ASSEMBLEIA DA REPÚBLICA

Lei n.º 18/2024

de 5 de fevereiro

Sumário: Regula o acesso a metadados referentes a comunicações eletrónicas para fins de investigação criminal, procedendo à alteração da Lei n.º 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva 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, conformando-a com os Acórdãos do Tribunal Constitucional n.os 268/2022 e 800/2023, e da Lei da Organização do Sistema Judiciário.

Regula o acesso a metadados referentes a comunicações eletrónicas para fins de investigação criminal, procedendo à alteração da Lei n.º 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva 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, conformando-a com os Acórdãos do Tribunal Constitucional n.os 268/2022 e 800/2023, e da Lei da Organização do Sistema Judiciário.

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 procede:

a) À segunda alteração à Lei n.º 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva 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, conformando-a com os Acórdãos do Tribunal Constitucional n.os 268/2022 e 800/2023;

b) À décima segunda alteração à Lei da Organização do Sistema Judiciário, aprovada pela Lei n.º 62/2013, de 26 de agosto, alterada pelas Leis n.os 40-A/2016, de 22 de dezembro, e 94/2017, de 23 de agosto, pela Lei Orgânica n.º 4/2017, de 25 de agosto, pela Lei n.º 23/2018, de 5 de junho, pelo Decreto-Lei n.º 110/2018, de 10 de dezembro, e pelas Leis n.os 19/2019, de 19 de fevereiro, 27/2019, de 28 de março, 55/2019, de 5 de agosto, 107/2019, de 9 de setembro, 77/2021, de 23 de abril, e 35/2023, de 21 de julho.

Artigo 2.º

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

Os artigos 2.º, 4.º, 6.º, 7.º, 9.º, 15.º, 16.º e 17.º da Lei n.º 32/2008, de 17 de julho, alterada pela Lei n.º 79/2021, de 24 de novembro, passam a ter a seguinte redação:

«Artigo 2.º

[...]

1 — [...]

2 — Para efeitos da presente lei, são aplicáveis, sem prejuízo do disposto no número anterior, as definições constantes do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conse-

lho, de 27 de abril de 2016, e das Leis n.os 41/2004, de 18 de agosto, que transpõe para a ordem jurídica nacional a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, e 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Artigo 4.º

[...]

1 — Os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar, nos termos previstos na presente lei, em Portugal ou no território de outro Estado-Membro da União Europeia, as seguintes categorias de dados:

a) [...]
b) [...]
c) [...]
d) [...]
e) [...]
f) [...]

2 — [...]
3 — [...]
4 — [...]
5 — [...]
6 — [...]
7 — [...]

Artigo 6.º

Período e regras de conservação

1 — Para efeitos da finalidade prevista no n.º 1 do artigo 3.º, as entidades referidas no n.º 1 do artigo 4.º devem conservar, pelo período de um ano a contar da data da conclusão da comunicação, os seguintes dados:

a) Os dados relativos à identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede pública de comunicações;
b) Os demais dados de base;
c) Os endereços de protocolo IP atribuídos à fonte de uma ligação.

2 — Os dados de tráfego e de localização apenas podem ser objeto de conservação mediante autorização judicial fundada na sua necessidade para a finalidade prevista no n.º 1 do artigo 3.º, sem prejuízo daqueles conservados pelas entidades referidas no n.º 1 do artigo 4.º nos termos definidos contratualmente com o cliente para efeitos emergentes das respetivas relações jurídicas comerciais ou por força de disposição legal especial.
3 — O pedido de autorização judicial para conservação de dados de tráfego e de localização tem caráter urgente e deve ser decidido no prazo máximo de 72 horas.
4 — De forma a salvaguardar a utilidade do pedido de autorização judicial para conservação de dados de tráfego e de localização, o Ministério Público comunica de imediato às entidades referidas no n.º 1 do artigo 4.º a submissão do pedido, não podendo os dados ser objeto de eliminação até à decisão final sobre a respetiva conservação.

5 — A fixação e a prorrogação do prazo de conservação de dados de tráfego e de localização referida nos números anteriores devem limitar-se ao estritamente necessário para a prossecução da finalidade prevista no n.º 1 do artigo 3.º, devendo cessar logo que se confirme a desnecessidade da sua conservação.

6 — As entidades referidas no n.º 1 do artigo 4.º não podem aceder aos dados aí elencados salvo nos casos previstos na lei ou definidos contratualmente com o cliente para efeitos emergentes das respetivas relações jurídicas comerciais.

7 — A autorização judicial a que se referem os n.os 2 e 3 compete a uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções.

Artigo 7.º

[...]

1 — [...]

a) [...]

b) Garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos a um nível de proteção e segurança nunca inferior aos dados na rede;

c) [...]

d) [...]

e) [...]

f) [...]

2 — [...]

3 — [...]

4 — As medidas técnicas e organizativas adequadas para assegurar um nível de segurança são aplicadas tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares.

5 — Na avaliação do nível de segurança adequado devem ser considerados, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

6 — O disposto nos números anteriores não prejudica a observação dos princípios nem o cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados, previstos no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e nas Leis n.os 41/2004, de 18 de agosto, 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, e 58/2019, de 8 de agosto, e respetiva regulamentação.

7 — *(Anterior n.º 5.)*

Artigo 9.º

[...]

1 — [...]

2 — A autorização prevista no número anterior só pode ser requerida pelo Ministério Público.

3 — [...]

4 — [...]
5 — [...]
6 — [...]
7 — Sem prejuízo do disposto no número seguinte, o despacho que autoriza a transmissão dos dados referentes às categorias previstas no n.º 1 do artigo 4.º é notificado ao titular dos dados no prazo máximo de 10 dias a contar da sua prolação.
8 — Se, em inquérito, o Ministério Público considerar que a notificação referida no número anterior comporta risco de pôr em causa a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas devidamente identificadas, pode solicitar ao juiz de instrução criminal que protele a notificação, a qual é realizada logo que a razão do protelamento deixar de existir ou, o mais tardar, no prazo máximo de 10 dias a contar da data em que for proferido despacho de encerramento desta fase processual.
9 — A transmissão dos dados referentes às categorias previstas no n.º 1 do artigo 4.º a autoridades de outros Estados só pode ocorrer no âmbito da cooperação judiciária internacional em matéria penal, de acordo com as regras fixadas na respetiva lei e desde que esses Estados garantam o mesmo nível de proteção de dados pessoais vigente no território da União Europeia.

Artigo 15.º

Aplicabilidade dos regimes sancionatórios previstos nas Leis n.os 58/2019, de 8 de agosto, e 41/2004, de 18 de agosto

O disposto nos artigos 12.º a 14.º não prejudica a aplicação do regime sancionatório estabelecido na Lei n.º 58/2019, de 8 de agosto, aplicável por incumprimento das obrigações previstas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, bem como do disposto no capítulo III da Lei n.º 41/2004, de 18 de agosto.

Artigo 16.º

Estatísticas

1 — A CNPD transmite anualmente à Comissão Europeia as estatísticas sobre a conservação dos dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações.
2 — [...]

a) O número de casos em que foram transmitidos dados às autoridades competentes;
b) [...]
c) O número de casos em que as solicitações das autoridades competentes não puderam ser satisfeitas.

3 — [...]

Artigo 17.º

[...]

1 — No final de cada biénio, a CNPD, em colaboração com a Autoridade Nacional de Comunicações, procede à avaliação de todos os procedimentos previstos na presente lei e elabora um relatório detalhado sobre a sua aplicação, que deve destacar os aspetos que carecem de aperfeiçoamento e incluir recomendações para superar constrangimentos detetados.
2 — O relatório previsto no número anterior deve ser remetido à Assembleia da República e ao Governo até 30 de junho do ano seguinte ao termo do período a que respeita.»

Artigo 3.º

Alteração à Lei da Organização do Sistema Judiciário

Os artigos 47.º e 54.º da Lei da Organização do Sistema Judiciário passam a ter a seguinte redação:

«Artigo 47.º

[...]

1 — [...]
2 — [...]
3 — [...]
4 — No Supremo Tribunal de Justiça há também uma formação das secções criminais, constituída pelos presidentes das secções criminais e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções, que procede ao controlo e autorização prévia da obtenção de dados de telecomunicações e Internet no quadro da atividade de produção de informações em matéria de espionagem e terrorismo do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa, bem como à autorização judicial para conservação de dados de tráfego e de localização no âmbito da Lei n.º 32/2008, de 17 de julho.

Artigo 54.º

[...]

1 — [...]
2 — [...]
3 — [...]
4 — A formação das secções criminais do Supremo Tribunal de Justiça, constituída nos termos do n.º 4 do artigo 47.º, procede ao controlo e autorização prévia dos pedidos fundamentados de acesso a dados de telecomunicações e Internet nos termos do procedimento previsto na lei especial que aprova o regime especial de acesso a dados de base e a dados de tráfego de comunicações eletrónicas pelo Sistema de Informações da República Portuguesa, bem como à autorização judicial para conservação de dados de tráfego e de localização no âmbito da Lei n.º 32/2008, de 17 de julho.»

Artigo 4.º

Republicação

É republicada, em anexo à presente lei, da qual faz parte integrante, a Lei n.º 32/2008, de 17 de julho, com a redação atual.

Artigo 5.º

Entrada em vigor

A presente lei entra em vigor no dia seguinte ao da sua publicação.

Aprovada em 5 de janeiro de 2024.

O Presidente da Assembleia da República, *Augusto Santos Silva.*

Promulgada em 29 de janeiro de 2024.

Publique-se.

O Presidente da República, Marcelo Rebelo de Sousa.

Referendada em 30 de janeiro de 2024.

O Primeiro-Ministro, *António Luís Santos da Costa.*

ANEXO

(a que se refere o artigo 4.º)

Republicação da Lei n.º 32/2008, de 17 de julho

Transpõe para a ordem jurídica interna a Diretiva 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

Artigo 1.º

Objeto

1 — A presente lei regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Diretiva 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, e que altera a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de junho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

2 — A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de agosto, e na legislação processual penal relativamente à interceção e gravação de comunicações.

Artigo 2.º

Definições

1 — Para efeitos da presente lei, entende-se por:

a) «Dados», os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador;

b) «Serviço telefónico», qualquer dos seguintes serviços:

i) Os serviços de chamada, incluindo as chamadas vocais, o correio vocal, a teleconferência ou a transmissão de dados;

ii) Os serviços suplementares, incluindo o reencaminhamento e a transferência de chamadas; e

iii) Os serviços de mensagens e multimédia, incluindo os serviços de mensagens curtas (SMS), os serviços de mensagens melhoradas (EMS) e os serviços multimédia (MMS);

c) «Código de identificação do utilizador» (*«user ID»*), um código único atribuído às pessoas, quando estas se tornam assinantes ou se inscrevem num serviço de acesso à Internet, ou num serviço de comunicação pela Internet;

d) «Identificador de célula» (*«cell ID»*), a identificação da célula de origem e de destino de uma chamada telefónica numa rede móvel;

e) «Chamada telefónica falhada», uma comunicação em que a ligação telefónica foi estabelecida, mas que não obteve resposta, ou em que houve uma intervenção do gestor da rede;

f) «Autoridades competentes», as autoridades judiciárias e as autoridades de polícia criminal das seguintes entidades:

i) A Polícia Judiciária;

ii) A Guarda Nacional Republicana;

iii) A Polícia de Segurança Pública;

iv) A Polícia Judiciária Militar;
v) O Serviço de Estrangeiros e Fronteiras;
vi) A Polícia Marítima;

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 — Para efeitos da presente lei, são aplicáveis, sem prejuízo do disposto no número anterior, as definições constantes do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e das Leis n.os 41/2004, de 18 de agosto, que transpõe para a ordem jurídica nacional a Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, e 58/2019, de 8 de agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Artigo 3.º

Finalidade do tratamento

1 — A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes.
2 — A transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º
3 — Os ficheiros destinados à conservação de dados no âmbito da presente lei têm que, obrigatoriamente, estar separados de quaisquer outros ficheiros para outros fins.
4 — O titular dos dados não pode opor-se à respetiva conservação e transmissão.

Artigo 4.º

Categorias de dados a conservar

1 — Os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar, nos termos previstos na presente lei, em Portugal ou no território de outro Estado-Membro da União Europeia, as seguintes categorias de dados:

a) Dados necessários para encontrar e identificar a fonte de uma comunicação;
b) Dados necessários para encontrar e identificar o destino de uma comunicação;
c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;
d) Dados necessários para identificar o tipo de comunicação;
e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
f) Dados necessários para identificar a localização do equipamento de comunicação móvel.

2 — Para os efeitos do disposto na alínea *a*) do número anterior, os dados necessários para encontrar e identificar a fonte de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) O número de telefone de origem;
ii) O nome e endereço do assinante ou do utilizador registado;

b) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:

i) Os códigos de identificação atribuídos ao utilizador;
ii) O código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública;
iii) O nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação.

3 — Para os efeitos do disposto na alínea *b*) do n.º 1, os dados necessários para encontrar e identificar o destino de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) Os números marcados e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada;
ii) O nome e o endereço do assinante, ou do utilizador registado;

b) No que diz respeito ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:

i) O código de identificação do utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da Internet;
ii) Os nomes e os endereços dos subscritores, ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação.

4 — Para os efeitos do disposto na alínea *c*) do n.º 1, os dados necessários para identificar a data, a hora e a duração de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;
b) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:

i) A data e a hora do início (*log in*) e do fim (*log off*) da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado;
ii) A data e a hora do início e do fim da ligação ao serviço de correio eletrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário.

5 — Para os efeitos do disposto na alínea *d*) do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, o serviço telefónico utilizado;
b) No que diz respeito ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet, o serviço de Internet utilizado.

6 — Para os efeitos do disposto na alínea *e*) do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, são os seguintes:

a) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino;

b) No que diz respeito às comunicações telefónicas na rede móvel:

i) Os números de telefone de origem e de destino;
ii) A Identidade Internacional de Assinante Móvel (*International Mobile Subscriber Identity*, ou IMSI) de quem telefona;
iii) A Identidade Internacional do Equipamento Móvel (*International Mobile Equipment Identity*, ou IMEI) de quem telefona;
iv) A IMSI do destinatário do telefonema;
v) A IMEI do destinatário do telefonema;
vi) No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da ativação inicial do serviço e o identificador da célula a partir da qual o serviço foi ativado;

c) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:

i) O número de telefone que solicita o acesso por linha telefónica;
ii) A linha de assinante digital (*digital subscriber line*, ou DSL), ou qualquer outro identificador terminal do autor da comunicação.

7 — Para os efeitos do disposto na alínea *f*) do n.º 1, os dados necessários para identificar a localização do equipamento de comunicação móvel são os seguintes:

a) O identificador da célula no início da comunicação;
b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respetivos identificadores de célula durante o período em que se procede à conservação de dados.

Artigo 5.º

Âmbito da obrigação de conservação dos dados

1 — Os dados telefónicos e da Internet relativos a chamadas telefónicas falhadas devem ser conservados quando sejam gerados ou tratados e armazenados pelas entidades referidas no n.º 1 do artigo 4.º, no contexto da oferta de serviços de comunicação.
2 — Os dados relativos a chamadas não estabelecidas não são conservados.

Artigo 6.º

Período e regras de conservação

1 — Para efeitos da finalidade prevista no n.º 1 do artigo 3.º, as entidades referidas no n.º 1 do artigo 4.º devem conservar, pelo período de um ano a contar da data da conclusão da comunicação, os seguintes dados:

a) Os dados relativos à identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede pública de comunicações;
b) Os demais dados de base;
c) Os endereços de protocolo IP atribuídos à fonte de uma ligação.

2 — Os dados de tráfego e de localização apenas podem ser objeto de conservação mediante autorização judicial fundada na sua necessidade para a finalidade prevista no n.º 1 do artigo 3.º, sem prejuízo daqueles conservados pelas entidades referidas no n.º 1 do artigo 4.º nos termos definidos contratualmente com o cliente para efeitos emergentes das respetivas relações jurídicas comerciais ou por força de disposição legal especial.
3 — O pedido de autorização judicial para conservação de dados de tráfego e de localização tem caráter urgente e deve ser decidido no prazo máximo de 72 horas.

4 — De forma a salvaguardar a utilidade do pedido de autorização judicial para conservação de dados de tráfego e de localização, o Ministério Público comunica de imediato às entidades referidas no n.º 1 do artigo 4.º a submissão do pedido, não podendo os dados ser objeto de eliminação até à decisão final sobre a respetiva conservação.

5 — A fixação e a prorrogação do prazo de conservação referida nos números anteriores devem limitar-se ao estritamente necessário para a prossecução da finalidade prevista no n.º 1 do artigo 3.º, devendo cessar logo que se confirme a desnecessidade da sua conservação.

6 — As entidades referidas no n.º 1 do artigo 4.º não podem aceder aos dados aí elencados salvo nos casos previstos na lei ou definidos contratualmente com o cliente para efeitos emergentes das respetivas relações jurídicas comerciais.

7 — A autorização judicial a que se referem os n.os 2 e 3 compete a uma formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções.

Artigo 7.º

Proteção e segurança dos dados

1 — As entidades referidas no n.º 1 do artigo 4.º devem:

a) Conservar os dados referentes às categorias previstas no artigo 4.º por forma a que possam ser transmitidos imediatamente, mediante despacho fundamentado do juiz, às autoridades competentes;

b) Garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos a um nível de proteção e segurança nunca inferior aos dados na rede;

c) Tomar as medidas técnicas e organizativas adequadas à proteção dos dados previstos no artigo 4.º contra a destruição acidental ou ilícita, a perda ou a alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;

d) Tomar as medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados referentes às categorias previstas no artigo 4.º;

e) Destruir os dados no final do período de conservação, exceto os dados que tenham sido preservados por ordem do juiz;

f) Destruir os dados que tenham sido preservados, quando tal lhe seja determinado por ordem do juiz.

2 — Os dados referentes às categorias previstas no artigo 4.º, com exceção dos dados relativos ao nome e endereço dos assinantes, devem permanecer bloqueados desde o início da sua conservação, só sendo alvo de desbloqueio para efeitos de transmissão, nos termos da presente lei, às autoridades competentes.

3 — A transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados.

4 — As medidas técnicas e organizativas adequadas para assegurar um nível de segurança são aplicadas tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares.

5 — Na avaliação do nível de segurança adequado devem ser considerados, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

6 — O disposto nos números anteriores não prejudica a observação dos princípios nem o cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança

dos dados, previstos no Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e nas Leis n.os 41/2004, de 18 de agosto, 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, e 58/2019, de 8 de agosto, e respetiva regulamentação.

7 — A autoridade pública competente para o controlo da aplicação do disposto no presente artigo é a Comissão Nacional de Proteção de Dados (CNPD).

Artigo 8.º

Registo de pessoas especialmente autorizadas

1 — A CNPD deve manter um registo eletrónico permanentemente atualizado das pessoas especialmente autorizadas a aceder aos dados, nos termos da alínea *d*) do n.º 1 do artigo anterior.

2 — Para os efeitos previstos no número anterior, os fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações devem remeter à CNPD, por via exclusivamente eletrónica, os dados necessários à identificação das pessoas especialmente autorizadas a aceder aos dados.

Artigo 9.º

Transmissão dos dados

1 — A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves.

2 — A autorização prevista no número anterior só pode ser requerida pelo Ministério Público.

3 — Só pode ser autorizada a transmissão de dados relativos:

a) Ao suspeito ou arguido;

b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou

c) A vítima de crime, mediante o respetivo consentimento, efetivo ou presumido.

4 — A decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à proteção do segredo profissional, nos termos legalmente previstos.

5 — O disposto nos números anteriores não prejudica a obtenção de dados sobre a localização celular necessários para afastar perigo para a vida ou de ofensa à integridade física grave, nos termos do artigo 252.º-A do Código de Processo Penal.

6 — As entidades referidas no n.º 1 do artigo 4.º devem elaborar registos da extração dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD.

7 — Sem prejuízo do disposto no número seguinte, o despacho que autoriza a transmissão dos dados referentes às categorias previstas no n.º 1 do artigo 4.º é notificado ao titular dos dados no prazo máximo de 10 dias a contar da sua prolação.

8 — Se, em inquérito, o Ministério Público considerar que a notificação referida no número anterior comporta risco de pôr em causa a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas devidamente identificadas, pode solicitar ao juiz de instrução criminal que protele a notificação, a qual é realizada logo que a razão do protelamento deixar de existir ou, o mais tardar, no prazo máximo de 10 dias a contar da data em que for proferido despacho de encerramento desta fase processual.

9 — A transmissão dos dados referentes às categorias previstas no n.º 1 do artigo 4.º a autoridades de outros Estados só pode ocorrer no âmbito da cooperação judiciária internacional em matéria penal, de acordo com as regras fixadas na respetiva lei e desde que esses Estados garantam o mesmo nível de proteção de dados pessoais vigente no território da União Europeia.

Artigo 10.º

Condições técnicas da transmissão dos dados

A transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança previstas no n.º 3 do artigo 7.º

Artigo 11.º

Destruição dos dados

1 — O juiz determina, oficiosamente ou a requerimento de qualquer interessado, a destruição dos dados na posse das autoridades competentes, bem como dos dados preservados pelas entidades referidas no n.º 1 do artigo 4.º, logo que os mesmos deixem de ser estritamente necessários para os fins a que se destinam.

2 — Considera-se que os dados deixam de ser estritamente necessários para o fim a que se destinam logo que ocorra uma das seguintes circunstâncias:

a) Arquivamento definitivo do processo penal;
b) Absolvição, transitada em julgado;
c) Condenação, transitada em julgado;
d) Prescrição do procedimento penal;
e) Amnistia.

Artigo 12.º

Contraordenações

1 — Sem prejuízo da responsabilidade criminal a que haja lugar nos termos da lei, constitui contraordenação:

a) A não conservação das categorias dos dados previstas no artigo 4.º;
b) O incumprimento do prazo de conservação previsto no artigo 6.º;
c) A não transmissão dos dados às autoridades competentes, quando autorizada nos termos do disposto no artigo 9.º;
d) O não envio dos dados necessários à identificação das pessoas especialmente autorizadas, nos termos do n.º 2 do artigo 8.º

2 — As contraordenações previstas no número anterior são puníveis com coimas de € 1500 a € 50 000 ou de € 5000 a € 10 000 000 consoante o agente seja uma pessoa singular ou coletiva.

3 — A tentativa e a negligência são puníveis.

Artigo 13.º

Crimes

1 — Constituem crime, punido com pena de prisão até dois anos ou multa até 240 dias:

a) O incumprimento de qualquer das regras relativas à proteção e à segurança dos dados previstas no artigo 7.º;

b) O não bloqueio dos dados, nos termos previstos no n.º 2 do artigo 7.º;

c) O acesso aos dados por pessoa não especialmente autorizada nos termos do n.º 1 do artigo 8.º

2 — A pena é agravada para o dobro dos seus limites quando o crime:

a) For cometido através de violação de regras técnicas de segurança;

b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais; ou

c) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.

3 — A tentativa e a negligência são puníveis.

Artigo 14.º

Processos de contraordenação e aplicação das coimas

1 — Compete à CNPD a instrução dos processos de contraordenação e a respetiva aplicação de coimas relativas às condutas previstas no artigo anterior.

2 — O montante das importâncias cobradas em resultado da aplicação das coimas é distribuído da seguinte forma:

a) 60 % para o Estado;

b) 40 % para a CNPD.

Artigo 15.º

Aplicabilidade dos regimes sancionatórios previstos nas Leis n.os 58/2019, de 8 de agosto, e 41/2004, de 18 de agosto

O disposto nos artigos 12.º a 14.º não prejudica a aplicação do regime sancionatório estabelecido na Lei n.º 58/2019, de 8 de agosto, aplicável por incumprimento das obrigações previstas no Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, bem como do disposto no capítulo III da Lei n.º 41/2004, de 18 de agosto.

Artigo 16.º

Estatísticas

1 — A CNPD transmite anualmente à Comissão Europeia as estatísticas sobre a conservação dos dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações.

2 — Tendo em vista o cumprimento do disposto no número anterior, as entidades referidas no n.º 1 do artigo 4.º devem, até 1 de março de cada ano, remeter à CNPD as seguintes informações, relativas ao ano civil anterior:

a) O número de casos em que foram transmitidos dados às autoridades competentes;

b) O período de tempo decorrido entre a data a partir da qual os dados foram conservados e a data em que as autoridades competentes solicitaram a sua transmissão; e

c) O número de casos em que as solicitações das autoridades competentes não puderam ser satisfeitas.

3 — As informações previstas no número anterior não podem conter quaisquer dados pessoais.

Artigo 17.º

Avaliação

1 — No final de cada biénio, a CNPD, em colaboração com a Autoridade Nacional de Comunicações, procede à avaliação de todos os procedimentos previstos na presente lei e elabora um relatório detalhado sobre a sua aplicação, que deve destacar os aspetos que carecem de aperfeiçoamento e incluir recomendações para superar constrangimentos detetados.

2 — O relatório previsto no número anterior deve ser remetido à Assembleia da República e ao Governo até 30 de junho do ano seguinte ao termo do período a que respeita.

Artigo 18.º

Produção de efeitos

A presente lei produz efeitos 90 dias após a publicação da portaria a que se refere o n.º 3 do artigo 7.º

117315008