7 – A apreensão de dados informáticos, consoante seja mais adequado e proporcional, tendo em conta os interesses do caso concreto, pode, nomeadamente, revestir as formas seguintes:

a) Apreensão do suporte onde está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respetiva leitura;

b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo;

c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou

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

8 – No caso da apreensão efetuada nos termos da alínea b) do número anterior, a cópia é efetuada em duplicado, sendo uma das cópias selada e confiada ao secretário judicial dos serviços onde o processo correr os seus termos e, se tal for tecnicamente possível, os dados apreendidos são certificados por meio de assinatura digital.

Artigo 17.º

Apreensão de mensagens de correio eletrónico ou de natureza semelhante

1 – Quando, no decurso de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, forem encontradas, armazenadas nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou de natureza semelhante que sejam necessárias à produção de prova, tendo em vista a descoberta da verdade, a autoridade judiciária competente autoriza ou ordena por despacho a sua apreensão.

2 – O órgão de polícia criminal pode efetuar as apreensões referidas no número anterior, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática legitimamente ordenada e executada nos termos do artigo 15.º, bem como quando haja urgência ou perigo na demora, devendo tal apreensão ser validada pela autoridade judiciária no prazo máximo de 72 horas.

3 – À apreensão de mensagens de correio eletrónico e de natureza semelhante aplica–se o disposto nos n.os 5 a 8 do artigo anterior.

4 – O Ministério Público apresenta ao juiz, sob pena de nulidade, as mensagens de correio eletrónico ou de natureza semelhante cuja apreensão tiver ordenado ou validado e que considere serem de grande interesse para a descoberta da verdade ou para a prova, ponderando o juiz a sua junção aos autos tendo em conta os interesses do caso concreto.

5 – Os suportes técnicos que contenham as mensagens apreendidas cuja junção não tenha sido determinada pelo juiz são guardados em envelope lacrado, à ordem do tribunal, e destruídos após o trânsito em julgado da decisão que puser termo ao processo.

6 – No que não se encontrar previsto nos números anteriores, é aplicável, com as necessárias adaptações, o regime da apreensão de correspondência previsto no Código de Processo Penal.

Artigo 18.º

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 à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.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 de instrução 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 registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respetivo âmbito, de acordo com as necessidades concretas da investigação.

4 – Em tudo o que não for contrariado pelo presente artigo, à interceção e registo de transmissões de dados informáticos é aplicável o regime da interceção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.

Artigo 19.º

Ações encobertas

1 – É admissível o recurso às ações encobertas previstas na Lei n.º 101/2001, de 25 de agosto, nos termos aí previstos, 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 abstrato, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, o abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.

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

CAPÍTULO IV
Cooperação Internacional

Artigo 20.º
Âmbito da cooperação internacional

As autoridades nacionais competentes cooperam com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 59/2019, de 8 de agosto.

Artigo 21.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 Portugal 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 atue 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 253.º do Código de Processo Penal.

5 – O Ministério Público deve, de modo a responder prontamente a pedidos de assistência imediata, assegurar a disponibilidade de magistrados e meios técnicos para levar a cabo quaisquer intervenções processuais urgentes da sua competência.

Artigo 22.º

Preservação e revelação expeditas de dados informáticos em cooperação internacional

1 – Pode ser solicitada a Portugal a preservação expedita de dados informáticos armazenados em sistema informático aqui localizado, relativos a crimes previstos no artigo 11.º, com vista à apresentação de um pedido de auxílio judiciário para fins de pesquisa, apreensão e divulgação dos mesmos.

2 – A solicitação especifica:

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 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 especifica, sob pena de nulidade:

a) A natureza dos dados;

b) Se forem conhecidos, a origem e o destino dos mesmos; e

c) O período de tempo pelo qual os dados devem ser preservados, até um máximo de três meses.

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

7 – A autoridade judiciária competente, ou a Polícia Judiciária mediante autorização daquela autoridade, podem ordenar a renovação da medida por períodos sujeitos ao limite previsto na alínea *c*) do n.º 5, desde que se verifiquem os respetivos requisitos de admissibilidade, até ao limite máximo de um ano.

8 – Quando seja apresentado o pedido de auxílio referido no n.º 1, a autoridade judiciária competente para dele decidir determina a preservação dos dados até à 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 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 13.º a 17.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 13.º.

10 – A autoridade nacional à qual, nos termos do número anterior, sejam comunicados dados de tráfego identificadores de fornecedor de serviço e da via através dos quais a comunicação foi efetuada, comunica–os rapidamente à autoridade requerente, por forma a permitir a essa autoridade a apresentação de nova solicitação de preservação expedita de dados informáticos.

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

Artigo 23.º

Motivos de recusa

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

a) Os dados informáticos em causa respeitarem a infração de natureza política ou infração conexa segundo as conceções do direito português;

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

c) O Estado terceiro requisitante não oferecer garantias adequadas de proteção dos dados pessoais.

2 – A solicitação de preservação expedita de dados informáticos pode ainda ser recusada quando houver fundadas razões para crer que a execução de pedido de auxílio judiciário subsequente para fins de pesquisa, apreensão e divulgação de tais dados será recusado por ausência de verificação do requisito da dupla incriminação.

Artigo 24.º

Acesso a dados informáticos em cooperação internacional

1 – Em execução de pedido de autoridade estrangeira competente, a autoridade judiciária competente pode proceder à pesquisa, apreensão e divulgação de dados informáticos armazenados em sistema informático localizado em Portugal, relativos a crimes previstos no artigo 11.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 portuguesas.

Artigo 25.º

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

As autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, de acordo com as normas sobre transferência de dados pessoais previstas na Lei n.º 59/2019, de 8 de agosto, podem:

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

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

Artigo 26.º

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 Portugal, 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 18.º, em caso nacional semelhante.

2 – É competente para a receção dos pedidos de interceção a Polícia Judiciária, que os apresentará ao Ministério Público, para que os apresente ao juiz de instrução criminal da comarca de Lisboa 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 portuguesas.

CAPÍTULO V

Disposições finais e transitórias

Artigo 27.º

Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses

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

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

b) Cometidos em benefício de pessoas coletivas com sede em território português;

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

d) Que visem sistemas informáticos localizados em território português, independentemente do local onde esses factos forem fisicamente praticados.

2 – Se, em função da aplicabilidade da lei penal portuguesa, forem simultaneamente competentes para conhecer de um dos crimes previstos na presente lei os tribunais portugueses e os tribunais de outro Estado membro da União Europeia, podendo 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 no seio da União Europeia para facilitar a cooperação entre as autoridades judiciárias dos Estados membros e a coordenação das respetivas ações, por forma a decidir qual dos dois Estados instaura ou prossegue o procedimento contra os agentes da infração, 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 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 atuou e o local onde está fisicamente instalado o sistema informático visado com a sua atuação, a competência cabe ao tribunal onde primeiro tiver havido notícia dos factos.

Artigo 28.º

Regime geral aplicável

Em tudo o que não contrarie o disposto na presente lei, aplicam–se aos crimes, às medidas processuais e à cooperação internacional em matéria penal nela previstos, respetivamente, as disposições do Código Penal, do Código de Processo Penal e da Lei n.º 144/99, de 31 de agosto.

Artigo 29.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 30.º

Proteção de dados pessoais

O tratamento de dados pessoais ao abrigo da presente lei efetua–se nos termos da Lei n.º 59/2019, de 8 de agosto, sendo aplicável, em caso de violação, o disposto no respetivo capítulo VII.

Artigo 31.º

Norma revogatória

É revogada a Lei n.º 109/91, de 17 de agosto.

Artigo 32.º

Entrada em vigor

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