

ASSEMBLEIA DA REPÚBLICA**Lei Orgânica n.º 4/2017**

de 25 de agosto

Aprova e regula o procedimento especial de acesso a dados de telecomunicações e *Internet* pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário).

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

Artigo 1.º**Objeto**

1 — A presente lei regula o procedimento especial de acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas que se mostrem estritamente necessários para a prossecução da atividade de produção de informações pelo Sistema de Informações da República Portuguesa (SIRP) relacionadas com a segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo, o qual é sujeito a acompanhamento do Ministério Público e controlo judicial.

2 — A presente lei procede ainda à segunda alteração à Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário), alterada pela Lei n.º 40-A/2016, de 22 de dezembro, que a republicou.

Artigo 2.º**Definições**

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

a) «Dados de telecomunicações», os registos ou informação constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas relativos à prestação de serviços telefónicos acessíveis ao público e à rede de suporte à transferência, entre pontos terminais da rede, de comunicações vocais, serviços de mensagens e multimédia e de outras formas de comunicação;

b) «Dados de *Internet*», os registos ou informação constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, relativos a sistemas de transmissão e a equipamentos de comutação ou encaminhamento que permitem o envio de sinais ou dados, quando não deem suporte a uma concreta comunicação.

2 — Para efeitos da presente lei, no âmbito dos «dados de telecomunicações e *Internet*», consideram-se:

a) «Dados de base», os dados para acesso à rede pelos utilizadores, compreendendo a identificação e morada destes, e o contrato de ligação à rede;

b) «Dados de localização de equipamento», os dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações que indiquem a posição geográfica do equipamento terminal de um serviço de telecomunicações acessível ao público, quando não deem suporte a uma concreta comunicação;

c) «Dados de tráfego», os dados tratados para efeitos do envio de uma comunicação através de uma rede de comu-

nicações eletrónicas ou no âmbito de um serviço de telecomunicações, ou para efeitos da faturação da mesma;

d) «Autoridades competentes», os dirigentes superiores e intermédios do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas de Defesa (SIED).

3 — A conservação e transmissão pelos prestadores de serviços de comunicações eletrónicas dos dados tipificados nos números anteriores obedecem exclusivamente às finalidades previstas no n.º 1 do artigo 1.º e nos artigos 3.º e 4.º

4 — A transmissão dos dados pelos prestadores de serviços de comunicações eletrónicas às autoridades competentes do SIS e do SIED, nos termos do artigo 11.º, só pode ser autorizada e ordenada por despacho judicial fundamentado de acordo com o procedimento estatuído na presente lei.

Artigo 3.º**Acesso a dados de base e de localização de equipamento**

Os oficiais de informações do SIS e do SIED podem ter acesso a dados de base e de localização de equipamento para efeitos de produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e à prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito.

Artigo 4.º**Acesso a dados de tráfego**

Os oficiais de informações do SIS e do SIED apenas podem ter acesso a dados de tráfego para efeitos de produção de informações necessárias à prevenção de atos de espionagem e do terrorismo.

Artigo 5.º**Comunicação ao Ministério Público e autorização judicial**

1 — O acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e *Internet* no âmbito da atividade de pesquisa depende de autorização judicial prévia e obrigatória, por uma formação das secções criminais do Supremo Tribunal de Justiça, constituída nos termos do artigo 8.º, que garanta a ponderação da relevância dos fundamentos do pedido e a salvaguarda dos direitos, liberdades e garantias constitucionalmente previstos.

2 — O processo de autorização de acesso aos dados é sempre comunicado ao Procurador-Geral da República.

Artigo 6.º**Admissibilidade do pedido**

1 — O pedido só pode ser autorizado quando houver razões para crer que a diligência é necessária, adequada e proporcional, nos termos seguintes:

a) Para a obtenção de informação sobre um alvo ou um intermediário determinado; ou

b) Para a obtenção de informação que seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência.

2 — É proibida a interconexão em tempo real com as bases de dados dos operadores de telecomunicações e *Internet* para o acesso direto em linha aos dados requeridos.

Artigo 7.º

Penas agravadas

1 — Quem, violando a proibição de ingerência do pessoal do SIRP na correspondência, nas telecomunicações e nos demais meios de comunicação, for condenado por qualquer dos crimes especialmente previstos nos artigos 193.º, 194.º e 384.º do Código Penal, aprovado pelo Decreto-Lei n.º 400/82, de 23 de setembro, nos artigos 6.º e 7.º da Lei n.º 109/2009, de 15 de setembro, e no artigo 44.º da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto, é punido com a pena aplicável ao crime respetivo agravada de um terço nos seus limites mínimo e máximo.

2 — Aos membros do gabinete do Secretário-Geral do Sistema de Informações da República Portuguesa, ao pessoal dirigente e ao demais pessoal do SIRP que seja condenado por prática com dolo dos tipos de crime referidos no número anterior, pode o tribunal, ponderadas as circunstâncias do caso concreto, aplicar na sentença a pena acessória de demissão ou suspensão até cinco anos do exercício de funções no SIRP, independentemente da medida disciplinar que ao caso for aplicável.

Artigo 8.º

Controlo judicial e autorização prévia

O controlo judicial e a autorização prévia do acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e *Internet* são efetuados por 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 9.º

Iniciativa

1 — O procedimento obrigatório e vinculado de autorização judicial prévia do acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e *Internet* inicia-se com o pedido elaborado pelos diretores do SIS ou do SIED, ou de quem os substitua em caso de ausência ou impedimento, enviado pelo Secretário-Geral do Sistema de Informações da República Portuguesa ao Presidente do Supremo Tribunal de Justiça, com conhecimento ao Procurador-Geral da República.

2 — O pedido previsto no número anterior é apresentado por escrito, devendo ser fundamentado, de modo detalhado e circunstanciado, e conter os seguintes elementos:

- a) Indicação da ação operacional concreta a realizar e das medidas pontuais de acesso requeridas;
- b) Factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham a adoção das medidas pontuais de acesso requeridas;
- c) Identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos referidos na alínea anterior e afetadas pelas medidas pontuais de acesso requeridas;
- d) Duração das medidas pontuais de acesso requeridas, que não pode exceder o prazo máximo de três meses, renovável por um único período sujeito ao mesmo limite, mediante autorização expressa, desde que se verifiquem os respetivos requisitos de admissibilidade.

3 — Para efeitos da presente lei, consideram-se «medidas pontuais de acesso» as providências de recolha de dados, por transferência autorizada e controlada caso a caso, com base numa suspeita concreta e individualizada, que não se prolongam no tempo, sendo a sua duração circunscrita, e que não se estendem à totalidade dos dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, não admitindo a aquisição de informação em larga escala, por transferência integral dos registos existentes, nem a ligação em tempo real às redes de comunicações eletrónicas.

Artigo 10.º

Apreciação judicial

1 — A apreciação judicial da necessidade, adequação e proporcionalidade do pedido, designadamente no que se refere à justa medida da espécie e da escala de informação obtida, compreende a definição das categorias de dados de telecomunicações e *Internet* a fornecer pelos operadores, segundo um juízo restritivo de proibição do excesso que interdite o acesso indiscriminado a todos os dados de telecomunicações e *Internet* de um determinado cidadão, bem como a definição das condições de proteção do segredo profissional.

2 — O acesso dos oficiais de informações do SIS e do SIED a dados de tráfego só pode ser autorizado no quadro da produção de informações de prevenção da espionagem e do terrorismo.

3 — A decisão judicial de concessão ou de denegação da autorização consta de despacho proferido no prazo máximo de 48 horas, fundamentado com base em informações claras e completas, nomeadamente quanto aos objetivos do processamento.

4 — Sem prejuízo do disposto no número anterior, em situações de urgência devidamente fundamentadas no pedido, o despacho previsto naquele número é proferido no prazo mais breve possível.

Artigo 11.º

Acesso aos dados autorizados

1 — A transmissão diferida dos dados de telecomunicações e *Internet* obtidos de acordo com o regime consagrado na presente lei processa-se mediante comunicação eletrónica, com conhecimento da formação das secções criminais do Supremo Tribunal de Justiça prevista no artigo 8.º e ao Procurador-Geral da República, nos termos das condições técnicas e de segurança fixadas em portaria do Primeiro-Ministro e dos membros do governo responsáveis pelas áreas das comunicações e da cibersegurança, 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, sem prejuízo da observação dos princípios e do cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados, previstos na Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto, e na Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, que a republicou, sob fiscalização e controlo da Comissão de Fiscalização de Dados do SIRP, nos termos da presente lei.

2 — O acesso do pessoal do SIRP a dados e informações conservados em arquivo nos centros de dados do SIS e

do SIED é determinado pelo princípio da necessidade de conhecer e só é concedido mediante autorização superior, tendo em vista o bom exercício das funções que lhe forem cometidas.

3 — O pessoal do SIRP ou quem aceder, tentar aceder, comunicar ou fizer uso dos dados ou informações, em violação do disposto no n.º 2 incorre em infração disciplinar grave, punível com sanção que pode ir até à pena de demissão ou outra medida que implique a imediata cessação de funções do infrator, nos termos do disposto no regime de necessidade de acesso aplicável ao pessoal do SIRP.

Artigo 12.º

Garantias

1 — O controlo judicial pela formação das secções criminais do Supremo Tribunal de Justiça visa garantir o respeito pelos direitos, liberdades e garantias e pelo princípio da legalidade da recolha, assegurando, nomeadamente, que os dados são:

a) Recolhidos para finalidades determinadas, explícitas e legítimas;

b) Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos.

2 — Após a comunicação prevista no n.º 1 do artigo anterior, a formação das secções criminais do Supremo Tribunal de Justiça valida o tratamento pelo SIS ou pelo SIED dos dados de telecomunicações e *Internet* considerados em conformidade com o disposto no número anterior.

3 — Compete à formação das secções criminais do Supremo Tribunal de Justiça determinar a todo o momento o cancelamento de procedimentos em curso de acesso a dados de telecomunicações e *Internet*, bem como ordenar a destruição imediata de todos os dados obtidos de forma ilegal ou abusiva, ou que violem o âmbito da autorização judicial prévia, bem como os dados que sejam manifestamente estranhos ao processo, nomeadamente quando não tenham relação com o objeto ou finalidades do pedido ou cujo tratamento possa afetar gravemente direitos, liberdades e garantias.

4 — O Procurador-Geral da República é notificado das decisões de cancelamento de acesso e de destruição dos dados, para efeitos do exercício das suas competências legais.

5 — A Comissão de Fiscalização de Dados do SIRP é notificada das decisões de cancelamento de acesso e de destruição dos dados, para efeitos do exercício das suas competências legais em matéria de proteção dos dados pessoais.

Artigo 13.º

Factos indiciários de espionagem e terrorismo

Os dados obtidos que indiciem a prática de crimes de espionagem e terrorismo são imediatamente comunicados ao Procurador-Geral da República para os devidos efeitos.

Artigo 14.º

Regime de proteção de dados

1 — Os dados de telecomunicações e *Internet* obtidos de acordo com o preceituado na presente lei são processados e conservados nos centros de dados do SIS e do SIED, sendo o diretor de cada centro de dados o responsável

pelo seu tratamento nos termos do regime de proteção de dados pessoais.

2 — Cabe ao responsável pelo tratamento assegurar que os dados inseridos no centro de dados do SIS ou do SIED são tratados:

a) De forma lícita e com respeito pelo princípio da boa-fé;

b) De forma compatível com as finalidades que determinaram a sua recolha;

c) De modo a assegurar que sejam apagados ou retificados os dados inexatos ou incompletos, tendo em conta as finalidades da recolha e tratamento;

d) De modo a que a conservação seja sempre fundamentada e restrita ao período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

3 — O tratamento dos dados obtidos, nomeadamente a inserção no centro de dados do SIS ou do SIED, bem como a atualidade, fundamento e prazo de conservação, arquivo e eliminação, obedece ao regime especial de proteção de dados pessoais do SIRP, bem como aos critérios e normas classificadas de segurança dos centros de dados do SIS e do SIED.

4 — Aos dados de telecomunicações e *Internet* constantes dos centros de dados do SIS e do SIED aplicam-se os prazos de conservação, eliminação e destruição definidos em regulamento aprovado pelo Conselho de Ministros, após o parecer obrigatório da Comissão de Fiscalização de Dados do SIRP e a apreciação do Conselho Superior de Informações, nos termos do regime do SIRP aplicável aos centros de dados do SIS e do SIED.

5 — O procedimento de acesso a dados de telecomunicações e *Internet* da presente lei é coberto pelo regime do segredo de Estado aplicável ao SIRP, sem prejuízo do disposto no regime do pessoal do SIRP relativo à credenciação de segurança.

Artigo 15.º

Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa

1 — A Comissão de Fiscalização de Dados do SIRP é a autoridade pública competente para a fiscalização do respeito pelos princípios e cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados obtidos de acordo com o procedimento obrigatório e vinculado previsto na presente lei.

2 — Sem prejuízo dos demais poderes de fiscalização previstos no regime geral aplicável aos centros de dados do SIS e do SIED, os dados de telecomunicações e *Internet* obtidos de acordo com o procedimento previsto na presente lei estão sujeitos à fiscalização oficiosa, por referência nominativa, da Comissão de Fiscalização de Dados do SIRP.

3 — Para os efeitos previstos no número anterior, a formação das secções criminais do Supremo Tribunal de Justiça comunica à Comissão de Fiscalização de Dados do SIRP as autorizações concedidas com referência nominativa.

4 — Os diretores dos centros de dados do SIS e do SIED prestam especial apoio à Comissão de Fiscalização de Dados do SIRP para efeitos do cumprimento do disposto no presente artigo.

5 — Das irregularidades ou violações verificadas deve a Comissão de Fiscalização de Dados do SIRP dar conhe-

cimento, através de relatório, ao Conselho de Fiscalização do SIRP.

6 — O direito de acesso dos cidadãos aos dados processados ou conservados nos centros de dados do SIS e do SIED é exercido através da Comissão de Fiscalização de Dados do SIRP segundo o procedimento previsto no regime geral aplicável aos centros de dados do SIS e do SIED quanto à fiscalização mediante participação.

7 — A Comissão de Fiscalização de Dados do SIRP deve ordenar o cancelamento ou retificação dos dados de telecomunicações e *Internet* recolhidos que envolvam violação dos direitos, liberdades e garantias consignados na Constituição e na lei e, se for caso disso, exercer a correspondente ação penal.

Artigo 16.º

Conselho de Fiscalização do Sistema de Informações da República Portuguesa

1 — O procedimento de acesso e os dados de telecomunicações e *Internet* obtidos nos termos do disposto na presente lei estão igualmente sujeitos aos poderes de fiscalização do Conselho de Fiscalização do SIRP.

2 — Compete ao Conselho de Fiscalização do SIRP receber do Secretário-Geral, com regularidade mínima bimensal, uma lista dos pedidos de autorização de acesso a dados de telecomunicações e *Internet* submetidos à formação das secções criminais referida no artigo 12.º, podendo solicitar e obter os esclarecimentos e informações complementares que considere necessários e adequados ao exercício das suas funções de fiscalização.

Artigo 17.º

Alteração à Lei da Organização do Sistema Judiciário

Os artigos 47.º e 54.º da Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário), alterada pela Lei n.º 40-A/2016, de 22 de dezembro, que a republicou, 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.

Artigo 54.º

[...]

- 1 —
- 2 —

3 — 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 telecomu-

nicações 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.»

Aprovada em 19 de julho de 2017.

O Presidente da Assembleia da República, *Eduardo Ferro Rodrigues*.

Promulgada em 14 de agosto de 2017.

Publique-se.

O Presidente da República, MARCELO REBELO DE SOUSA.

Referendada em 16 de agosto de 2017.

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

Lei n.º 99/2017

de 25 de agosto

Procede à segunda alteração à Lei n.º 12/2009, de 26 de março, que estabelece o regime jurídico da qualidade e segurança relativa à dádiva, colheita e análise, processamento, preservação, armazenamento, distribuição e aplicação de tecidos e células de origem humana, e transpõe as Diretivas 2015/565/UE e 2015/566/UE, da Comissão, de 8 de abril de 2015.

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

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objeto

1 — A presente lei procede à segunda alteração à Lei n.º 12/2009, de 26 de março, que estabelece o regime jurídico da qualidade e segurança relativa à dádiva, colheita, análise, processamento, preservação, armazenamento, distribuição e aplicação de tecidos e células de origem humana, alterada pela Lei n.º 1/2015, de 8 de janeiro, de forma a transpor para a ordem jurídica interna a Diretiva 2015/565/UE, da Comissão, de 8 de abril de 2015, que altera a Diretiva 2006/86/CE no que se refere a certos requisitos técnicos para a codificação dos tecidos e células de origem humana.

2 — A presente lei estabelece ainda os procedimentos de verificação da equivalência das normas de qualidade e segurança dos tecidos e células importados e transpõe para a ordem jurídica interna a Diretiva 2015/566/UE, da Comissão, de 8 de abril de 2015.

CAPÍTULO II

Alteração legislativa

Artigo 2.º

Alteração à Lei n.º 12/2009, de 26 de março

Os artigos 4.º, 5.º, 6.º, 8.º, 12.º, 13.º, 14.º, 20.º, 22.º e 25.º da Lei n.º 12/2009, de 26 de março, alterada pela