ASSEMBLEIA DA REPÚBLICA

DIVISÃO DE INFORMAÇÃO
LEGISLATIVA PARLAMENTAR

NOVEMBRO 2022

METADADOS

ENQUADRAMENTO NACIONAL E INTERNACIONAL

SÍNTESE
INFORMATIVA

FICHA TÉCNICA

Divisão de Informação Legislativa e Parlamentar – DILP

Título:
Metadados – Enquadramento Nacional e Internacional

Pesquisa, compilação, análise e tratamento por:
Belchior Lourenço, Fernando Bento Ribeiro, Filipa Paixão, Maria João Godinho, Rui Brito e Sandra Rolo

Arranjo e Composição Gráfica:
Nuno Amorim

Síntese Informativa n.º 75

Data de publicação:
Novembro de 2022

Av. D. Carlos I, 128-132 – 3.º
1200-651 LISBOA

ÍNDICE

NOTA PRÉVIA

A pedido do Senhor Coordenador do Grupo de Trabalho – Metadados, foi elaborada a presente síntese informativa em matéria de metadados.

O referido Grupo de Trabalho foi constituído para preparação da nova apreciação na generalidade dos Projetos de Lei n.os 70/XV/1.ª (PSD) - Procede à segunda 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, conformando-a com o Acórdão do Tribunal Constitucional n.º 268/2022, 79/XV/1.ª (CH) - Altera a Lei n.º 32/2008, de 17 de julho, por forma a harmonizá-la com os preceitos constitucionais em vigor e 100/XV/1.ª (PCP) - Altera a Lei n.º 32/2008, de 17 de julho sobre conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas e da Proposta de Lei n.º 11/XV/1.ª (GOV) - Regula o acesso a metadados referentes a Comunicações Eletrónicas para fins de investigação criminal.

A síntese incide sobre o enquadramento jurídico da matéria aqui em causa em vários países da União Europeia, em concreto, na Alemanha, na Áustria, na Bélgica, na Dinamarca, em Espanha, na Eslovénia, na Finlândia, em França, nos Países Baixos, na Irlanda, em Itália e na Suécia. É igualmente efetuado o enquadramento da matéria no Reino Unido.

Considera-se útil efetuar um enquadramento do tema dos metadados e do que serve de fundamento às alterações legislativas propostas.

Neste seguimento, os metadados podem definir-se como «dados sobre dados», correspondendo a marcos ou pontos de referência que permitem circunscrever a informação de todas as formas, nomeadamente identificando, descrevendo ou localizando tal informação.

Têm vindo a ser entendidos como estando separados do núcleo duro da informação, ou seja, do seu conteúdo. Quer isto dizer que, muito embora permitam perceber, por exemplo, quem fez determinada chamada, a quem ligou e quanto tempo durou a conversa, não revelam o seu conteúdo. O mesmo se passa, por exemplo, com imagens ou vídeos: sabe-se quando e onde foram captados, mas não o que contêm.

São, por isso, uma espécie de rasto digital de todos os dados que enviamos ou comunicações que efetuamos.

A questão que tem vindo a ser colocada, quer a nível nacional, quer a nível europeu, é a da admissibilidade da retenção dos metadados resultantes de comunicações face ao direito à reserva da vida privada e à proteção dos dados pessoais.

I) UNIÃO EUROPEIA

No contexto europeu, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas[1], visou harmonizar «as disposições dos Estados-Membros necessárias para garantir um nível equivalente de protecção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade, no que respeita ao tratamento de dados pessoais no sector das comunicações electrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações electrónicas na Comunidade» (n.º 1 do artigo 1.º). Entre outros, este diploma estabeleceu:

1. A obrigação dos Estados-Membros garantirem a «confidencialidade das comunicações e respectivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações electrónicas publicamente disponíveis», proibindo, nomeadamente, o armazenamento de «dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, excepto quando legalmente autorizados a fazê-lo» (n.º 1 do artigo 5.º);
2. A obrigatoriedade da eliminação ou da ocultação da identidade referente a «dados de tráfego relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações electrónicas publicamente disponíveis», assim que deixem de ser necessários (n.º 1 do artigo 6.º);
3. A possibilidade dos Estados-Membros poderem adotar medidas restritivas dos direitos inerentes às obrigações supra referidas, «sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas» (n.º 1 do artigo 15.º).

Por seu lado, a Diretiva 2006/24/CEE, 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, pretendeu «harmonizar as disposições dos Estados-Membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro» (n.º 1 do artigo 1.º).

[1] Texto retirado do portal legislativo da União Europeia *EUR-LEX*. Todas as referências legislativas e jurisprudenciais relativas à União Europeia são feitas para este portal oficial, salvo indicação em contrário. Consultas efetuadas a 25/11/2022.

Esta Diretiva, para além de aditar o n.º 1-A[2] ao artigo 15.º da Diretiva 2002/58/CE, estabeleceu a obrigação de os Estados-Membros tomarem medidas para garantir a conservação dos dados previstos no diploma[3], «na medida em que sejam gerados ou tratados no contexto da oferta dos serviços de comunicações em causa por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações quando estes fornecedores estejam sob a sua jurisdição» (n.º 1 do artigo 3.º). O artigo 4.º obriga a que os Estados-Membros diligenciem no sentido de assegurar que, aos dados que tenham sido conservados, apenas possam ter acesso as autoridades nacionais competentes, nos casos específicos previstos na legislação nacional, desde que respeitados os requisitos da necessidade e da proporcionalidade.

As categorias de dados que devem ser conservados, ao abrigo desta Diretiva, vêm previstos no seu artigo 5.º, o qual contém especificações consoante se trate de comunicações telefónicas nas redes fixa e móvel ou de acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet. De uma forma geral, devem ser conservados os dados que se mostrem necessários para:

1) encontrar e identificar a fonte de uma comunicação;
2) encontrar e identificar o destino de uma comunicação;
3) identificar a data, a hora e a duração de uma comunicação;
4) identificar o tipo de comunicação;
5) identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
6) identificar a localização do equipamento de comunicação móvel.

Acrescenta-se no n.º 3 do mesmo artigo 5.º que «não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações».

Relativamente ao período de conservação, determina-se no artigo 6.º da Diretiva que os dados supra elencados devem ser conservados por períodos entre seis meses e dois anos, a contar da data da comunicação.

Esta Diretiva deveria ter sido transposta para o ordenamento jurídico dos Estados-Membros até ao dia 15 de setembro de 2007, sendo que, de acordo com a informação constante do portal *EUR-LEX*, todos os países já terão, através de uma ou mais medidas legislativas, procedido a tal transposição.

A Diretiva 2006/24/CE, foi considerada inválida por decisão do Tribunal de Justiça da União Europeia (TJUE), de 8 de abril de 2014, relativa aos processos n.ºs C-293/12 e C-594/12.

A referida decisão de invalidade teve por fundamento o seguinte entendimento:

[2] No qual se estabelece que «o n.º 1 não é aplicável aos dados cuja conservação seja especificamente exigida pela Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, 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 (8), para os fins mencionados no n.º 1 do artigo 1.o dessa diretiva».
[3] O conceito de dados aplicável à Diretiva 2006/24/CEE abrange «os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador» [alínea a) do n.º 2 do artigo 2.º].

1. Os dados elencados pela Diretiva, muito embora não incidam sobre o conteúdo, são «suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados» (ponto 27).
2. «Em tais circunstâncias, apesar de a Diretiva 2006/24 não autorizar, como resulta dos seus artigos 1.°, n.º 2, e 5.°, n.º 2, a conservação do conteúdo da comunicação e das informações consultadas através de uma rede de comunicações eletrónicas, não está excluído que a conservação dos dados em causa possa ter incidência na utilização, pelos assinantes ou pelos utilizadores registados, dos meios de comunicação previstos por esta diretiva e, consequentemente, no exercício, por estes últimos, da sua liberdade de expressão, garantida pelo artigo 11.º da Carta[4].» (ponto 28).
3. «A conservação dos dados, para efeitos do eventual acesso aos mesmos pelas autoridades nacionais competentes, como prevista pela Diretiva 2006/24, diz direta e especificamente respeito à vida privada e, assim, aos direitos garantidos pelo artigo 7. º[5] da Carta. Além disso, essa conservação dos dados está abrangida pelo âmbito de aplicação do artigo 8. º[6] desta, uma vez que constitui um tratamento de dados pessoais na aceção deste artigo e deve, assim, necessariamente, respeitar as exigências de proteção de dados resultantes deste artigo» (ponto 29).
4. O acesso das autoridades nacionais competentes aos dados constitui uma ingerência suplementar neste direito fundamental (ponto 35).
5. No que respeita à justificação da referida ingerência, conclui-se que «em conformidade com o artigo 52.º, n.º 1[7], da Carta, qualquer restrição ao exercício dos direitos e liberdades reconhecidos por esta deve ser prevista por lei, respeitar o conteúdo essencial desses direitos e liberdades, e, na observância do princípio da proporcionalidade, só podem ser introduzidas restrições a esses direitos e liberdades se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteção dos direitos e liberdades de terceiros» (ponto 38).

[4] O artigo 11.º da Carta dos Direitos Fundamentais da União Europeia (de ora em diante designada apenas por Carta), estabelece o seguinte: «1. Qualquer pessoa tem direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras. 2. São respeitados a liberdade e o pluralismo dos meios de comunicação social.»

[5] Nos termos do qual «todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.»

[6] O qual dispõe: «1. Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.»

[7] No qual se estabelece que «Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros.» Repare-se que a obrigação pelo respeito do princípio da proporcionalidade vem igualmente prevista no Tratado da UE, em concreto, no n.º 3 do artigo 5.º, nos termos do qual «em virtude do princípio da proporcionalidade, o conteúdo e a forma da ação da União não devem exceder o necessário para alcançar os objetivos dos Tratados».

6. Tendo em conta a extrema importância dos dados gerados pelas comunicações eletrónicas na prevenção de infrações e na luta contra a criminalidade, designadamente a criminalidade organizada, entendeu o TJUE que a sua conservação, com vista a permitir o eventual acesso aos mesmos pelas autoridades nacionais competentes, responde efetivamente a um objetivo de interesse geral, sendo, portanto, uma medida adequada à realização do objetivo prosseguido pela diretiva (ponto 49).
7. Contudo, não entende o referido Tribunal que seja uma medida necessária à realização de tal objetivo, tendo em conta que:
   a) A Diretiva «abrange de maneira geral todas as pessoas, todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego, não sendo efetuada nenhuma diferenciação, limitação ou exceção em função do objetivo de luta contra as infrações graves» (ponto 57);
   b) De facto, a Diretiva «não exige nenhuma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública e, designadamente, não se limita a uma conservação nem de dados relativos a um período de tempo e/ou a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar implicadas, de uma maneira ou de outra, numa infração grave, nem de dados relativos a pessoas, cuja conservação, por outros motivos, pudesse contribuir para a prevenção, a deteção ou a repressão de infrações graves» (ponto 58);
   c) Assim, a Diretiva «não estabelece regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta, comportando uma ingerência nestes direitos fundamentais, de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que se limita efetivamente ao estritamente necessário» (ponto 65).
8. Por fim, refere-se ainda na decisão que, «no que respeita às regras relativas à segurança e à proteção dos dados conservados pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, há que concluir que a Diretiva 2006/24 não prevê garantias suficientes, como exige o artigo 8.º da Carta, que permitam assegurar uma proteção eficaz dos dados conservados contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos» (ponto 66).

De referir é, ainda, a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

O n.º 1 do artigo 4.º desta Diretiva impõe que os Estados-Membros aprovem legislação interna que reconheça que os dados pessoais devam ser: «objeto de um tratamento lícito e leal» [alínea a)]; «recolhidos para finalidades determinadas, explícitas e legítimas, e não tratados de uma forma incompatível com essas finalidades» [alínea b)]; «adequados, pertinentes e limitados ao mínimo necessário relativamente às finalidades para as quais são tratados» [alínea c)]; «exatos e atualizados sempre que necessário; devem ser tomadas todas as medidas razoáveis para que os dados inexatos, tendo em conta as finalidades para as

quais são tratados, sejam apagados ou retificados sem demora» [alínea d)]; «conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados» [alínea e)]; e, «tratados de uma forma que garanta a sua segurança adequada, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas» [alínea f)].

Por seu lado, o artigo 5.º impõe que os Estados-Membros prevejam «prazos adequados para o apagamento dos dados pessoais ou para a avaliação periódica da necessidade de os conservar» devendo «ser previstas regras processuais que garantam o cumprimento desses prazos».

O artigo 6.º da Diretiva obriga a que o responsável pelo tratamento de dados estabeleça uma distinção entre diferentes categorias de titulares de dados, em concreto, entre suspeitos e condenados por cometerem uma infração penal, vítimas ou potenciais vítimas de uma infração penal e terceiros envolvidos numa infração penal.

Por fim, o artigo 15.º determina quais as informações que o responsável pelo tratamento de dados deve facultar ao titular dos dados, sem prejuízo da possibilidade de adiar, limitar ou recusar a prestação de tais informações, «se e enquanto tais medidas constituírem medidas necessárias e proporcionadas numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de: a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais; b) Evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais; c) Proteger a segurança pública; d) Proteger a segurança nacional; e) Proteger os direitos e as liberdades de terceiros.»

O Regulamento (UE) 2016/679 do Parlamento Europeu 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados [RGPD]), regula a proteção conferida às pessoas singulares a respeito do tratamento de dados pessoais, determinando que os dados de base, de tráfego e de localização, na medida em que permitam identificar uma pessoa singular, ficam sujeitos à disciplina europeia de tratamento de dados pessoais (n.º 1 do artigo 3.º, conjugado com o n.º 1 do artigo 4.º).

Quer isto dizer que, nos termos das alíneas a) e b) do n.º 1 do artigo 5.º, tais dados apenas podem ser recolhidos para satisfazer finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades. A sua conservação não pode ser feita de forma a poder identificar os titulares, só podendo manter-se pelo período necessário para o cumprimento das finalidades que justificam o seu tratamento.

A **6 de outubro de 2020**, o TJUE voltou a pronunciar-se sobre esta matéria, confirmando a sua jurisprudência anterior, no sentido de que os dados das comunicações eletrónicas são confidenciais e, em princípio, os dados de tráfego e de localização não podem ser conservados de forma geral e indiscriminada.

O TJUE estabeleceu, contudo, exceções limitadas a esta regra, as quais poderão ser fundamentadas nos seguintes termos:

1. **Segurança nacional**: o interesse primordial na proteção das funções essenciais do Estado e dos interesses fundamentais da sociedade pode justificar que a conservação de dados constitua um objetivo legítimo para essa conservação, mas apenas se:
   a) existirem indícios concretos de uma ameaça real e atual ou previsível para a segurança nacional;
   b) seja definido um prazo para a conservação, sujeito a prorrogação em função da persistência da ameaça, desde que de forma não sistemática;
   c) a decisão de imposição da conservação ser objeto de fiscalização por um tribunal ou por uma entidade administrativa independente cuja decisão seja vinculativa.
2. **Luta contra a criminalidade e salvaguarda da segurança pública**: a conservação seletiva dos dados de tráfego e de localização, bem como a conservação generalizada e indiscriminada dos endereços IP de origem, pode ser justificada nesses casos, desde que seja limitada no que diz respeito às categorias de dados, aos meios de comunicação, às pessoas em causa e ao período temporal. Relativamente aos dados de identificação civil, é também permitida a conservação generalizada e indiscriminada de dados para efeitos de luta contra a criminalidade ou de prevenção de ameaças graves à segurança pública em geral, sem especificação de qualquer período de conservação.

Nesta decisão do TJUE conclui-se ainda pela possibilidade da existência de regulamentações nacionais que imponham aos prestadores de serviços de comunicações eletrónicas o recurso, por um lado, à análise automatizada e à recolha em tempo real de dados de tráfego e de dados de localização e, por outro, à recolha em tempo real de dados técnicos relativos à localização dos equipamentos terminais utilizados, quando:

I. «o recurso à análise automatizada esteja limitado a situações em que um Estado-Membro se encontra confrontado com uma ameaça grave para a segurança nacional que se revele real e atual ou previsível, podendo o recurso a essa análise ser objeto de fiscalização efetiva, quer por um órgão jurisdicional quer por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos, destinada a verificar a existência de uma situação que justifique a referida medida, bem como o respeito das condições e das garantias que devem estar previstas»;
II. «o recurso a uma recolha em tempo real de dados de tráfego e de dados de localização esteja limitado às pessoas em relação às quais existe uma razão válida para suspeitar que estão de alguma forma envolvidas em atividades terroristas e esteja sujeito a fiscalização prévia, quer por um órgão jurisdicional quer por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos, a fim de assegurar que tal recolha em tempo real apenas é autorizada no limite do estritamente necessário.»

Por fim, no acórdão de 20 de setembro de 2022, referente aos processos apensos C-793/19 e C-794/19, o TJUE confirma que o Direito da UE «se opõe a medidas legislativas nacionais que preveem, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a

segurança pública, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização».

Não se opõe, contudo, a que os Estados-membros aprovem medidas legislativas que:

1. Para efeitos da **salvaguarda da segurança nacional**, imponham aos prestadores de serviços de comunicações eletrónicas que procedam a uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, verificados os pressupostos mencionados a propósito do acórdão de 6 de outubro de 2020 (ponto 1 supra).
2. Para efeitos da **salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,** imponham aos prestadores de serviços de comunicações eletrónicas que procedam a uma:
   a) conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas renovável;
   b) conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;
   c) conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos.
3. Para efeitos da luta contra a criminalidade grave e, a *fortiori*, da salvaguarda da segurança nacional, imponham aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, que procedam, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem.

Essa legislação nacional deve, além disso, assegurar, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito pelas respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso.

No contexto da UE, cumpre ainda fazer referência ao seguinte:

1. A Comissão Europeia apresentou, a 11 de janeiro de 2017, uma Proposta de Regulamento relativa ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas). Esta proposta encontra-se em fase discussão no Parlamento[8].

   De acordo com o artigo 11.º da Proposta, «O direito da União ou o direito dos Estados-Membros podem restringir, através de medidas legislativas, o âmbito das obrigações e dos direitos previstos nos artigos 5.º a 8.º, sempre que tal restrição respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária, adequada e proporcionada, numa sociedade

[8] Conforme informação constante do portal do Parlamento Europeu.

democrática, para salvaguardar um ou mais dos interesses públicos gerais a que se refere o artigo 23.º, n.º 1, alíneas a) a e), do Regulamento (UE) 2016/679 ou uma função de controlo, de inspeção ou de regulamentação associada ao exercício da autoridade pública relativamente a esses interesses» (n.º 1).

2. Por seu lado, o Conselho Europeu, na sequência da reunião ocorrida a 10 e 11 de dezembro de 2020, na qual o tema da retenção de dados foi abordado, concluiu[9] que «é fundamental que as autoridades responsáveis pela aplicação da lei e as autoridades judiciárias possam exercer os seus poderes legais, tanto em linha como fora de linha, para combater a criminalidade grave. O Conselho Europeu salienta a necessidade de fazer avançar os trabalhos respeitantes à conservação de dados necessária para combater a criminalidade grave, à luz da jurisprudência mais recente do Tribunal de Justiça Europeu e no pleno respeito dos direitos e das liberdades fundamentais» (26), exortando, nessa sequência, «os Estados-Membros a intensificarem os seus esforços no sentido de utilizar plenamente as bases de dados e os sistemas de informação europeus, em particular no que diz respeito à introdução, nas bases de dados, de dados pertinentes sobre pessoas que um Estado-Membro considere representarem uma ameaça grave de terrorismo ou extremismo violento, incluindo os combatentes terroristas estrangeiros» (28).

II) PORTUGAL

A Lei n.º 41/2004, de 18 de agosto[10], transpôs para a ordem jurídica nacional a Diretiva n.º 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 setor das comunicações eletrónicas, assegurando «a proteção dos interesses legítimos dos assinantes que sejam pessoas coletivas na medida em que tal proteção seja compatível com a sua natureza» (n.º 3 do artigo 1.º). Na mesma norma determina-se que são definidas em legislação especial «as exceções à aplicação da presente lei que se mostrem estritamente necessárias para a proteção de atividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infrações penais» (n.º 4).

A Lei n.º 32/2008, de 17 de julho, também designada por «Lei dos Metadados», transpôs para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março. Este diploma estabelece as regras relativas à conservação dos dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas em termos equivalentes ao que vem previsto na Diretiva n.º 2006/24/CE.

[9] Conclusões disponíveis no portal do Conselho Europeu.
[10] Texto consolidado retirado do sítio da internet do Diário da República Eletrónico. Todas as referências legislativas e jurisprudenciais relativas a Portugal são feitas para este portal oficial, salvo indicação em contrário. Consultas efetuadas a 23/11/2022.

Assim:

1. Determina-se no n.º 1 do artigo 3.º que «a conservação e a transmissão dos dados[11] têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes».
2. O elenco de categorias de dados discorrido no artigo 4.º coincide integralmente com o que vem previsto na Diretiva 2006/24/CE, a saber, os dados necessários para:
    a) Encontrar e identificar a fonte de uma comunicação;
    b) Encontrar e identificar o destino de uma comunicação;
    c) Identificar a data, a hora e a duração de uma comunicação;
    d) Identificar o tipo de comunicação;
    e) Identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
    f) Identificar a localização do equipamento de comunicação móvel.

    O mesmo se diga em relação às especificações previstas para cada uma das categorias.
3. O n.º 2 do artigo 1.º proíbe a conservação de dados que revelem o conteúdo das comunicações, «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».
4. De acordo com o n.º 1 do artigo 5.º, conjugado com o n.º 1 do artigo 4.º, os dados telefónicos e da internet relativos a chamadas telefónicas falhadas devem ser conservados quando sejam gerados ou tratados e armazenados por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações.
5. Os dados abrangidos pelo diploma devem ser conservados pelo período de um ano a contar da data da conclusão da comunicação (artigo 6.º).
6. Nos termos do artigo 9.º. tais dados são transmitidos mediante autorização do juiz de instrução, por despacho fundamentado, «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» (n.º 1), e mediante requerimento do Ministério Público ou da autoridade de polícia criminal competente (n.º 2). Para a transmissão aqui em causa, apenas se exige o consentimento, efetivo ou presumido, da vítima de crime, quando os dados lhe digam respeito, o mesmo não se aplicando ao suspeito, arguido ou seu intermediário (n.º 3).

    A transmissão dos dados deve, contudo, apenas ser deferida se respeitar os princípios da adequação, necessidade e proporcionalidade (n.º 4), sem prejuízo da «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» (n.º 5).

[11] A definição de «dados» constante do diploma corresponde, *ipsis verbis*, à definição constante da Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março [alínea a) do n.º 1 do artigo 2.º].

Os termos das condições técnicas e de segurança em que se processa a comunicação eletrónica para efeitos da transmissão de 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 foram fixados na Portaria n.º 469/2009, de 6 de maio.

A 19 abril de 2022, a requerimento da Provedora de Justiça, o Tribunal Constitucional (TC) declarou, no acórdão n.º 268/2022[12], a inconstitucionalidade, com força obrigatória geral, de alguns artigos desta lei, em concreto:

1. Da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma lei;
2. Da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros.

Tal decisão foi proferida com base nos seguintes fundamentos:

1. O tratamento dos metadados a que se referem as normas fiscalizadas (dados de base[13], dados de tráfego[14] que não pressupõem uma comunicação interpessoal e dados de tráfego relativos a comunicações interpessoais), ao manter o rastreio dos passos dos utilizadores, seja quanto à sua localização, seja quanto à utilização que fazem da internet, seja quanto às pessoas com quem contactam ou tentam contactar, por telefone, correio eletrónico, mensagens escritas ou através da internet, é suscetível de comprimir os direitos à reserva da intimidade da vida privada, ao livre desenvolvimento da personalidade (n.º 1 do artigo 26.º da Constituição da República Portuguesa[15][16]) e à autodeterminação informativa (n.os 1[17] e 4[18] do artigo 35.º da Constituição da República Portuguesa) (ponto 10).

[12] Publicado no Diário da República, 1.ª Série, a 3 de junho de 2022.
[13] Os dados de base referem-se à conexão à rede, independentemente de qualquer comunicação, permitindo a identificação do utilizador de certo equipamento – nome, morada e telefone (conforme referido em vários acórdãos do TC, nomeadamente o Acórdão n.º 403/2015).
[14] Os dados de tráfego são definidos como «os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência) (conforme referido no Acórdão n.º 403/2015 do TC).
[15] Dispõe esta norma que «A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação»
[16] Texto consolidado retirado do portal da Assembleia da República. Todas as referências legislativas relativas à Constituição da República Portuguesa são feitas para este portal oficial, salvo indicação em contrário. Consultas efetuadas a 18/11/2022.
[17] Prevê-se nesta norma que «Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.»
[18] De acordo com esta norma, «É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.»

2. O direito à reserva da intimidade da vida tutela os indivíduos contra o acesso a um conjunto de informações que dizem respeito apenas aos próprios (por onde circulam, em que momento, em que contextos), envolvendo a proteção constitucional dos dados que permitem retirar conclusões sobre essas circunstâncias (ponto 11).
3. Ao determinar a conservação e o armazenamento dos dados pessoais aí elencados pelo período de um ano, as normas dos artigos 4.º e 6.º da Lei n.º 32/2008, de 17 de julho, constringem, pelo menos, os direitos à reserva da intimidade da vida privada, ao livre desenvolvimento da personalidade e à autodeterminação informativa (ponto 15).
4. «É desde logo evidente que as normas fiscalizadas não obedecem a uma das condições de que depende a conformidade constitucional das medidas legislativas relativas à conservação de dados pessoais: o legislador não prescreveu a necessidade de o armazenamento dos dados ocorrer no território da União Europeia, pondo em causa a efetividade dos direitos avalizados pelos n.os 1 e 4 do artigo 35.º da Constituição, interpretados em conformidade com o disposto nos artigos 7.º e 8.º da CDFUE[19]. Ao admitir que tais dados possam ser conservados em países subtraídos à fiscalização por autoridade administrativa independente e aos direitos de auditoria dos visados, o legislador transgride a injunção de previsão do seu armazenamento em local em que sejam efetivas as garantias constitucionais de proteção e a intervenção da autoridade administrativa independente (n.º 2[20] do artigo 35.º da Constituição), falecendo a garantia de proteção destes dados contra a devassa ou difusão. Com efeito, o ordenamento apenas tutelou a transferência para Estados terceiros de tais dados pessoais e somente no que respeita a pessoas singulares; não tendo determinado, como resultava da injunção constitucional, a obrigação de armazenamento desses dados num Estado-Membro da União Europeia.» (ponto 16).
5. «Mesmo que o legislador tivesse previsto tal obrigação, as normas fiscalizadas sempre envolveriam — pelo menos quanto aos dados de tráfego — uma restrição desproporcionada aos direitos consagrados nos n.os 1 e 4 do artigo 35.º da Constituição, em conjugação com o n.º 1 do artigo 26.º, interpretados em conformidade com o disposto nos artigos 7.º e 8.º da CDFUE» (ponto 17).
6. Ao não se prever a notificação dos visados de que as seus dados foram acedidos pelos órgãos competentes de investigação criminal, «restringe -se de modo desproporcionado o direito à autodeterminação informativa, consagrado no artigo 35.º, n.º 1, da Constituição (na dimensão de controlo do acesso de terceiros a dados pessoais) afetando, igualmente, o direito a uma tutela jurisdicional efetiva (artigo 20.º, n.º 1[21], da Constituição), por prejudicar a viabilidade prática de exercício de controlo judicial de acessos abusivos ou ilícitos aos dados conservados» (ponto 19.2).

[19] Carta dos Direitos Fundamentais da União Europeia.
[20] Estabelece-se nesta norma que «A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.»
[21] Dispõe esta norma que «A todos é assegurado o acesso ao direito e aos tribunais para defesa dos seus direitos e interesses legalmente protegidos, não podendo a justiça ser denegada por insuficiência de meios económicos.»

A Lei n.º 58/2019, de 8 de agosto, 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.

De acordo com o artigo 21.º, «o prazo de conservação de dados pessoais é o que estiver fixado por norma legal ou regulamentar ou, na falta desta, o que se revele necessário para a prossecução da finalidade» (n.º 1). Acrescenta-se no n.º 5 que «nos casos em que existe um prazo de conservação de dados imposto por lei, só pode ser exercido o direito ao apagamento previsto no artigo 17.º do RGPD findo esse prazo».

A Lei n.º 59/2019, de 8 de agosto, aprovou as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Entre outras normas, esta lei prevê, em termos idênticos aos definidos no artigo 4.º da Diretiva, os princípios gerais de proteção de dados.

A Comissão Nacional de Proteção de Dados (CNPD)[22], concluiu, na Deliberação n.º 641/2017[23], que «a Lei n.º 32/2008 contém normas que preveem a restrição ou ingerência nos direitos fundamentais ao respeito pela vida privada e pelas comunicações e à proteção dos dados pessoais com grande amplitude e intensidade, em clara violação do princípio da proporcionalidade e, portanto, em violação do n.º 1 do artigo 52.º da Carta dos Direitos Fundamentais da União. Com os mesmos fundamentos, existe uma restrição desproporcionada dos direitos à reserva da intimidade da vida provada, à inviolabilidade das comunicações e à proteção dos dados pessoais, em violação do disposto no n.º 2 do artigo 18.º da Constituição da República Portuguesa. Recomenda, por isso, a CNPD a revisão da Lei n.º 32/2008, de 17 de julho. (…) o regime deve distinguir as situações de uma concreta suspeita de prática de crime grave das situações em que haja indícios fortes de preparação de crimes graves.»

QUADRO-SÍNTESE DO ENQUADRAMENTO INTERNACIONAL

Sem prejuízo do seu desenvolvimento adiante, entende-se que é útil, nesta sede, deixar um quadro-síntese que sumarize o enquadramento da situação de cada um dos países abordados na sequência da aprovação da Diretiva 2006/24/CEE, bem como da sua situação após a decisão de invalidade, pelo TJUE, daquela mesma Diretiva:

[22] Portal oficial da CNPD.
[23] Texto integral disponível no portal oficial da CNPD.

País	Diploma de transposição da Diretiva 2006/24/CEE	Consequências da decisão de invalidade da Diretiva 2006/24/CEE por parte do TJUE
Alemanha	*Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*, aprovada em 2007 (não vigente - declarada inconstitucional em 2010) *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*, aprovada em 2015 (nunca aplicada)	Muito embora o Governo tenha anunciado a apresentação de uma iniciativa legislativa no sentido de alterar a redação da lei das telecomunicações ainda em vigor nesta matéria, não se localizou, contudo, tal iniciativa e as pesquisas realizadas parecem indicar não existir consenso no Governo quanto aos termos em que a nova lei deverá ser redigida.
Áustria	*27. Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird* *33. Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Sicherheitspolizeigesetz geändert werden*, ambas publicadas em maio de 2011 (não vigentes – declaradas inconstitucionais em 2014)	Atualmente, a Áustria não tem legislação que preveja a retenção de dados de forma generalizada e indiscriminada.
Bélgica	*Loi du 30 juillet 2013, portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle* (transposição parcial)	O Tribunal Constitucional deste país procedeu à anulação da *Loi du 30 juillet 2013, portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle* pelo *Arrêt n.º 84/2015 du 11 juin 2015*
Eslovénia	Electronic Communications Act (ZEKom-1)	Várias normas foram revogadas, revogação essa confirmada pelo Act Amending the Electronic Communications Act (ZEKom-1C).
Espanha	*Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*	Não foram introduzidas alterações legislativas, na sequência da decisão do TJUE.
Finlândia	Lei 343/2008, que introduziu alterações na Lei de Proteção de Dados de Comunicações Eletrónicas (516/2004)	Foram efetuadas alterações à Lei de Proteção de dados e Comunicações Eletrónicas, cujo nome foi alterado para Lei dos Serviços de Comunicações Eletrónicas.

França	*Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques*	Algumas normas do *Décret n.º 2006~358* foram anuladas pelo acórdão de 21/04/2021, n.º 393099, proferido pelo *Conseil d`État* (em concreto a *Assemblée*)
Irlanda	*Communications (Retention of Data) Act 2011 (Revised)*	Revogação do diploma de transposição pelo *Communications (Retention of Data) Act 2022*
Itália	*Decreto Legislativo 30 maggio 2008, n. 109*	Não foram introduzidas alterações legislativas na sequência da decisão do TJUE.
Países Baixos	Lei de 2009 e alteração introduzida à Lei de Telecomunicações	Não foram introduzidas alterações legislativas, muito embora tenha havido uma iniciativa legislativa nesse sentido, mas cujo processo legislativo não foi concluído. A decisão do Tribunal de Haia (C/09/480009 / KG ZA 14/1575), de 11 de março de 2015, determinou a cessação de vigência da Lei de Retenção de Dados de Telecomunicações.
Reino Unido	*Data Retention (EC Directive) Regulations 2007* *Data Retention (EC Directive) Regulations 2009*	Não foram introduzidas alterações específicas aos diplomas de transposição da Diretiva.
Suécia	Electronic Communications Act (2003:389) Swedish Code of Judicial Procedure Act on Collecting Information about Electronic Communications in the Law Enforcement Agencies' Intelligence Activities (2012:278)	Foram introduzidas alterações legislativas na sequência da decisão do TJUE.

2. ENQUADRAMENTO INTERNACIONAL

ALEMANHA

A Alemanha transpôs a Diretiva 2006/24/CE através da *Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG*[24] (lei que aprova o novo regime de vigilância das telecomunicações e outras medidas de investigação, transpondo a Diretiva 2006/24/CE), de 21 de dezembro de 2007, que alterou a *Telekommunikationsgesetz*[25] (TKG - lei das telecomunicações) e o *Strafprocessordnung*[26] (StPO - Código de Processo Penal); entre outros aspetos, refira-se que aquela lei previa a conservação de dados das comunicações telefónicas e eletrónicas por um período de seis meses. Em 2 de março de 2010, as normas introduzidas por aquela lei foram declaradas inconstitucionais pelo *Bundesverfassungsgericht* (Tribunal Constitucional) por violação do *artikel 10* da *Grundgesetz* (Constituição), que consagra o direito ao sigilo da correspondência, não pela conservação de dados em si mas pela forma e alcance com que a mesma estava prevista[27].

Em 2015 foi aprovada nova lei sobre conservação de dados das comunicações – a *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*[28] *(VerkDSpG* – lei que determina a obrigação de conservação de dados e o prazo máximo dessa conservação), que alterou novamente a lei das telecomunicações e o Código de Processo Penal. Assim, na sua redação atual, o §176[29] da lei das telecomunicações prevê que os operadores têm, a partir de 1 de julho de 2017, obrigação de conservação dos dados de tráfego dos seus clientes durante 10 semanas e dos dados de localização durante 4 semanas.

Os dados de tráfego em causa são elencados nos n.os 2 e 3[30] do mesmo dispositivo e o n.º 5 determina expressamente a exclusão do armazenamento, com base nestas normas, do conteúdo das comunicações, dos dados sobre páginas da *Internet* visitadas e dos dados dos serviços de correio eletrónico.

---

[24] Diploma retirado do portal da imprensa oficial alemã (*Bundesgesetzblatt)*.
[25] Diploma consolidado, na sua redação atual, retirado do portal oficial *GESETZE-IM-INTERNET.DE*. Todas as referências relativas à legislação da Alemanha devem considerar-se remetidas para o referido portal, salvo indicação expressa em contrário. Consultas efetuadas a 25/11/2022.
[26] Diploma consolidado na sua redação atual.
[27] A decisão pode ser consultada no portal do Tribunal Constitucional.
[28] Diploma retirado do portal da imprensa oficial alemã.
[29] Na numeração atual; era o §113 aquando da aprovação da *VerkDSpG.*
[30] Relativamente às comunicações de voz, devem ser armazenados: o número de telefone ou outro identificador das linhas; a data e a hora do início e o fim da ligação, com especificação do fuso horário subjacente; informações sobre o serviço utilizado, caso existam vários; no caso de comunicação de voz móvel, acresce ainda o identificador internacional dos utilizadores e a data e a hora da primeira ativação do serviço, indicando o fuso horário subjacente, no caso de serviços pré-pagos; e no caso dos serviços de comunicação de voz da Internet, também os endereços do Protocolo de Internet (IP) das linhas e de identificação dos utilizadores; estas prescrições aplicam-se também às mensagens escritas e outras. Relativamente aos serviços de acesso à Internet, devem ser armazenados: o endereço IP atribuído ao utilizador; um identificador exclusivo da ligação através da qual a Internet é usada, bem como a identificação de utilizador atribuída; data e hora do início e fim do uso da Internet no endereço em causa, especificando o fuso horário subjacente.

A lei das telecomunicações regula ainda outros aspetos da conservação de dados – o §177 determina como é feita a utilização dos dados, o §178 prevê medidas com vista à garantia da segurança dos dados (como o encriptamento e o armazenamento em servidores diferentes dos das operações correntes) e o §179 regula o registo dos acessos. É atribuída à *Bundesnetzagentur (BNetzA* - agência federal reguladora do setor das telecomunicações, correios, eletricidade, gás e ferrovia) competência para fiscalizar o cumprimento destas normas.

No entanto, ainda antes da aplicação destas normas, em 22 de junho de 2017, isto é, uns dias antes de os operadores terem de iniciar a conservação dos dados, o *Oberverwaltungsgericht* (tribunal administrativo de segunda instância) do Estado da Renânia do Norte-Vestefália, deu provimento a uma providência cautelar intentada por um operador de telecomunicações isentando-o de conservar os dados, designadamente por considerar a lei alemã incompatível com o direito da União Europeia. No entendimento deste tribunal é necessário restringir o número de pessoas afetadas pelo armazenamento de dados a casos em que haja pelo menos uma conexão indireta com crimes graves ou a prevenção de graves ameaças à segurança pública, bem como garantir que são tomadas medidas rigorosas para proteger os dados armazenados contra o uso indevido[31].

Em consequência, a *Bundesnetzagentur* declarou não pretender responsabilizar operadores de telecomunicações que não cumprissem a obrigação de conservação de dados a partir de 1 de julho de 2017 até haver um esclarecimento final da questão (cfr. declaração disponível no respetivo portal na Internet).

Também o *Bundesverwaltungsgericht* (Tribunal Administrativo Federal, que julga em última instância) entendeu, a propósito da transposição da Diretiva *e-Privacy*[32], haver dúvidas quanto à compatibilidade da lei alemã com as normas europeias, tendo em conta anteriores decisões do Tribunal de Justiça da União Europeia (TJUE), como as proferidas nos casos relativos à Suécia e ao Reino Unido (C-203/15 - *Tele2 Sverige* e C-698/15 - *Watson*). Como tal, em setembro de 2019, remeteu a questão ao TJUE e suspendeu a instância até haver decisão deste[33].

A decisão do TJUE (Processos apensos C-793/19 – *SpaceNet*, e C-794/19 – *TeleKom Deutschland*) foi anunciada em 20 de setembro de 2022, tendo o mesmo considerado que a lei alemã viola o direito da União Europeia já que a conservação indiferenciada e generalizada de dados de telecomunicações, mesmo que pelos períodos limitados de 4 e 10 semanas, põe em causa os direitos fundamentais das pessoas visadas.

[31] Conforme explicado em nota de imprensa disponível no portal do ministério da justiça do Estado da Renânia do Norte-Vestefália em: https://www.ovg.nrw.de/behoerde/presse/pressemitteilungen/01_archiv/2017/36_170622/index.php.
[32] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.
[33] A fundamentação desta decisão do Tribunal Administrativo Federal encontra-se explicada nesta nota de imprensa no respetivo sítio da *internet.*

O Ministro Federal da Justiça congratulou-se publicamente com esta decisão do TJUE[34] e anunciou que o Governo iria apresentar muito em breve uma iniciativa legislativa no sentido de alterar a redação da lei das telecomunicações ainda em vigor nesta matéria. Não se localizou, contudo, tal iniciativa e as pesquisas realizadas parecem indicar não existir consenso no Governo quanto aos termos em que a nova lei deverá ser redigida. Um dos pontos de discórdia parece ser a questão dos endereços IP no âmbito do combate à criminalidade grave, em particular os crimes sexuais contra crianças. De um lado os que defendem que também aqui se deve seguir o procedimento «*quick freeze*», visto configurar uma muito menor ingerência nos direitos fundamentais, como é o caso do Ministro da Justiça, Marco Buschmann (FDP), e do outro os que defendem a sua conservação indiferenciada e generalizada para esse fim, tendo em conta que o TJUE o considera admissível, como é o caso da Ministra do Interior, Nancy Faeser (SPD)[35] [36].

A 27 de setembro passado o *Bundestag* discutiu um projeto de resolução apresentado pelo grupo parlamentar CDU/CSU, instando o Governo federal a apresentar uma iniciativa legislativa «que implemente a possibilidade admitida pelo Tribunal de Justiça da União Europeia de conservação dos endereços IP para investigação de crimes de abuso sexual de crianças e pornografia infantil»[37], que baixou para discussão na Comissão de Assuntos Jurídicos, em conexão com várias outras comissões[38].

[34] O vídeo da conferência de imprensa na sequência do anúncio da decisão do TJUE pode ser visto aqui, estando disponível na página do Ministério Federal da Justiça onde é explicada de forma sintética a decisão do TJUE e o procedimento *quick freeze*. Já anteriormente notícias da comunicação social davam conta de o mesmo Ministro ser defensor deste tipo de solução e contrário ao armazenamento de dados de forma generalizada e indiferenciada.
[35] Recorde-se que o atual Governo alemão resulta de coligação entre SPD, FDP e Verdes.
[36] Toda esta questão pode ser lida em maior detalhe na edição de 4 de outubro do jornal do *Bundestag*, *Das Parlament*.
[37] Texto integral do debate disponível no portal do *Bundestag*; um resumo da discussão pode ser lido em https://www.bundestag.de/dokumente/textarchiv/2022/kw39-de-ip-adressen-911398.
[38] Como referido na página da referida iniciativa no portal do *Bundestag.*

ÁUSTRIA

A Diretiva 2006/24/CE suscitou grande atenção por parte dos meios de comunicação social e da opinião pública na Áustria ainda antes da sua adoção a nível europeu, essencialmente por preocupações com as suas implicações na privacidade e proteção dos dados dos utilizadores. Acabou por ser transposta apenas em 2012, mais de quatro anos depois do prazo (e após a condenação da Áustria por esse facto em 2010, pelo TJUE), através de alterações à lei das telecomunicações então em vigor (*Telekommunicationsgesetz 2003*[39]), aprovadas pela Lei Federal n.º 27, publicada a 18 de maio de 2011 (*27. Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird*), e também à lei da polícia de segurança (*Sicherheitspolizeigesetz*[40]), designadamente ao seu §53, e aos §§134 e 135 e outros do Código do Processo Penal (*Strafprozessordnung*[41]), estas através da Lei Federal n.º 33, publicada a 20 de maio de 2011 (*33. Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Sicherheitspolizeigesetz geändert werden*). Entre outros aspetos, previa-se a obrigação de os operadores de telecomunicações conservarem, de forma indiscriminada e indiferenciada, dados de tráfego e localização das comunicações pelo prazo de seis meses para fins de deteção, investigação e repressão de crimes graves, para cujo acesso era necessária uma ordem do Ministério Público, nos termos do Código de Processo Penal. Esta obrigação só produzia efeitos a partir de 1 de abril de 2012[42].

No entanto, pouco tempo depois a validade daquelas normas foi questionada junto do *Bundesverfassungsgericht* (Tribunal Constitucional), o qual suspendeu o processo e remeteu a questão ao TJUE para apreciação da compatibilidade da Diretiva com a Carta dos Direitos Fundamentais da União Europeia, em especial no que se refere aos direitos à reserva da vida privada e familiar, à proteção de dados pessoais e à liberdade de expressão[43]. Em 2014, o TJUE declarou a invalidade da Diretiva na decisão relativa aos processos apensos C-293/12 e C-594/12, que ficou conhecida como *Digital Rights Ireland*, e nesse

[39] Diploma consolidado retirado do portal oficial *RIS.BKA.GV.AT*. Todas as referências relativas à legislação da Áustria devem considerar-se remetidas para o referido portal, salvo indicação expressa em contrário. Consultas efetuadas a 25/11/2022.
[40] Aqui na sua versão consolidada atualmente em vigor.
[41] *Idem*.
[42] Os fornecedores de serviços de acesso à Internet deviam conservar: nome, endereço e identificação do utilizador a quem foi atribuído um endereço IP público num determinado momento, indicando o fuso horário subjacente; data e hora da atribuição e retirada de um endereço IP público num serviço de acesso à Internet, indicando o fuso horário subjacente; número de telefone da linha de chamada para acesso por linha telefónica; identificador único da linha utilizada para aceder à Internet. Os fornecedores de serviços telefónicos, incluindo através da Internet, deviam conservar: número de assinante ou outro identificador das linhas de origem e de destino da chamada, incluindo em caso de reencaminhamento de chamadas ou desvio de chamadas; nome e endereço dos utilizadores de origem e destino da chamada; data, hora do início e duração da comunicação, indicando o fuso horário subjacente; tipo de serviço utilizado (chamadas, serviços suplementares e serviços de mensagens e multimédia). No caso de redes móveis, determinava-se ainda a conservação de: identificador de assinante móvel internacional (IMSI) das linhas de origem e destino; identificador internacional do equipamento móvel (IMEI) de origem e destino da chamada; data e hora da primeira ativação do serviço e identificador de localização (ID da célula) onde o serviço foi ativado, no caso de serviços pré-pagos anónimos; identificador de localização (ID da célula) no início de uma ligação. Quanto aos prestadores de serviços de correio eletrónico, estavam obrigados a conservar: identificador atribuído ao utilizador; nome e endereço do utilizador; endereço eletrónico e endereço IP público do remetente e endereço eletrónico dos destinatários de mensagens de correio eletrónico; data, hora, ID e endereço IP do utilizador, indicando o fuso horário subjacente.
[43] Como explicado nesta nota à imprensa em inglês disponível no portal do Tribunal Constitucional austríaco.

mesmo ano o Tribunal Constitucional austríaco declarou inconstitucionais as normas que transpuseram a Diretiva, que assim cessam a sua vigência pouco mais de dois anos após entrarem em vigor[44].

Assim, atualmente, a Áustria não tem legislação que preveja a retenção de dados de forma generalizada e indiscriminada, mas está prevista a possibilidade de acesso pelos órgãos de investigação criminal a dados conservados para efeitos de faturação. Nos termos do §167 da atual lei das telecomunicações (*Telekommunikationsgesetz 2021*)[45], os operadores de telecomunicações devem conservar os dados de tráfego e localização das comunicações que sejam necessários para efeitos de faturação por um período geral de três meses (que pode ser mais longo em caso de reclamação, por exemplo, estendendo-se até ao pagamento e término do prazo para contestar), findo o qual devem ser apagados ou anonimizados. O n.º 2b do §135 (conjugado com o n.º 1 do §137) do *Strafprozeßordnung* (Código de Processo Penal) prevê a possibilidade de o Ministério Público, no âmbito de uma investigação criminal, determinar a conservação dos referidos dados por um período máximo de 12 meses. Este procedimento é conhecido como «*quick freeze*» e significa não uma obrigação de conservar dados mas sim de não eliminação de dados que foram conservados para outros fins e é por muitos considerado como não constituindo uma verdadeira alternativa à retenção generalizada de dados para fins de investigação criminal[46].

Quanto aos dados de localização, note-se que estão abrangidos apenas os necessários para efeitos de faturação, sendo que os restantes apenas podem ser processados se anonimizados ou mediante autorização do titular dos dados (§169 da lei das telecomunicações), isto sem prejuízo de situações de perigo iminente (para localizar o utilizador que faça uma chama de emergência, por exemplo, nos termos do §124 da mesma lei).

[44] A síntese e o texto integral da decisão podem ser consultados no já mencionado portal legislativo e no portal do Tribunal Constitucional, respetivamente.
[45] Também disponível em versão bilingue alemão/inglês.
[46] Veja-se a este propósito o resultado do estudo realizado para a Comissão Europeia *Study on the retention of electronic communications non-content data for law enforcement purposes*, publicado em dezembro de 2020, que se baseou nas respostas a um conjunto de questionários por parte de entidades nacionais dos Estados analisados, entre os quais a Áustria.

BÉLGICA

Como resulta do teor do artigo 2. da *Loi du 30 juillet 2013, portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle* foi por esta lei, que ocorreu a transposição parcial da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006 e do n.º 1 do artigo 15.º[47] da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 para o direito interno belga.

O Tribunal Constitucional anulou, conforme melhor desenvolvido infra, a *Loi du 30 juillet 2013.*
Não obstante, cumpre fazer referência à forma como as Diretivas acima mencionadas foram transpostas para o ordenamento jurídico belga.

O Capítulo 2. da *Loi du 30 juillet 2013*. (artigos 3. a 6.) procedia a alterações à *Loi du 13 juin 2005 relative aux communications électroniques*[48], concretamente ao seu artigo 4.. Este artigo enunciava as várias definições legais inerentes ao domínio das comunicações eletrónicas, sendo que o ponto 11º fixava a noção de operador como qualquer pessoa sujeita à obrigação de apresentar uma notificação nos termos do artigo 9.[49]. A norma aditava ainda o ponto 74º, o qual previa que eram consideradas chamadas sem sucesso quaisquer comunicações durante as quais uma chamada era efetuada, mas em que o seu atendimento não se verificava ou que era objeto de uma intervenção do operador de rede.

O artigo 5. concretizava a modificação no teor do artigo 126. da *Loi du 13 juin 2005*, como é o caso do conteúdo do primeiro e segundo parágrafos do § 1er., os quais determinavam que, sem prejuízo da *Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, os prestadores de serviços ao público de telefone fixo, telefone móvel, acesso à *Internet*, correio eletrónico e serviços de telefone através da *Internet*, bem como os prestadores das redes públicas de comunicações eletrónicas subjacentes podem conservar os dados de tráfego, localização, identificação dos utilizadores finais, os elementos de identificação do serviço de comunicações eletrónicas utilizado e do

[47] Esta norma institui que «Os Estados-Membros podem adoptar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.ºs 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.ºs 1 e 2 do artigo 6.º do Tratado da União Europeia».

[48] Diploma consolidado retirado do portal oficial *http://www.ejustice.just.fgov.be*. Todas as ligações eletrónicas a referências legislativas respeitantes à Bélgica são feitas para o referido portal, salvo indicação em contrário. Consultado no dia 14/11/2022.

[49] Norma que identifica os elementos a serem reportados, através desse documento, *ao Institut belge des services postaux et des télécommunications (IBPT)*. Este é, nos termos do ponto 3º do artigo 2. e do artigo 13. da *Loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges*, um organismo de interesse público dotado de personalidade jurídica. Uma das suas missões é, de acordo com a alínea *a*) do ponto 3º do artigo 14. da mesma lei, o controlo do respeito das disposições insertas na *Loi du 13 juin 2005 relative aux communications électroniques*.

equipamento terminal presumivelmente utilizado, gerados ou processados por estes no decurso da prestação dos serviços das comunicações em causa.
Para efeitos do presente artigo, a noção de prestadores de serviços compreendia, igualmente, os revendedores em nome próprio e por conta própria.

Quanto ao artigo 6. introduzia o § 3ter no artigo 145. da mesma lei, sendo que esta norma estabelecia as sanções aplicáveis a qualquer pessoa que, no exercício das suas funções, fora das circunstâncias previstas na lei, ou sem o cumprimento das formalidades exigidas pela lei, com intenção fraudulenta ou de causar danos, acedesse, conservasse ou utilizasse os dados abrangidos pelo diploma.

E o Capítulo 3. (artigo 7.) introduzia um novo parágrafo ao artigo 90decies do *Code d'instruction criminelle* - Livro Primeiro (artigos 8. a 136ter)[50], o qual estabelecia que ao relatório (elaborado pelo Ministro da Justiça e apresentado ao Parlamento sobre a aplicação dos artigos 90ter a 90novies deste código) é anexado a informação descrita no parágrafo 3 do § 6 do artigo 126. da *Loi du 13 juin 2005 relative aux communications électroniques*.

Conforme referido supra, o Tribunal Constitucional belga procedeu à anulação da *Loi du 30 juillet 2013, portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle* pelo *Arrêt n.º 84/2015 du 11 juin 2015*, processo que teve origem em dois recursos interpostos junto deste órgão: um pela *Ordre des barreaux francophones et germanophone*[51] (Ordem dos Advogados de língua francesa e alemã), cujo requerimento deu entrada no tribunal no dia 24 de fevereiro de 2014; e outro pelas associações sem fins lucrativos «*Liga voor Mensenrechten*[52]» e «*Ligue des Droits de l'Homme*[53]» [Liga dos Direitos do Homem» (holandesa e francesa)], este requerimento foi recebido no tribunal no dia 25 de fevereiro de 2014. Em tais recursos requeria-se respetivamente, a anulação do artigo 5. e a anulação da *Loi du 30 juillet 2013*.

No ponto B.6. deste acórdão é mencionado o Acórdão do Tribunal de Justiça da União Europeia, de 8 de abril de 2014[54].

Neste seguimento, refere o Tribunal Constitucional, no ponto B.9., tal como o Tribunal de Justiça da União Europeia decidiu no seu acórdão (ponto 34), a obrigação imposta, pelos artigos 3.º e 6.º da Diretiva n.º 2006/24/CE, aos prestadores de serviços de comunicações eletrónicas acessíveis ao público ou de redes públicas de comunicação de conservar por um determinado período de tempo os dados relativos à vida privada de uma pessoa e às suas comunicações, como aquelas que são previstas no artigo 5.º da mesma

[50] Texto consolidado, consultado no dia 25/11/2022.
[51] Página eletrónica acessível em https://www.avocats.be/fr/qui-sommes-nous, consultada no dia 14/11/2022.
[52] Sítio da *Internet* disponível em *https://mensenrechten.be/*, consultado no dia 14/11/2022.
[53] Página eletrónica em https://www.liguedh.be/, consultada no dia 14/11/2022.
[54] O acórdão encontra-se acessível em https://curia.europa.eu/juris/document/document.jsf?mode=lst&pageIndex=0&docid=150642&part=1&doclang=PT&text=&dir=&occ=first&cid=252522, consultado no dia 14/11/2022.

diretiva, constituem uma ingerência nos direitos garantidos pelo artigo 7.º[55] da Carta[56]. Por outro lado, conforme expõe a mesma instituição da União Europeia, os artigos 4.º e 8.º dessa diretiva, estabelecem as regras quanto ao acesso pelas autoridades nacionais competentes aos dados, as quais são igualmente uma ingerência nos direitos garantidos pela mesma norma da Carta.

Segundo a mesma instituição da União Europeia, esta ingerência é, de acordo com o disposto no ponto 37 do seu acórdão, considerada particularmente grave.

O Tribunal Constitucional, ao longo do acórdão, reproduz algumas partes do supracitado acórdão do Tribunal de Justiça da União Europeia.

No ponto B.11., o Tribunal Constitucional menciona que pelas mesmas razões que levou o Tribunal de Justiça da União Europeia a decidir pela invalidade da diretiva 2006/24/CE, com a adoção do artigo 5. da *Loi du 30 juillet 2013*, o legislador ultrapassou os limites impostos pelo princípio da proporcionalidade no que concerne aos artigos 7.º, 8.º, n.º 1 do artigo 52.º da Carta.

Por seu turno, o ponto B.12. do acórdão, o Tribunal Constitucional decide que, em razão da sua natureza indissociável com o artigo 5., também é necessário anular os artigos 1. a 4., 6. e 7. da *Loi du 30 juillet 2013*, o que significa que, esta decisão anulou totalmente a referida lei.

Cumpre, ainda, identificar outros atos legislativos relativos ao mesmo domínio jurídico – a recolha e conservação de dados no setor das comunicações eletrónicas que foram objeto de anulação por acórdãos do Tribunal Constitucional:

- A *Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques*[57], na redação atual, reflete as decisões do Tribunal Constitucional que resultaram de dois acórdãos emanados por este órgão, o *Arrêt n.º 96/2018 du 19 juillet 2018*[58], o qual menciona o acórdão de 21 de dezembro de 2016 do Tribunal de Justiça da União Europeia sobre os processos *Tele2 Sverige AB,* C-203/15 *et Secretary of State for the Home Department,* C-698/15.

  No ponto A.3.1. deste acórdão do Tribunal Constitucional é julgada a falta de distinção entre as pessoas cujas comunicações se encontram sujeitas a segredo profissional e os outros utilizadores.

  A decisão do Tribunal Constitucional foi submeter, antes de decidir sobre o mérito, ao Tribunal de Justiça da União Europeia três questões prejudiciais, e suspender o exame dos casos até o Tribunal de Justiça da União Europeia proferisse uma decisão nos processos C-207/16 *Ministerio Fiscal* e C-623/17 *Privacy International/Secretary of State for Foreign and Commonwealth Affairs* e outros.

[55] Norma que estipula o respeito pela vida privada e familiar, a qual dita que, «Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações».
[56] Acessível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12016P/TXT, consultada no dia 14/11/2022.
[57] Texto consolidado, consultado no dia 15/11/2002.
[58] Disponível em *https://www.const-court.be/public/f/2018/2018-096f.pdf*, consultado no dia 15/11/2022.

Sobre a mesma lei foi proferido outro acórdão do Tribunal Constitucional, o *Arrêt n.º 57/2021 du 22 avril 2021*[59], o qual foi no sentido da anulação da alínea *b*) do artigo 2. e dos artigos 3. a 11. e 14. da *Loi du 29 mai 2016*. Esta decisão teve por base os Acórdãos do Tribunal de Justiça da União Europeia de 2 outubro de 2018 sobre o processo C-207/16 *Ministerio Fiscal*, e de 6 de outubro de 2020 relativo ao processo C-623/17 *Privacy International/Secretary of State for Foreign and Commonwealth Affairs* e outros;

- A *Loi du 1er septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité* [60], concretamente os artigos 2. e 3. foram objeto de recurso e, por conseguinte, de decisão de anulação. A anulação produziu efeitos apenas na medida em que o conteúdo anterior desses artigos, o 127. da *Loi du 13 juin 2005 relative aux communications électroniques* e o artigo 16/2 da *Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*, não delimitava os elementos de identificação que eram recolhidos e tratados e os documentos de identificação a ter em conta, conforme determinado na *Arrêt n.º 158/2021 du 18 novembre 2021*[61] do Tribunal Constitucional. Entendeu-se que o diploma era igualmente desconforme com a recomendação deste mesmo órgão para a entrada em vigor, até 31 de dezembro de 2022, inclusive, de uma lei que enumere esses dados e os documentos de identificação.

  O artigo 127. da *Loi du 13 juin 2005 relative aux communications électroniques* e o artigo 16/2. da *Loi du 30 novembre 1998 organique des services de renseignement et de sécurité*[62] passam a integrar, através dos artigos 12 e 35 da *Loi du 20 julliet 2022, relative à la collecte et à la conservation des données d'identification et des métodonnées dans le secteur des communications életroniques et à la foumiture de ces données aux autorités*[63], o teor da decisão aqui em causa.

[59] Acessível em *https://www.const-court.be/public/f/2021/2021-057f.pdf*, consultado no dia 15/11/2022.
[60] Texto consolidado, consultado no dia 15/11/2022.
[61] Disponível em *https://www.const-court.be/public/f/2021/2021-158f.pdf*, consultado no dia 15/11/2022.
[62] Texto consolidado, consultado no dia 15/11/2022.
[63] Texto consolidado, consultado a 25/11/2022.

ESLOVÉNIA[64]

A Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, foi transposta para o direito nacional a 20 de dezembro de 2012, através do Electronic Communications Act (ZEKom-1)[65], tendo este normativo entrado em vigor a 15 de janeiro de 2013.

Após a entrada em vigor da Diretiva 2006/24/CEE, do Parlamento e do Conselho, de 15 de março de 2006, o *Information Commissioner of the Republic* requereu, a 3 de julho de 2014, a fiscalização da constitucionalidade dos artigos 162 a 169 do *Electronic Communications Act (ZEKom-1)*. Isto tendo em conta que foi igualmente neste diploma que foram introduzidas as alterações que transpuseram a referida Diretiva O Tribunal Constitucional da República da Eslovénia[66] decidiu-se[67] pela revogação[68] das disposições supracitadas, ordenando aos operadores de comunicações eletrónicas, a destruição imediata da totalidade dos dados decorrentes do presente quadro legal.

Na decorrência do quadro legal supracitado, assim como do Acórdão do Tribunal de Justiça da União Europeia (TJUE) de 8 de Abril de 2014, a Assembleia Nacional da República da Eslovénia[69] aprovou o Act Amending the Electronic Communications Act (ZEKom-1C)[70], de 21 de julho de 2017, tendo sido mantida a revogação dos artigos 162 a 169, supracitados.

[64] A informação contida neste resumo tem origem na resposta a um pedido realizado ao Parlamento esloveno, estando todas as ligações eletrónicas a remeter para as ligações indicadas nessa resposta, em língua eslovena
[65] Disponível no sítio da Internet do *pisrs.si* (versão inglesa). Consultas efetuadas a 25.11.2022.
[66] Portal oficial. Consultas efetuadas a 25.11.2022.
[67] «*Odločbo o razveljavitvi členov 162, 163, 164, 165, 166, 167, 168 in 169 Zakona o elektronskih komunikacijah*».
[68] Disponível no sítio da Internet do *pisrs.si*. Consultas efetuadas a 25.11.2022.
[69] Disponível no sítio da Internet do *dz-rs.si*. Consultas efetuadas a 25.11.2022.
[70] Disponível no sítio da Internet do *pisrs.si*. Consultas efetuadas a 25.11.2022.

ESPANHA

Em Espanha, a Diretiva 2006/24/CE foi transposta pela *Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*[71], que sofreu apenas uma alteração, pela *Ley 9/2014, de 9 de mayo, General de Telecomunicaciones*.

A Ley 25/2007, também conhecida com *Ley de Conservacíon de Datos,* ou LCD, prevê que os operadores de comunicações devem conservar, durante um período de 12 meses, os dados especificados no *artículo 3*, isto é, os dados necessários para encontrar e identificar a origem de uma comunicação (por telefone, telemóvel ou Internet), para identificar o destino de uma comunicação[72], para determinar a data, hora e duração de uma comunicação, para identificar o tipo de comunicação e para identificar os equipamentos de comunicação dos utilizadores ou o que é considerado como equipamento de comunicação, bem como os dados de acesso à Internet. Elencam-se, assim, relativamente a cada um dos tipos de comunicação, os dados a conservar, em que se incluem nome e morada do(s) utilizador(es), data e hora de início e fim, local, número(s) de telefone ou telemóvel, tipo de comunicação (voz, SMS, etc.), códigos internacionais de utilizadores e equipamentos[73], endereço IP. Em qualquer caso, está expressamente excluída a conservação do conteúdo de qualquer comunicação.

Relativamente ao prazo de conservação, prevê-se, relativamente a certos dados ou categorias de dados, a possibilidade de alargamento ou redução, a determinar por regulamentação posterior, após consulta dos operadores, até um máximo de dois anos ou um mínimo de seis meses, tendo em consideração o custo de armazenamento e conservação dos dados, bem como o interesse dos dados para efeitos de investigação, deteção e repressão de crimes graves.

Por outro lado, determina-se que é necessária autorização judicial prévia para qualquer transmissão desses dados a outras entidades, que apenas podem ser as forças e corpos de segurança e a *Dirección Adjunta de Vigilancia Aduanera*, em ambos os casos quando no desempenho de funções de polícia criminal, e o *Centro Nacional de Inteligencia*, no âmbito de investigações de segurança de pessoas ou entidades.

De acordo com as pesquisas realizadas, o disposto na LCD foi alvo de discussão na doutrina e na sociedade civil desde a sua aprovação. Em 2008 terá sido solicitado ao *Defensor del Pueblo* (Provedor de Justiça) que suscitasse junto do Tribunal Constitucional a questão da inconstitucionalidade da LCD, o que o *Defensor* não

[71] Diploma consolidado, na sua redação atual, retirado do portal oficial *BOE.ES*. Todas as referências relativas à legislação de Espanha devem considerar-se remetidas para o referido portal, salvo indicação expressa em contrário. Consultas efetuadas a 25/11/2022.
[72] Incluindo transferência e reencaminhamento de comunicações.
[73] Identidade Internacional de Assinante Móvel (IMSI) e Identidade Internacional do Equipamento Móvel (IMEI).

terá feito por entender que estava estabelecido um controlo judicial eficaz e, portanto, os direitos humanos em causa não estavam limitados[74].

A polémica em torno da LCD intensificou-se após 2014, com a decisão do TJUE de declarar inválida a Diretiva 2006/24/CE no processo *Digital Rights Ireland* [75]

Contudo, nos processos em que a questão foi suscitada, o *Tribunal Supremo*[76] recusou sempre a perda de validade da lei espanhola. Veja-se, por exemplo, o acórdão de 18 de abril de 2017 (processo STS 1594/2017, de 18 de abril), em que o *Tribunal Supremo* considerou que a decisão do TJUE não afetava a validade da lei espanhola, nomeadamente por esta prever no seu *artículo 6* que «'os dados conservados em conformidade com o disposto nesta lei só podem ser transmitidos para os fins nela previstos e autorização judicial prévia', o que não constituía uma garantia imposta pela Diretiva 2006/24 que é transposta pela *Ley 25/2007*, de forma que o legislador atribui a mesma proteção a direitos que não têm a mesma natureza e como tal idêntico nível de tutela, como são os consagrados no artigo 18.3 [da Constituição], ingerência no conteúdo de conversas telefónicas, e a transmissão de dados eletrónicos de tráfego ou associados».

Mais recentemente, o *Tribunal Supremo* reitera, no processo STS 1966/2020, que «os requisitos indicados pelo TJUE estão incluídos na nossa legislação interna, tanto a proteção do direito à intimidade como o princípio da proporcionalidade, e sujeitos à autorização de autoridade independente da administrativa, que é a judicial, e estão restringidos à investigação e repressão de crimes graves previstos no Código Penal e em leis especiais, de modo que em cada caso será o juiz de instrução correspondente a decidir a transmissão de dados de tráfego de comunicações eletrónicas, o que naturalmente implica que a decisão deve ser ajustada ao princípio da proporcionalidade estabelecido expressamente na nossa lei processual penal (…), o que em princípio não parece incompatível com a exigência de uma regulamentação nacional que não permita a conservação generalizada e indiferenciada de todos os dados de tráfego e de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica. Consequentemente (…) não restam dúvidas quanto à observância da proporcionalidade da ingerência em matéria de comunicações telefónicas, visto estarem previstas em lei e serem determinadas por um órgão judicial, que se encontra fora da estrutura de investigação criminal, em decisão fundamentada que analisa as necessidades da sua adoção para a investigação criminal, a gravidade dos factos e os direitos fundamentais em causa».

Por outro lado, no âmbito do processo C-207/16 - *Ministerio Fiscal* (2018), o TJUE, embora não se pronuncie sobre a aplicabilidade ou vigência da LCD espanhola (não era, de resto, essa a questão suscitada, mas sim a de saber se os dados conservados só podem ser transmitidos no âmbito da prática de crimes graves), acaba por considerar que «deve partir-se da premissa segundo a qual os dados em causa no processo principal

[74] De acordo com notícia publicada pela *Asociacíon de Internautas*, organização sem fins lucrativos de defesa dos direitos dos utilizadores de telefone e internet.
[75] Sobre a evolução desta questão em Espanha veja-se o artigo « *La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión*», publicado na *Revista de Internet, Derecho y Política* da *Universitat Oberta de Catalunya*, de outubro de 2021.
[76] Tribunal de última instância em todas as ordens jurisdicionais, com exceção do previsto para as garantias constitucionais, que é competência do Tribunal Constitucional.

foram conservados em conformidade com a legislação nacional, no respeito dos requisitos estabelecidos no artigo 15.º, n.º 1, da Diretiva 2002/58 (…)»[77].

Na doutrina espanhola, não parece haver consenso sobre a questão. Por um lado, os que defendem que o juiz nacional, ao avaliar a validade das provas tem de o fazer também à luz do direito europeu, o que significa que provas obtidas através da recolha massiva de dados ao abrigo da LCD não são admissíveis, na medida em que violam direitos fundamentais, e por outro os que entendem que a não admissão de dados assim recolhido põe em risco a investigação de múltiplos crimes informáticos.[78]

Refira-se finalmente que em junho de 2022 foi aprovada pelo Parlamento espanhol, uma nova *Ley General de Telecomunicaciones*, que mantém (no *artículo 61*) a remissão para a LCD constante da *Ley General de Telecomunicaciones* anterior (*artículo 42)*, determinando que a conservação e transmissão dos dados gerados ou tratados no âmbito da prestação de serviços de comunicações eletrónicas ou de redes públicas de comunicação aos agentes competentes por via da correspondente autorização judicial com vista à deteção, investigação e julgamento de crimes graves[79] rege-se pelo disposto na LCD. Esta norma está inserida no capítulo dedicado à «salvaguarda de direitos fundamentais, sigilo das comunicações e proteção de dados pessoais e direitos públicos e obrigações relativas a redes e serviços de comunicação eletrónica». No preâmbulo desta lei explica-se que a mesma está «em consonância com a Carta dos Direitos Digitais apresentada pelo Governo em 14 de julho de 2021, como marco para a produção normativa e políticas públicas que garantam a proteção dos direitos individuais e coletivos perante as novas situações e circunstâncias geradas no ambiente digital».

[77] Recorde-se que aquele artigo da Diretiva 2002/58/CE (conhecida como Diretiva *e-Privacy*) prevê a possibilidade de os Estados-Membros adotarem medidas legislativas para restringir o âmbito dos direitos e obrigações previstos na mesma diretiva «sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas (…) Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário (…)».

[78] Como refere LÓPEZ-POZAS, Fernando L. Ibáñez, em *De las masivas interceptaciones de datos a las masivas vulneraciones de derechos fundamentales: la respuesta del Tribunal de Justicia de la Union Europea, in Diario La Ley*, n.º 10033, *Sección Tribuna*, de 21 de março de 2022, Wolters Kluwer, consultado em 10/11/2022.

[79] São delitos graves os punidos com penas graves, que, nos termos do *artículo 33* do Código Penal espanhol, são as seguintes: a prisão permanente reavaliável; prisão por mais de 5 anos; inabilitação absoluta; inabilitação por mais de 5 anos; suspensão de emprego ou cargo público por mais de 5 anos; inibição de condução de veículos automotores e ciclomotores por mais de 8 anos; inibição do direito de uso e porte de armas por mais de 8 anos; interdição de residir ou frequentar determinados locais por mais de 5 anos; proibição de se aproximar da vítima, seus familiares ou outras pessoas por mais de 5 anos; proibição de contactar com a vítima, seus familiares ou outras pessoas por mais de 5 anos; inibição de exercício de responsabilidades parentais.

FINLÂNDIA[80]

A transposição para o direito nacional finlandês da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, 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, concretizou-se através da aprovação da Lei 343/2008[81], que alterava a Lei de Proteção de Dados de Comunicações Eletrónicas (516/2004). Este diploma veio a sofrer novas alterações na sequência da decisão do Tribunal de Justiça da UE de 2014, como se verá adiante.

Na sua redação após transposição da Diretiva 2006/24/CE, o diploma previa o seguinte.

A secção 8 deste diploma definia regras gerais de utilização, determinando que a aplicação deste capítulo, *i.e.* a retenção de metadados, apenas seria permitida na medida necessária para a prossecução da finalidade destas normas, não podendo afetar a confidencialidade das mensagens e a proteção da privacidade mais do que o estritamente necessário. Apenas é permitido divulgar informações de identificação às partes autorizadas a processar esses dados em situação relevante.

A secção 19 definia a obrigação das empresas de telecomunicações, e dos prestadores de serviço de valor acrescentado, de acautelar da segurança da informação no armazenamento dos dados necessários para cumprir estas obrigações, devendo identificar os funcionários que estariam autorizados a processar os dados armazenados, mantendo a obrigação de zelar pela segurança da informação dos assinantes e utilizadores perante terceiros que total ou parcialmente implementassem um serviço de internet, um serviço de comunicações, o armazenamento de dados ou serviços de valor acrescentado.

Na secção 31, determinava-se que a Autoridade Reguladora de Comunicações da Finlândia deveria preparar os regulamentos a serem emitidos com base nesta lei, devendo consultar e colaborar com o Ministério dos Transportes e Comunicações.

A secção 36 determinava que o direito de acesso à informação por outras autoridades para prevenir, descobrir ou investigar crimes, estava regulamentado na Lei da Polícia, Lei da Guarda de Fronteira (578/2005), sobre o tratamento de dados pessoais na Guarda de Fronteira na lei (579/2005), a Lei Aduaneira (1466/1994) e na Lei de Medidas Coercitivas.

Finalmente, determinava que as informações armazenadas com base na secção 14 desta lei só podiam ser obtidas de empresas de serviços por autoridades que, com base na lei, estivessem autorizadas a requerer e receber essas informações. Que deviam ser tomadas as medidas necessárias para implementar a lei mesmo antes da sua entrada em vigor, devendo as empresas de serviços começar a armazenar informações sobre serviços de e-mail e serviços de telefone pela internet, de acordo com esta lei, até 15 de março 2009.

[80] A informação contida neste resumo tem origem na resposta a um pedido realizado ao Parlamento finlandês, estando todas as ligações eletrónicas a remeter para as ligações indicadas nessa resposta, em língua finlandesa.
[81] Texto retirado do portal legislativo *FINLEX.FI*. Todas as referências legislativas relativas à Finlândia são feitas para este portal oficial, salvo indicação em contrário. Consultas efetuadas a 25/11/2025.

Em 2014, na sequência da decisão do Tribunal de Justiça da UE, operou-se uma reforma desta legislação, tendo a legislação anterior sido substituída pela presente Lei dos Serviços de Comunicações Eletrônicas (917/2014), cuja tradução oficial para inglês o parlamento finlandês refere infelizmente não refletir ainda as alterações operadas, especialmente ao capítulo 19[82], relativo às informações prestadas às autoridades e a obrigação de armazenar dados de transmissão. Estas alterações foram introduzidas com o apoio da Comissão de Direito Constitucional do Parlamento finlandês.

A Parte VI deste diploma aborda a questão da confidencialidade das comunicações e da proteção da privacidade, relevando para este tema o capítulo 19, constituído por três secções, 157 a 159. A secção 157 estabelece a obrigação de manter informações necessárias às autoridades pelos períodos de armazenamento definidos. No entanto, essas informações só podem ser usadas de acordo com a Lei de Medidas Coercitivas (806/2011) no capítulo 10, seção 6, subseção 2, para investigar e processar os suspeitos relativamente a esses crimes – utilização de um endereço ou terminal eletrónico na utilização do crime, punível com pela de pelo menos 2 anos. A obrigação de retenção aplica-se aos dados:

> 1) fornecidos pela empresa responsável pela conservação do serviço telefónico de uma rede de comunicações móveis ou de serviço SMS, incluindo chamadas, onde a conexão foi estabelecida, mas a chamada não foi atendida ou a chamada foi bloqueada devido a medidas de gestão de rede;
>
> 2) fornecidos pela empresa responsável pela conservação do serviço de telefone pela Internet, que é fornecido pela empresa de serviços aos clientes finais até uma chamada com base no protocolo de conexão com a internet [*Internet protocol-enabled service*];
>
> 3) fornecidos pela empresa fornecedora de serviço de ligação à internet obrigada à conservação dos dados.

A obrigação de conservação de dados aplica-se ao nome e endereço do assinante ou utilizador registado, ao identificador de assinatura e informações - que podem ser usados para identificar o serviço de comunicação do utilizador -, o tipo de comunicação, o destinatário da comunicação, bem como as horas e duração dessa comunicação, incluindo o encaminhamento de chamadas. Relativamente ao primeiro ponto, a obrigação de retenção aplica-se às informações que podem ser utilizadas para identificar o dispositivo utilizado para a comunicação, a localização desse dispositivo e da conexão utilizada no início da comunicação. No serviço referido no n.º 3, a obrigação de armazenamento aplica-se ao nome e endereço do assinante e utilizador registado, ao identificador de conexão e ao endereço de instalação, bem como a informações que podem ser usadas para identificar o serviço de comunicação do utilizador, o dispositivo utilizado para estabelecer a comunicação e o horário e duração do uso do serviço. A informação a conservar deve ser limitada apenas ao necessário para a implementação técnica dos registos pretendidos. Os dados de serviço referidos no ponto 1 devem ser mantidos por 12 meses, os referidos no ponto 3 por 9 meses, e os referidos no ponto 2 por 6 meses. O período de retenção de dados começa no momento do evento de comunicação. A obrigação de retenção não se aplica ao conteúdo da mensagem e os metadados não podem tem origem na informação de

[82] Pág. 47 no original, página 61 na versão desatualizada em inglês.

proxy da navegação de sítios de internet. Um requisito para a obrigação de conservação é que a informação esteja disponível e seja gerada ou processada em conexão com serviços de comunicações publicamente disponíveis ao abrigo desta lei ou da Lei de Dados Pessoais (523/1999). A Autoridade Reguladora de Comunicações Finlandesa definiria num regulamento os detalhes técnicos sobre os dados a serem conservados com base nesta obrigação legal.

A secção 158 define as obrigações e procedimentos para o processamento dos dados a serem mantidos para eventual utilização pelas autoridades. Nesta secção está previsto que, antes de implementar a obrigação de retenção, um operador discutirá com o Ministério do Interior as necessidades das autoridades em matéria de retenção de dados. A implementação deve seguir os princípios de custo-benefício, devendo ser consideradas as necessidades comerciais do operador sob a obrigação de retenção, as características técnicas do sistema e as necessidades da autoridade que paga os custos da retenção. Os dados devem ser retidos de forma a evitar que os mesmos sejam repetidos em várias localizações. Refere também que a retenção de dados deverá ser planeada de tal forma que a mesma informação não seja armazenada por várias empresas e que o Ministério do Interior tem o direito de contratar, a um fornecedor externo ao fornecedor de serviços, um sistema para a transferência destes dados. Por outro lado, a empresa tem o direito de incluir no sistema informático os dados que ainda estejam em processamento no âmbito da sua atividade empresarial.

Assim, podemos concluir que, desde a reforma, a retenção de dados na Finlândia foi limitada a certos serviços de comunicações eletrónicas, e a Lei de Serviços de Comunicações Eletrónicas contém disposições detalhadas sobre os tipos de dados a serem retidos para cada serviço. Na sequência da avaliação da necessidade realizada no âmbito da reforma, alguns serviços foram excluídos (deixou então de ser exigida a retenção de informações sobre os serviços telefónicos de rede fixa, serviços de correio eletrónico, serviços adicionais, serviços EMS[83] e serviços multimédia). Na avaliação da necessidade, os períodos de retenção de dados também foram reduzidos e escalonados por tipo de serviço. Atualmente, os períodos de retenção variam entre 6 e 12 meses. A obrigação de retenção é imposta a certas operadoras de telecomunicações com base na sua quota de mercado e cobertura geográfica.

[83] Informação fornecida pelo Parlamento finlandês, ficando a dúvida sobre se a referência é a *Element Management System* ou a *Emergency Medical Services*.

FRANÇA

Pela pesquisa efetuada no portal oficial *legifrance.gouv.fr*[84], a transposição completa da Diretiva n.º 2006/24/CE para o direito nacional ocorreu pela aprovação e publicação do *Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques*.

Este ato jurídico, na redação original, é composto por cinco artigos, sendo que o artigo 1 confere um novo conteúdo aos artigos R10-12, R10-13 e R10-14 do *Code des postes et des communications électroniques*. Em particular o artigo R10-13 prescreve que:

I. Em aplicação do n.º II do artigo L34-1[85]-[86], os operadores de comunicações eletrónicas retêm, para efeitos de investigação, verificação e de acusação de infrações penais:
   a) As informações que permitam identificar o utilizador;
   b) Os dados relacionados com os equipamentos terminais de comunicação utilizados;
   c) As caraterísticas técnicas, bem como a data, o horário e a duração de cada comunicação;
   d) Os elementos relativos a serviços adicionais solicitados ou utilizados e os seus prestadores;
   e) As informações que permitam identificar o destinatário ou destinatários da comunicação.
II. Para as atividades de telefone, os operadores guardam os dados mencionados no n.º I e, além disso, os que possibilitam identificar a origem e a localização da comunicação.
III. O período de retenção dos dados identificados neste artigo é de um ano a contar do dia do registo.
IV. Os custos adicionais identificáveis e específicos suportados pelos operadores exigidos pelas autoridades judiciárias pela prestação dos dados enumerados no presente artigo são compensados segundo as modalidades previstas no artigo R213-1[87] do *Code de procédure pénale*.

O artigo 2 renumerou o artigo R11 do mesmo código para R10-11.

Por sua vez, o artigo 3 inseriu o ponto 23º ao artigo R92 do *Code de procédure pénale*, e criou a seção 11 no Capítulo II do Título X do Livro V, com o título «*Des frais des opérateurs de communications électroniques*» (Os custos dos operadores de comunicações eletrónicas), a qual compreende o artigo R213-1.

O artigo 4 define o âmbito de aplicação das disposições nos territórios ultramarinos do país, *Mayotte*, *Nouvelle-Calédonie*, Polinésia francesa, e nas ilhas *Wallis* e *Futuna*.

---

[84] Resultados acessíveis em https://www.legifrance.gouv.fr/search/all?tab_selection=all&searchField=ALL&query=Directive+2006%2F24%2FCE&searchType=ALL&typePagination=DEFAULT&pageSize=25&page=1&tab_selection=all#all
Todas as ligações eletrónicas a referências legislativas referentes a França são feitas para o referido portal. Consultados no dia 25/11/2022.

[85] Redação em vigor durante o período entre o dia 24/01/2006 até ao dia 14/06/2009.

[86] Norma que declarava que, para efeitos de investigação, verificação e de acusação de infrações penais, com o único objetivo de disponibilizar, conforme o necessário, as informações às autoridades judiciais, as operações de eliminação ou tornar anónimas determinadas categorias de dados podem ser adiadas por um período máximo de um ano.

[87] Artigo criado pelo artigo 3 do *Décret n° 2006-358 du 24 mars 2006*.

Embora, o Tribunal de Justiça da União Europeia tenha proferido a sua decisão, pelo seu acórdão, de 8 de abril de 2014[88], de invalidade supracitada diretiva como inválida, e consequentemente tal diploma tenha deixado vigorar no ordenamento jurídico da União Europeia, o *Décret n.º 358 du 24 mars 2006*, como se pode constatar pela sua redação atual[89], continua a vigorar na ordem jurídica francesa.

Após a decisão de invalidade da Diretiva 2006/24/CE pelo Tribunal de Justiça da União Europeia, o *Conseil d`État*[90], em concreto a *Assemblée*, proferiu uma decisão, pelo acórdão de 21/04/2021, n.º 393099, invocando, nos fundamentos apresentados os acórdãos do Tribunal de Justiça da União Europeia, de 8 de abril de 2014 - *Digital Rights Ireland Ltd* (C-293/12 e C-594/12), de 21 de dezembro de 2016 - *ele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson* e outros (C-203/15 e C-698/15), de 6 de outubro de 2020 - *La Quadrature du net* e outros (C-511/18, C-512/18 e C520/18), e de 2 de março de 2021 - *H.K. / Prokuratuur* (C-746/18). No acórdão aqui em causa decidiu-se que:

- Pelo artigo 1er as decisões do Primeiro-Ministro que recusam a revogação do artigo R10-13[91] do *Code des postes et des communications électroniques* e do *Décret du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne*[92] são anuladas, na medida em que estas normas, por um lado, não limitam as finalidades da obrigação generalizada e indiferenciada de conservação de dados de tráfego e de dados de localização que não sejam dados de identidade civil, dados de contacto e de pagamento, dados contratuais e de conta e endereços IP para a salvaguarda da segurança nacional e, em segundo lugar, não prejam uma revisão periódica da existência de uma ameaça grave, real e presente ou previsível à segurança nacional;
- Pelo artigo 2 é fixado o prazo de seis meses a contar desta decisão para o Primeiro-Ministro revogar estas disposições; e
- Pelo artigo 3, o *Conseil d'Etat* expressa que os *Décrets n.os 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement*, *autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure*[93] (redação original) e *2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement*[94] (redação original) são anulados apenas na medida em que permitem a aplicação das disposições dos artigos L851-1, L851-2, L851-4 e do ponto IV do artigo L851-3 do *Code de la sécurité intérieure*[95] sem um controlo prévio por uma autoridade administrativa independente dotada de um poder de emitir parecer favorável ou por um tribunal, fora dos casos de emergência devidamente justificados.

[88] O acórdão encontra-se acessível em https://curia.europa.eu/juris/document/document.jsf?mode=lst&pageIndex=0&docid=150642&part=1&doclang=PT&text=&dir=&occ=first&cid=252522, consultado no dia 25/11/2022.
[89] Consultada no dia 17/11/2022.
[90] Portal oficial.
[91] Na redação vigente entre o dia 1/04/2012 a 21/10/2021.
[92] Texto consolidado em vigor até 20/10/2021, consultado no dia 25/11/2022.
[93] Consultada no dia 25/11/2022.
[94] Consultada no dia 25/11/2022.
[95] Texto consolidado, consultado no dia 25/11/2022.

Por seu turno, a *Commission Nationale de l'Informatique et des Libertés (CNIL)*[96_97] emitiu várias deliberações onde indica a Diretiva 2002/58 (CE) do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações eletrónicas, alterada pelas Diretivas 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006 e 2009/136 (CE) do Parlamento Europeu e do Conselho, de 25 de novembro de 2009. Exemplo disso é a:

- A *Délibération n° 2014-474 du 27 novembre 2014 portant adoption d'une norme simplifiée relative aux traitements automatisés de données à caractère personnel mis en œuvre par les organismes publics et privés destinés à l'écoute et à l'enregistrement des conversations téléphoniques sur le lieu de travail*, cujo artigo 1 estabelece que só podem beneficiar do procedimento da declaração simplificada de conformidade à presente norma as operações de tratamento automatizado utilizadas pelos organismos públicos e privados relacionadas com a escuta e ao registo pontual das conversas telefónicas no local de trabalho que reúnam as condições definidas nos artigos seguintes desta deliberação. Mais se refere na referida *Délibération* que se excluem do seu âmbito:

    - O tratamento realizado pelos organismos, cujas missões consistam na recolha de dados sensíveis na aceção do artigo 8 da *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*[98] ;
    - As gravações audiovisuais;
    - As escutas e as gravações que se encontrem ligadas com os dados provenientes de uma captura do écran do computador de um funcionário;
    - O registo permanente ou sistemático das chamadas no local de trabalho, incluindo para efeitos de prova.

Igualmente exemplo é a:

- *Délibération SAN-2021-024 du 31 décembre 2021*, a qual também alude à competência material e territorial enquanto entidade nacional de fiscalização quanto à observância das disposições insertas no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados) e na *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, através da qual decide impor uma multa administrativa à empresa *Facebook Ireland Limited*, dada a violação do regime previsto no artigo 82[99] da *Loi n° 78-17 du 6 janvier 1978.*

---

[96] Sítio da *Internet* disponível em *https://www.cnil.fr*, consultado no dia 25/11/2022.

[97] Esta autoridade administrativa independente corresponde, de acordo com o artigo 8 da *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (texto consolidado, consultado no dia 25/11/2022) à entidade de controlo nacional, no sentido e para a aplicação do Regulamento (UE) 2016/679 do Parlamento Europeu 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).
As regras do seu funcionamento encontram-se insertas no *Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* (texto consolidado, consultado no dia 25/11/2022), e no seu *Règlement intérieur* (Regimento interno).

[98] Texto consolidado, consultado no dia 25/11/2022.

[99] Norma que estabelece que, todo o assinante ou utilizador de um serviço de comunicações eletrónicas deve ser informado de forma clara e completa, a menos que tenha sido previamente informado pelo responsável pelo tratamento ou seu representante:
1º Da finalidade de toda ação destinada a ceder, por transmissão eletrónica, as informações já armazenadas no seu equipamento terminal de comunicações eletrónicas, ou de registo de dados neste equipamento;

Noutros atos, esta entidade administrativa independente, faz igualmente referência à decisão de invalidade da Diretivas 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006 proferida no acórdão do Tribunal de Justiça da União Europeia de 8 de abril de 2014:

- ✓ *Délibération n° 2014-484 du 4 décembre 2014 portant avis sur un projet de décret relatif à l'accès administratif aux données de connexion et portant application de l'article L. 246-4 du code de la sécurité intérieure*;
- ✓ *Délibération n° 2015-455 du 17 décembre 2015 portant avis sur un projet de décret en Conseil d'État relatif aux techniques de recueil de renseignement.*

2.º Dos meios de que dispõe para se opor a este facto.
Tal acesso ou registo só pode ter lugar na condição de o assinante ou utilizador ter expressado, depois de receber esta informação, o seu consentimento que pode resultar de parâmetros apropriados do seu dispositivo de conexão ou de todo outro dispositivo colocado sob o seu controlo.
Estas disposições não são aplicáveis se o acesso às informações guardadas ou o seu registo no equipamento terminal do utilizador.
1º Seja, para a finalidade exclusiva de permitir ou facilitar a comunicação por via eletrónica;
2º Seja, estritamente necessário para a prestação de um serviço de comunicação *online*, a pedido expresso do utilizador.
Redação consolidada, consultada no dia 17/11/2022.

IRLANDA

A *Communications (Retention of Data) Act 2011 (Revised)*[100] (de ora em diante designado apenas por *Act 2011*) procedeu à transposição, para o ordenamento jurídico irlandês, da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006.

O âmbito objetivo do referido *Act 2011* vem estabelecido no *Schedule 2* do diploma e equivale, no geral, ao que se prevê na Diretiva, a saber:

i) Comunicações telefónicas nas redes fixa e móvel

a) Dados necessários para encontrar e identificar a fonte de uma comunicação:
   1) o número de telefone de origem;
   2) o nome e endereço do assinante ou do utilizador registado.

b) Dados necessários para encontrar e identificar o destino de uma comunicação:
   1) o(s) número(s) marcados (o número ou números de telefone de destino) 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;
   2) o nome e o endereço do assinante, ou do utilizador registado.

c) Dados necessários para identificar a data, a hora e a duração de uma comunicação.

d) Dados necessários para identificar o tipo de comunicação: o serviço telefónico utilizado.

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores ou aquilo que se considera ser o seu equipamento:
   1) os números de telefone de origem e de destino,
   2) a Identidade Internacional de Assinante Móvel («*International Mobile Subscriber Identity*», ou IMSI) de quem telefona,
   3) a Identidade Internacional do Equipamento Móvel («*International Mobile Equipment Identity*», ou IMEI) de quem telefona,
   4) 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.

f) Dados necessários para identificar a localização do equipamento de comunicação móvel:
   1) o identificador da célula no início da comunicação;
   2) 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.

ii) Acesso à internet, ao correio eletrónico através da internet e às comunicações telefónicas através da internet

a) Dados necessários para encontrar e identificar a fonte de uma comunicação:
   1) o(s) código(s) de identificação atribuído(s) ao utilizador;

[100] Texto consolidado até 25 de maio de 2018, retirado do portal legislativo *LAWREFORM.IE*. Consultas efetuadas a 25/11/2022.

2) o código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública;
3) 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.

b) Dados necessários para encontrar e identificar o destino de uma comunicação:
1) o(s) número(s) marcados (o número ou números de telefone de destino) 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;
2) o nome e o endereço do assinante, ou do utilizador registado;

c) Dados necessários para identificar a data, a hora e a duração de uma comunicação:
1) 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;
2) a data e a hora do início e do fim da ligação ao serviço de correio eletrónico através da internet ou de comunicações telefónicas através da internet, com base em determinado fuso horário.

d) Dados necessários para identificar o tipo de comunicação: o serviço internet utilizado.

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento:
1) o número de telefone que solicita o acesso por linha telefónica;
2) a linha de assinante digital («*digital subscriber line*», ou DSL), ou qualquer outro identificador terminal do autor da comunicação.

Pode ser solicitado, de acordo com a *section* 6, a um fornecedor de serviço público de comunicações eletrónicas ou de uma rede de comunicações pública, a divulgação de dados, para fins de:

1º. Prevenção, identificação, investigação ou acusação, relacionados com uma infração grave, por um membro da *Garda Síochána*[101][102] que exerça um cargo não inferior ao de superintendente-chefe;
2º. Salvaguarda da segurança do Estado, por um membro da *Garda Síochána* que exerça um cargo não inferior ao de superintendente-chefe ou por um agente da Força de Defesa Permanente que exerça cargo de coronel ou superior;
3º. Salvaguarda da vida humana, por um membro da *Garda Síochána* que exerça um cargo não inferior ao de superintendente-chefe;
4º. Prevenção, identificação, investigação ou acusação, relacionados com infrações fiscais, por um agente da Autoridade Tributária que exerça o cargo de agente principal ou superior;

[101] Portal oficial.
[102] A *Garda Siochána* corresponde à força policial nacional civil da República da Irlanda, com atribuições de polícia judiciária e polícia preventiva uniformizada.

5º. Prevenção, identificação, investigação ou acusação relacionados com infrações no âmbito do direito da concorrência, por um membro da Comissão de Proteção do Consumidor e da Concorrência.

Quanto ao período de conservação, o *Act 2011* prevê o prazo de um ano, no caso de comunicações telefónicas nas redes fixa e móvel, ou de dois anos, no caso de dados gerados através de acessos à internet, correio eletrónico ou outras comunicações telefónicas através da internet (*section 3*).

O *Communications (Retention of Data) Act 2022*[103] veio alterar o *Act de 2011,* no sentido de garantir a conformidade do diploma com as decisões do Tribunal de Justiça da União Europeia, no que se refere à conservação geral e indiscriminada dos dados resultantes de comunicações que tenha por fundamento a segurança nacional e o cumprimento da lei.

Em geral, o *Communications (Retention of Data) Act 2022* atualizou as normas do *Act 2011*, tendo introduzido ainda dois novos tipos de ordens legais, a ordem de conservação e a ordem de produção, os quais possibilitam a conservação e a produção de determinadas categorias de dados resultantes de comunicações ocorridas em certas circunstâncias, desde que estas tenham sido aprovadas judicialmente.

O diploma de 2022 alarga o elenco de entidades que podem ter acesso aos dados conservados, em concreto, permitindo o acesso a membros da *Garda Síochána* que exerçam o cargo de superintendente ou superior, ou de inspetor ou superior[104], a membros da Força de Segurança que exerçam o cargo de tenente-coronel ou superior, ou o de comandante ou superior[105]. Por seu lado, no caso dos membros da Comissão de Proteção do Consumidor e da Concorrência, passou a exigir-se que estes exercessem, no mínimo, o cargo de agente principal.

Alarga igualmente o catálogo de fundamentos que podem justificar o acesso a dados pelos membros da *Garda Síochána*, passando a abranger as situações, não só de risco para a vida, mas também para a segurança pessoal de pessoa, bem como a determinação da localização de pessoa desaparecida.

No caso do acesso por agente da Força de Defesa Permanente, especifica-se que a segurança de Estado passível de justificar tal acesso se relaciona, não só com dados necessários à salvaguarda da segurança do Estado, mas também com dados que se refiram a pessoas que representem um perigo real ou potencial à segurança do Estado. O mesmo raciocínio aplica-se aos agentes da Autoridade Tributária e da Comissão de Proteção do Consumidor e da Concorrência, no que se refere, respetivamente, às infrações fiscais e ao direito da concorrência.

As secções 6B, 6D e 6E do diploma preveem ainda normas especiais aplicáveis aos pedidos urgentes.

O diploma de 2022 aditou a *Section 7* ao *Act 2011*.

Assim, e como se referiu supra, a *Section 7A* prevê a figura da «ordem de conservação». Esta ordem pode ser solicitada por um membro da *Garda Síochána*, das Forças de Defesa, da Autoridade Tributária ou da

[103] Texto consolidado, retirado do portal legislativo *IRISHSTATUTEBOOK.IE*. Consultas efetuadas a 25/11/2022
[104] No caso de os requerentes exercerem o cargo de inspetor ou cargos superiores que sejam hierarquicamente inferiores ao cargo de superintendente, o acesso à informação deve ser solicitado a um juiz competente.
[105] No caso de os requerentes exercerem o cargo de comandante ou cargos superiores que sejam hierarquicamente inferiores ao cargo de tenente-coronel, o acesso à informação deve ser solicitado a um juiz competente.

Comissão de Proteção do Consumidor e da Concorrência, sempre que estejam em causa dados previstos no *Schedule 2*. Pressuposto é igualmente que tenha sido autorizada judicialmente e que o recurso à ordem de conservação tenha suporte legal, ou seja, que se justifique, nomeadamente, como forma de resposta à prática de infrações graves, por razões de segurança nacional ou de salvaguarda da vida humana. Neste caso, os fornecedores de serviços de comunicação ficam obrigados a conservar os dados pelo tempo que seja determinado.

A *Section 7B* prevê, por seu lado, a figura da «ordem de produção», nos termos da qual um membro da *Garda Síochána*, das Forças de Defesa, da Autoridade Tributária, ou da Comissão de Proteção do Consumidor e da Concorrência poderá solicitar a produção de dados previstos no *Schedule 2*, nas circunstâncias referidas para a *Section 7A*.[106]

O *Irish Council for Civil Liberties* (ICCL) emitiu, a 5 de julho de 2022, um comunicado[107] sobre a ainda então *Communications (Retention of Data) (Amendment) Bill 2022*[108], cuja redação corresponde, na íntegra, ao que veio a ser aprovado e se tornou no *Communications (Retention of Data) Act 2022*. Naquele comunicado, o ICCL defendeu que o novo diploma apenas abarca parcialmente as conclusões do Tribunal de Justiça da União Europeia, identificando as seguintes fragilidades:

1. A possibilidade de renovação do prazo de um ano de conservação dos dados prevista na *Section 4*, a qual tem por efeito a conservação por tempo indeterminado.
2. A não definição do conceito de segurança nacional.
3. A não previsão de mecanismos que permitam a proteção das fontes jornalísticas.
4. A não previsão de um mecanismo de supervisão.
5. A não previsão de uma solução judicial e de outros procedimentos no caso de violação de direitos, incluindo direitos fundamentais, cometidos no âmbito do cumprimento do disposto no diploma.
6. O diploma estabelece a possibilidade de validação retroativa de conservação ilegal de dados (*Section* 9).
7. O diploma interfere com a independência dos tribunais e da Comissão de Proteção de Dados, ao prever a continuidade da conservação de dados ilegalmente retidos (*Section* 9), relativamente aos processos que estejam pendentes.

[106] Para mais informações sobre este tema, consultar o *Explanatory Memorandum* preparado pelas *Houses of the Oireachtas*.
[107] Disponível no portal do *Irish Council for Civil Liberties*.
[108] Texto disponível no portal da *Houses of the Oireachtas*. Consultado a 25/11/2022.

ITÁLIA

O *Decreto Legislativo 30 maggio 2008, n. 109*[109] procedeu à transposição da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação dos 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.

Especificamente, enquanto o artigo 1.º define o conteúdo de certas expressões recorrentes no diploma, o artigo 2.º altera o artigo 132.º do chamado *Código da Proteção de Dados Pessoais* (*Decreto Legislativo 30 giugno 2003, n.196*, *recante il Codice in materia di protezione dei dati personali*), com especial referência ao período de retenção de dados relativos ao tráfego telefónico e telemático por operadores telefónicos e de comunicações eletrónicas.

O artigo 3.º identifica por sua vez as categorias de dados que devem ser conservados por estes operadores, e o artigo 4.º confia ao «*Garante para a proteção de dados pessoais*»[110] a tarefa de assegurar o cumprimento das disposições sobre segurança e medidas organizacionais para o correto armazenamento dos dados.

O artigo 5.º, por outro lado, estabelece as sanções administrativas relativas à violação das disposições sobre a conservação de dados telefónicos e telemáticos de tráfego, enquanto o artigo 6.º prevê certas disposições transitórias e finais.

Na ordem jurídica italiana, o artigo 132º do *Decreto Legislativo 30 giugno 2003, n.196*, prevê que os dados relativos ao tráfego telefónico devem ser conservados pelo fornecedor durante vinte e quatro meses a contar da data da comunicação, para efeitos de investigação e repressão de crimes, enquanto que, para os mesmos efeitos, os dados relativos ao tráfego telemático, excluindo em qualquer caso o conteúdo das comunicações, devem ser conservados pelo fornecedor durante doze meses a contar da data da comunicação.

Dentro destes prazos, os dados serão solicitados ao fornecedor por decreto fundamentado do Ministério Público, também a pedido do advogado de defesa do arguido, da pessoa sob investigação, da parte lesada e dos outros particulares. O advogado de defesa do arguido ou da pessoa sob investigação pode solicitar, diretamente ao fornecedor, os dados relativos aos serviços em nome do seu cliente, na forma estabelecida no artigo 391º-*quater* do Código de Processo Penal, nas condições estabelecidas no artigo 8º, n.º 2, alínea f), para o tráfego de entrada.

Deixando de lado as disposições relativas à realização de investigações preventivas previstas no artigo 226.º do '*Decreto Legislativo 28 luglio 1989, n. 271*', ou seja, para efeitos de investigação e repressão de delitos específicos, o "*Código de Proteção de Dados*" prevê, nos termos do artigo 132º-*bis*, que os prestadores devem estabelecer procedimentos internos para responder aos pedidos feitos em conformidade com as disposições que regem as formas de acesso aos dados pessoais dos utilizadores.

[109] Texto retirado do portal legislativo italiano *NORMATTIVA.IT*. Todas as referências legislativas referentes a Itália são feitas para este portal oficial, salvo indicação em contrário. Consultas efetuadas a 25/11/2022.
[110] O *Garante per la protezione dei dati personali* é uma entidade equiparável à Comissão Nacional para a Proteção de Dados.

Por uma questão de exaustividade, deve salientar-se que o não cumprimento da obrigação de conservação de dados implica a aplicação de uma sanção administrativa contra o prestador de serviços. O artigo 162-*bis* (sanções por retenção de dados de tráfego) do Código da Proteção de Dados prevê o seguinte: «a menos que o ato constitua uma infração e sob reserva do disposto no nº 2 do artigo 5º do decreto legislativo que transpõe a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, em caso de violação do disposto nos nºs 1 e 1-A do artigo 132º, é aplicável uma coima administrativa que varia entre 10 000 € e 50 000 €».

Por outro lado, o supracitado artigo 5.º, n.º 2, do prevê: «a menos que o ato constitua uma infração, a omissão ou o armazenamento incompleto de dados nos termos do artigo 132, n.º 1 e 1-*bis*, do Código, será punido com uma sanção administrativa pecuniária que varia entre 10 000 € e 50 000 €, que pode ser aumentada até três vezes com base nas condições económicas dos responsáveis pela violação. No caso da atribuição de um endereço IP que não permita a identificação inequívoca do utilizador ou assinante, aplica-se a sanção administrativa pecuniária que varia entre 5 000 € e 50 000 €, que pode ser aumentada até três vezes devido às condições económicas dos responsáveis pela violação. As violações são contestadas e as sanções são aplicadas pelo *Ministério do Desenvolvimento Económico*.

Na sequência da decisão do Tribunal de Justiça, de 8 de abril de 2014, relativa aos processos n.os C-293/12 e C-594/12, etal como em Portugal, têm tido lugar, em Itália, processos judiciais que contestam a admissibilidade de metadados. No entanto, os tribunais italianos têm vindo a considerar que as leis nacionais relativas à conservação de dados não são contrárias às constituições nacionais.

Dois casos recentes apresentados perante o Tribunal de Cassação analisaram se o atual quadro jurídico italiano para a retenção de dados, incluindo o **período de retenção de 72 meses** para certos crimes graves (massacre, atos de guerra civil, crimes do tipo mafioso, homicídio, roubo agravado, extorsão agravada, rapto para resgate, terrorismo, pornografia infantil, participação em grupos armados), é compatível com os princípios e regras da UE, afirmando que estes princípios dizem respeito ao acesso a metadados e não às regras sobre retenção.

Num processo em 2019, o autor argumentou que a lei italiana sobre a conservação de dados não era compatível com a CDFUE, tal como interpretada pela jurisprudência do TJUE. Argumentou que a lei italiana não preencheria o teste da proporcionalidade, uma vez que prevê o acesso e a conservação de dados não constantes de qualquer tipo de crime; e o poder de autorizar o acesso aos dados é concedido ao Ministério Público em vez de um juiz ou outra autoridade independente. O Tribunal de Cassação declarou que a legislação italiana é compatível com a legislação da UE, afirmando que: «a jurisprudência do TJUE diz respeito apenas aos Estados-Membros que não dispõem de legislação sobre conservação e acesso aos dados, sendo que a Itália adotou regras específicas sobre conservação de dados; e a legislação italiana é proporcional porque os prazos são adequados e o Ministério Público é um órgão suficientemente independente». - *Acórdãos do Tribunal de Cassação n.os 36380/2019 e 5741/2020.* [111]

[111] Texto integral disponível no portal *ITALGIURE.GIUSTIZIA.IT*.

Não foram identificados outros processos judiciais ou alterações legais, embora a autoridade de proteção de dados italiana tenha adotado uma posição crítica em relação ao alargamento do período de conservação para 72 meses em vários pareceres emitidos em 2018. Defende uma revisão da legislação nacional para a tornar conforme com a jurisprudência do TJUE.

A título de exemplo, vejam-se os seguintes pareceres:

1. *Parere sullo schema di decreto legislativo recante Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio - 22 febbraio 2018*[112] (Parecer sobre o projeto de decreto legislativo de aplicação da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho - 22 de fevereiro de 2018)
2. *Parere sullo schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 - 22 maggio 2018*[113] (Parecer sobre o projeto de decreto legislativo que contém disposições para a adaptação da legislação nacional às disposições do Regulamento (UE) 2016/679 - 22 de maio de 2018).
3. *Sicurezza dei dati di traffico telefonico e telematico - 17 gennaio 2008*[114] (Segurança dos dados de tráfego telefónico e telemático - 17 de janeiro de 2008)

Refira-se ainda que, em Itália, é concedido o acesso a metadados a advogados de defesa em processos penais. O artigo 132.º, n.º 3 do Código de Proteção de Dados confere à defesa o direito de solicitar o acesso a dados não relacionados com as contas pertencentes ao seu cliente, que seja suspeito ou arguido num processo penal, por um período de 24 meses.

O ordenamento jurídico italiano não prevê expressamente um papel para as autoridades policiais no acesso aos dados não constantes do conteúdo, uma vez que a polícia está «ao serviço» do Ministério Público. Contudo, com base em certas disposições da lei e práticas no terreno, é evidente que a polícia pode aceder aos dados para investigações e procedimentos criminais, mas apenas com a autorização e a pedido do Ministério Público. Para a investigação de certos crimes (crime organizado e terrorismo), os dirigentes máximos das autoridades (por exemplo, o Ministro dos Assuntos Internos, certas autoridades que apliquem a lei) podem solicitar o acesso a dados que não sejam de conteúdo, mas estes dados não podem ser utilizados em processos penais.

Como se disse supra, as entidades reguladoras de telecomunicações têm competência para sancionar os fornecedores de serviços de comunicações eletrónicas pelo não cumprimento das obrigações nacionais em matéria de conservação geral de dados. Apesar desta opção, as sanções continuam a ser um último recurso, principalmente devido ao cumprimento geral por parte dos fornecedores de serviços de comunicações eletrónicas.

Embora exista uma obrigação de retenção de dados em Itália, a autoridade reguladora de telecomunicações tem um papel mais de monitorização. A sua principal função é a manutenção do *Registro degli Operatori di*

[112] Texto disponível no portal oficial do *GARANTEPRIVACY*.
[113] [113] Texto disponível no portal oficial do *GARANTEPRIVACY*.
[114] [114] Texto disponível no portal oficial do *GARANTEPRIVACY*.

Comunicazione (ROC) [Registo de Operadores de Comunicação][115], que inclui todos os operadores de mercado que recebem dados pessoais. No entanto, o quadro legislativo também inclui sanções para os fornecedores que não cumpram as suas obrigações de apoio às autoridades, incluindo suspensão ou mesmo perda da sua licença e possíveis sanções penais.

Relativamente à retenção de dados, em Itália, foi introduzida uma distinção adicional em 2017, através da *Legge 20 novembre 2017, n. 167* – *«Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea»*; segundo a qual os metadados devem ser retidos durante 72 meses para serem acedidos em caso de terrorismo ou outros crimes graves (artigo 24.º do diploma, «*Períodos de retenção de dados do tráfego telefónico e telemático*»).

Na prática, porém, como os fornecedores de serviços em Itália não podem conhecer os tipos de dados criminais que podem ser solicitados no futuro, retêm todos os dados não relativos a conteúdos durante 72 meses, por defeito. Para crimes não graves, os pedidos de acesso devem ser feitos dentro dos prazos estabelecidos pela legislação nacional sobre retenção de dados. Os fornecedores podem também reter dados de tráfego, identificação e localização para fins internos (por exemplo, comerciais, de marketing, de faturação). Em Itália, o período máximo de retenção legal para fins internos é de seis meses.

Acresce que em Itália, a Autoridade de Proteção de Dados[116] publicou um catálogo que especifica os requisitos legais para os aspetos técnicos da gestão e segurança de dados (*Principi fondamentali del trattamento*).[117]

Os metadados retidos para fins de aplicação da lei devem ser retidos separadamente dos metadados retidos para outros fins técnicos/comerciais.

Sendo um país que requer autorização *ex-ante*, na Itália, o acesso aos metadados é controlado pelos procuradores públicos. A situação é semelhante: em todos os casos, o procurador público deve solicitar o acesso a dados não relacionados com o conteúdo, e outras autoridades só podem agir com a autorização e a pedido do procurador público.. A lei prevê ainda o direito do advogado a aceder aos metadados das linhas telefónicas/internet detidas pela pessoa investigada/arguido durante um período de 24 meses.

Refira-se ainda que o Regulamento Geral de Proteção de Dados, o RGPD, veio alterar o chamado Código de Proteção de Dados Pessoais.

O *Decreto Legislativo 10 agosto 2018, n. 101*, contém disposições para a adaptação da legislação nacional às disposições do RGPD

O RGPD aplica-se essencialmente em duas situações: 1) quando o tratamento de dados tem lugar no contexto das atividades de um titular ou responsável pelo tratamento localizado na União Europeia; 2) quando

[115] *Registro degli operatori di comunicazione - AGCOM*. (*Autorità per le Garanzie nelle Comunicazioni* -Autoridade de Garantia das Comunicações)
[116] *Compiti - Garante Privacy*
[117] Texto disponível no portal oficial do *GARANTEPRIVACY*.

o tratamento de dados de indivíduos localizados na União Europeia tem lugar por um responsável pelo tratamento ou processador que também não está estabelecido na União Europeia.

O âmbito de aplicação territorial parece, assim, ter sido esculpido de acordo com as razões que levaram o Tribunal a anular a Diretiva 2006/24/CE, tal como refletido no acórdão *Digital Rights Ireland*. Além disso, a transferência de dados para Estados terceiros deve também respeitar os princípios consagrados no artigo 8.º da Carta. O RGPD procede através de uma lista precisa de definições, atualizada de acordo com a noção de «comunicação» contida nas explicações do artigo 7.º da Carta. As noções de perfil, pseudonímia, dados genéticos e dados biométricos são então consagradas no artigo 4.º.

PAÍSES BAIXOS[118]

A transposição para o direito nacional holandês da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de Março de 2006, 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", foi iniciada pela apresentação pelo governo ao Parlamento, em 14 de setembro de 2007, de uma proposta para alterar a Lei de Telecomunicações e a Lei de Ofensas Económicas (EK 31.145, A[119]).

Essa proposta previa que os prestadores de redes públicas de telecomunicações e de serviços de telecomunicações (acesso à internet, correio eletrónico e (internet) telecomunicações) ficassem obrigados a reter os dados de tráfego e localização por um período de doze meses para efeitos de investigação e repressão de crimes graves. Não se tratava de preservar o conteúdo da comunicação, apenas os metadados. A proposta continha disposições sobre os dados a conservar, os períodos de conservação, a proteção e segurança dos dados conservados e a sua supervisão, proteção legal e sanções. Embora os custos de investimento e de funcionamento fossem suportados pelos prestadores, estes teriam direito ao reembolso dos custos administrativos e de pessoal decorrentes da recuperação dos dados retidos a pedido das autoridades competentes. A proposta do governo foi adotada pela Câmara dos Deputados em 22 de maio de 2008 e posteriormente pelo Senado em 7 de julho de 2009. Durante a discussão no Senado, que decorreu entre 6 e 7 de julho de 2009, oito moções foram apresentadas, tendo a nova lei sido aprovada, entrando em vigor a 1 de setembro de 2009.

Esta alteração legislativa à Lei de Telecomunicações aditou um artigo 13.2ª que determinava a conservação dos dados de tráfego e localização, assim como dos dados necessários para identificar o assinante ou utilizador das chamadas, incluindo as tentativas de chamada malsucedidas, quer as não atendidas, quer as sujeitas a medidas de gestão de rede. O artigo 13.4 era alterado no sentido de obrigar os prestadores de redes públicas de telecomunicações e de serviços de telecomunicações a fornecerem imediatamente a um pedido de informação relativo a um utilizador, ou ao tráfego de telecomunicações desse utilizador, que fosse solicitada no âmbito de uma investigação criminal conduzida nos termos dos artigos 126n, 126na, 126u ou 126ua do Código de Procedimento Penal, ou do artigo 28º da Lei dos Serviços de Inteligência e Segurança de 2002. A redação do art.º 13.5 obrigava também os referidos prestadores a providenciar informação relativa ao acesso não autorizado aos dados, a manter segredo relativamente a esta informação, e a tomar as medidas técnicas e organizativas apropriadas para proteger a informação de destruição, perda ou modificação, acesso, processamento ou cópia não autorizada. Para além de garantir que apenas as pessoas especialmente autorizadas teriam acesso à informação, os prestadores teriam que ser capazes de eliminar os dados após o término do período determinado.

[118] A informação contida neste resumo tem origem na resposta a um pedido realizado ao Parlamento holandês, estando todas as ligações eletrónicas a remeter para as ligações indicadas nessa resposta, em língua holandesa.
[119] Texto retirado do portal legislativo *EERSTEKAMER.NL*. Todas as referências legislativas relativas à Holanda são feitas para este portal oficial, salvo indicação em contrário. Consultas efetuadas a 25/11/2025.

No entanto, durante a referida discussão da proposta do governo no Senado em 2009, na sequência de um pedido nesse sentido por parte dos membros dessa câmara alta, o ministro anunciou que, por meio de emenda legislativa, a obrigação de retenção de dados da internet seria posteriormente reduzida para 6 meses. Tal veio a concretizar-se através de uma nova proposta de alteração à Lei das Telecomunicações (a 32.185), que foi aprovada por unanimidade pela Câmara dos Representantes em 21 de junho de 2011, sendo publicada a alteração à Lei de Telecomunicações a 15 de julho de 2011. Com a alteração imposta pelo art.º 1, o artigo 13.2 da Lei das Telecomunicações passou a determinar que os dados referidos no segundo parágrafo continuariam a ser conservados pelos prestadores por um período de doze meses para os dados referentes a comunicações telefónicas através de rede fixa ou móvel, mas esse período seria reduzido para os seis meses para os dados relativos ao acesso à Internet, correio eletrónico pela Internet e comunicação telefónica pela Internet, contados a partir da data da comunicação.

Consequentemente, à data da decisão do Tribunal de Justiça da UE relativa aos processos n.os C-293/12 e C-594/12, 8 de abril de 2014, as regras da referida Diretiva 2006/24/CE já tinham sido transpostas para o ordenamento jurídico holandês. Na sequência desta decisão da justiça europeia, um conjunto de associações de direitos humanos, de advogados criminais, de jornalistas e algumas empresas privadas de responsabilidade limitada iniciaram um processo judicial, contra o estado holandês, relativo ao incumprimento do direito fundamental à privacidade ao aprovar e aplicar a legislação anteriormente referida. A decisão do Tribunal de Haia (C/09/480009 / KG ZA 14/1575), de 11 de março de 2015, determinou a cessação de vigência da Lei de Retenção de Dados de Telecomunicações e condenou o Estado ao pagamento das custas do processo, das custas subsequentes e das custas judiciais incorridas pelo serviço da sentença.

Face à nulidade decretada naquela Diretiva, o governo elaborou uma nova proposta[120] de alteração da Lei das Telecomunicações e do Código de Processo Penal (*Telecommunicatiewet en het Wetboek van Strafvordering*). Nesta nova proposta, o governo argumentava que, como os suspeitos não apareciam imediatamente no caso de crimes graves, era necessário que a polícia e o Ministério Público armazenassem dados de internet e telefone do passado recente para investigação e acusação. Esta obrigação de retenção diria respeito apenas aos dados de tráfego, não ao conteúdo da conversa. Os períodos de retenção permaneceriam inalterados: 6 meses para dados de internet, 12 meses para dados de comunicação telefónica. O Ministério Público só teria acesso aos dados de trânsito retidos após autorização do juiz de instrução. Os provedores de serviços de telecomunicações também seriam obrigados a armazenar e processar seus dados dentro da União Europeia. Como resultado, entendiam que a supervisão da proteção de dados pessoais ficaria bem regulamentada.

Por exemplo, a alteração ao art.º 13.4 passava a especificar o tipo de informação sobre o utilizador que teria de ser fornecida: nome, endereço, código postal, local de residência, número e tipo de serviço. Ao contrário da proposta anterior, o artigo 2º desta proposta alterava vários artigos do Código de Procedimento Penal, começando pelo art.º 126n, aditando 3 novos números que determinavam que: o pedido de informação só poderia ser apresentado aos prestadores se justificado pela gravidade do crime e após prévia autorização

[120] Texto disponível no portal *TWEEDEKAMER.NL. Consultas efetuadas a 25/11/2022.*

escrita pelo juiz de instrução, a requerimento do Ministério Público; que em casos urgentes esse pedido podia ser apresentado oralmente pelo Ministério Público, com a obrigação de o apresentar por escrito num prazo de 3 dias. Este pedido incluiria obrigatoriamente: a indicação do crime e, se conhecido, o nome ou outra indicação do suspeito tão precisa quanto possível; os factos ou circunstâncias que demonstrassem estarem preenchidas as condições referidas legais; se conhecido, o nome ou outra indicação tão precisa quanto possível da pessoa sobre a qual os dados estão sendo reivindicados; os dados reivindicados; o período temporal abrangido pelo pedido.

Submetida à Câmara dos Representantes em 12 de setembro de 2016 (34.537[121]), em 6 de julho 2017 (TK 34.707, no. 31) foi incluída na lista de temas controversos da Câmara dos Representantes que, em 2 de fevereiro de 2021 (TK 35,718, no. 9), a declarou como controversa, tendo a Câmara dos Representantes cessado o escrutínio desta proposta sem que o processo legislativo tivesse sido concluído.

[121] Texto disponível no portal *TWEEDEKAMER.NL Consultas efetuadas a 25/11/2022.*

REINO UNIDO

A Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, 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, foi inicialmente transposta pelo Reino Unido através das *Data Retention (EC Directive) Regulations 2007*[122].

Contudo, este diploma transpôs apenas as normas da Diretiva que diziam respeito aos dados resultantes de comunicações de rede fixa ou de telefonia móvel, tendo o Reino Unido anunciado que iria adiar a aplicação da Diretiva no que se referia à conservação de dados resultantes de comunicações resultantes de acessos à internet, de comunicações telefónicas através da internet ou de correio eletrónico.

A transposição destes aspetos da Diretiva veio a ser concretizada através das *Data Retention (EC Directive) Regulations 2009* (de ora em diante designadas apenas por *Regulations 2009*) que revogaram o diploma de 2007.

As *Regulations 2009* impõem que os fornecedores de comunicações públicas que tenham sido notificados para tal (*Regulation 10*) conservem os dados abrangidos pela previsão do *Schedule* do diploma, o que equivale, no geral, ao que se prevê na Diretiva, mas com uma sistematização diferente. De facto, nas *Regulations 2009*, esta matéria vem dividida em três partes:

1º. Comunicações telefónicas na rede fixa:

i) Dados necessários para localizar e identificar a fonte de uma comunicação:

a) o número de telefone de origem;

b) o nome e endereço do assinante ou do utilizador registado.

ii) Dados necessários para encontrar e identificar o destino de uma comunicação:

a) o(s) número(s) marcados (o número ou números de telefone de destino) 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;

b) o nome e o endereço do assinante, ou do utilizador registado.

iii) Dados necessários para identificar a data, a hora e a duração de uma comunicação:

a) a data e a hora do início e do fim da comunicação;

b) o serviço telefónico utilizado.

2º. Telefonia móvel:

i) Dados necessários para localizar e identificar a fonte de uma comunicação:

[122] Texto consolidado retirado do portal legislativo *LEGISLATION.GOV.UK*. Todas as referências legislativas relativas ao Reino Unido são feitas para este portal oficial, salvo indicação em contrário. Consultas efetuadas a 25/11/2022.

a) o número de telefone de origem;

b) o nome e endereço do assinante ou do utilizador registado.

ii) Dados necessários para encontrar e identificar o destino de uma comunicação:

a) o(s) número(s) marcados (o número ou números de telefone de destino) 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;

b) o nome e o endereço do assinante, ou do utilizador registado.

iii) Dados necessários para identificar a data, a hora e a duração de uma comunicação: a data e a hora do início e do fim da comunicação.

iv) Dados necessários para identificar o tipo da comunicação: o serviço telefónico utilizado.

v) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento:

a) a Identidade Internacional de Assinante Móvel («*International Mobile Subscriber Identity*», ou IMSI) e a Identidade Internacional do Equipamento Móvel («*International Mobile Equipment Identity*», ou IMEI) de quem telefona;

b) a IMSI e a IMEI do destinatário do telefonema;

c) 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.

vi) Dados necessários para identificar a localização do equipamento de comunicação móvel:

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

3º. Dados obtidos através do acesso à internet, de comunicações por correio eletrónico através da internet ou de comunicações telefónicas através da internet

i) Dados necessários para encontrar e identificar a fonte de uma comunicação:

a) o(s) código(s) de identificação atribuído(s) ao utilizador;

b) o código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública;

c) 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.

ii) Dados necessários para identificar o destino de uma comunicação:

a) no caso de comunicações telefónicas através da internet, o código de identificação de utilizador ou o número de telefone do destinatário pretendido;

b) no caso de comunicações por correio eletrónico através da internet ou de comunicações telefónicas através da internet, o(s) nome(s) e o(s) endereço(s) do(s) subscritor(es), ou do(s) utilizador(es) registado(s), e o código de identificação de utilizador do destinatário pretendido da comunicação.

iii) Dados necessários para identificar a data, a hora e a duração de uma comunicação:

a) No caso de dados obtidos através do acesso à internet, 1) 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, 2) endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à internet a uma comunicação, e 3) o código de identificação de utilizador do subscritor ou do utilizador registado;

b) No caso de comunicações por correio eletrónico através da internet ou de comunicações telefónicas através da internet, 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.

iv) Dados necessários para identificar o tipo de comunicação: no caso de comunicações por correio eletrónico através da internet ou de comunicações telefónicas através da internet, o serviço de internet utilizado.

v) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento:

a) No caso de acesso por linha telefónica, o número de telefone de origem;

b) Nos outros casos, a linha de assinante digital («*digital subscriber line*», ou DSL), ou qualquer outro identificador terminal do autor da comunicação.

Relativamente aos motivos que fundamentam o acesso aos dados, as *Regulations 2009* incluem uma previsão abstrata, determinando, na *Regulation 7*, que o acesso aos dados conservados nos termos do diploma só pode ser obtido em determinadas circunstâncias ou nas circunstâncias nas quais a divulgação dos dados é permitida ou exigida por lei.

Os dados devem ser conservados, de acordo com a *Regulation 5*, por um período de 12 meses, contado a partir do momento da comunicação em causa.

A decisão do Tribunal de Justiça da União Europeia, de 8 de abril de 2014, não implicou, até ao momento, nenhuma alteração diretamente nas *Regulations 2009.*

Contudo, é de referir o *Data Retention and Acquisition Regulations 2018* (de ora em diante designadas por *Regulations 2018*), que introduziram alterações ao *Regulation of Investigatory Powers Act 2000* e ao *Investigatory Powers Act 2016*. As *Regulations 2018* preveem a forma como os operadores postais e de telecomunicações podem reter os dados resultantes de comunicações, e a aquisição de tais dados pelas autoridades públicas e tornam efetivo o código de prática[123] relacionado com tais previsões.

Em especial, a *Regulation 8* introduz alterações à *Section 87* do *Investigatory Powers Act 2016*, no sentido de possibilitar que o Secretário de Estado envie uma solicitação de conservação de dados a um operador de telecomunicações, nos casos em que considere que tal solicitação: 1) satisfaz interesses de segurança nacional, 2) tem finalidades que se inserem no âmbito do procedimento criminal, 3) é do interesse do bem estar económico do Reino Unido (desde que tal interesse seja igualmente relevante no âmbito da segurança nacional), 4) é do interesse da segurança pública, 5) tem por fim prevenir a morte ou danos físicos ou psicológicos em pessoas ou mitigar esses mesmos danos, 6) tem por fim prestar apoio a investigações em casos de erros judiciários.

[123] Disponível no portal da *Asset Publishing and Research*.

SUÉCIA[124]

De acordo com as informações prestadas pelo Sveriges Riksdag[125], a Diretiva 2006/24/CE do Parlamento e do Conselho, de 15 de março de 2006 não foi transposta para a legislação nacional sueca dentro do prazo de transposição previsto (o prazo limite era até 15/09/2007). Nessa sequência, foi instaurado um processo por infração contra a Suécia (Case C-270/11)[126]. A transposição para o direito nacional apenas ocorreu a 1 de Maio de 2012, ainda antes do Acórdão do Tribunal de Justiça da União Europeia (TJUE) de 8 de Abril de 2014. *The Digital Ireland case* (processos apensos C-293/12 e C-594/12).

As disposições relativas à conservação de dados foram implementadas através do Electronic Communications Act (2003:389)[127], sendo que o diploma define que os períodos de conservação de dados variam conforme a sua tipologia, de acordo com o disposto no *§ 16 d*, abrangendo obrigações de conservação dos dados que variam entre dois, seis e dez meses. Relativamente às disposições relativas ao fornecimento de dados de tráfego às autoridades judiciais, as mesmas foram introduzidas através do Swedish Code of Judicial Procedure[128] e do Act on Collecting Information about Electronic Communications in the Law Enforcement Agencies' Intelligence Activities (2012:278)[129]. De acordo com o parecer das autoridades governamentais, as disposições daí decorrentes reforçaram a importância da proteção da privacidade.

No seguimento do Acórdão Tele2 Sverige and Watson[130], o Governo sueco criou uma comissão[131] com o objetivo de rever e alterar o enquadramento legal nacional vigente. As alterações que decorreram dos trabalhos da referida comissão resultaram nas seguintes ações[132]:

- Na limitação do âmbito da conservação de dados;
- Na diferenciação do período temporal de conservação de dados;
- No fim da permissão de conservação de dados fora do espaço da União Europeia;
- Na obrigatoriedade de recurso à decisão de um procurador, por parte das entidades judiciais, para efeitos de obtenção de dados de comunicações eletrónicas para efeitos de investigação;

[124] A informação contida neste resumo tem origem na resposta a um pedido realizado ao Parlamento sueco, estando todas as ligações eletrónicas a remeter para as ligações indicadas nessa resposta, em língua sueca.
[125] Disponível no sítio da Internet do *RIKSDAGEN.SE*, Todas as referências legislativas relativas à Suécia são feitas para este portal oficial, salvo indicação em contrário Consultas efetuadas a 25.11.2022.
[126] Disponível no sítio da Internet do *eur-lex.europa.eu*. Consultas efetuadas a 25.11.2022.
[127] Nos termos da *Government. bill 2010/11:46*. Disponível no sítio da Internet do *REGERINGEN.SE*. Consultas efetuadas a 25.11.2022.
[128] Publicação de Junho de 2015
[129] Nos termos *da Government bill. 2011/12:55*. Disponível no sítio da Internet do *REGERINGEN.SE*. Consultas efetuadas a 25.11.2022.
[130] Texto retirado do portal legislativo da União Europeia *EUR-LEX*. Consultas efetuadas a 25.11.2022
[131] No âmbito do procedimento denominado «*inquiry stage*». Disponível no sítio da Internet do *government.se*. Consultas efetuadas a 25.11.2022.
[132] Nos termos da *Government bill. 2018/19:86*. Disponível no sítio da Internet do *regeringen.se*. Consultas efetuadas a 25.11.2022.

- Na criação da possibilidade de obtenção de autorização para o acesso a dados relativos a atividades criminais que envolvam espionagem em empresas públicas, e criminalidade violenta ou detenção ilegal.

As alterações legislativas acima identificadas e introduzidas na *Electronic Communications Act (2003:389)*, supracitada, entraram em vigor em 1 de outubro de 2019.[133] O Parlamento sueco entendeu, contudo, que as alterações legislativas impunham demasiadas limitações à conservação de dados. Nestes termos, foi assim entendimento do Parlamento de que a conservação de dados deveria ser estendida tanto quanto possível dentro do quadro legal europeu. Em agosto de 2021, o Governo decidiu-se pela criação de uma nova comissão cujo mandato[134] incluía o seguinte âmbito:

- análise das condições nas quais novos serviços de comunicação seriam cobertos pela obrigação de conservação de dados;
- A consideração de alterações legislativas que visem manter ou reforçar a capacidade das autoridades judiciais; e
- A revisão dos recentes desenvolvimentos legais que decorre da jurisprudência do TJUE relativamente ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

Adicionalmente, o Governo sueco pronunciou-se[135], conjuntamente com outros Estados-Membros, a favor da extensão do âmbito de conservação de dados[136].

[133] Informações adicionais podem ser consultadas no Committee report 2018/19:JuU27, do *Swedish Riksdag*.
[134] Disponível no sítio da Internet do *riksdagen.se*. Consultas efetuadas a 25.11.2022.
[135] Disponível no sítio da Internet do *DATA.RIKSDAGEN.SE*. Consultas efetuadas a 25.11.2022.
[136] *Joined cases C-203/15 and C-698/15, joined cases C-793/19 and C-794/19, C-140/20 and C-470/21*.