Projeto de Lei n.º 70/XV/1 (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

Data de admissão: 12 de maio de 2022

Projeto de Lei n.º 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***

Data de admissão: 23 de maio de 2022

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias (1.ª)

ÍNDICE

Elaborada por: Sónia Milhano (DAPLEN), (DILP), Fernando Bento Ribeiro e Maria João Godinho (BIB), João Carlos Oliveira (BIB), Liliane Sanches da Silva e Nélia Monte Cid (DAC)
Data: 30.5.2022

I. A INICIATIVA

Projeto de Lei n.º 70/XV (PSD)

O Projeto de Lei em epígrafe preconiza a alteração da Lei n.º 32/2008, de 17 de julho, que *transpõe para a ordem jurídica interna a Directiva 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações* (informalmente designada Lei dos metadados), no sentido de a conformar com o Acordão do Tribunal Constitucional n.º 268/2022, que declarou a inconstitucionalidade com força obrigatória geral, dos artigos 4.º, 6.º e 9.º da Lei.

Como breve enquadramento que se impõe para a compreensão da iniciativa, cumpre recordar que a Lei n.º 32/2008 visou estabelecer a obrigação de os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações conservarem dados de tráfego e dados de localização relativos a essa comunicações, bem como dados conexos necessários para identificar o assinante ou utilizador, estando, porém, expressamente proibida a conservação de dados relativos ao conteúdo de comunicações.

A conservação destes dados tem por finalidade a investigação, deteção e repressão penal de crimes graves, considerando-se estes aqueles que, à luz da legislação processual penal, admitem a interceção e a gravação de conversações ou comunicações telefónicas. O acesso a este tipo de dados apenas pode ser solicitado pelo Ministério Público ou pela autoridade de polícia criminal competente, estando sempre dependente de decisão do juiz, devendo o acesso ser limitado em termos de adequação, necessidade e proporcionalidade face ao caso concreto.

Constituindo a referida decisão do Tribunal Constitucional o impulso legiferante invocado pelos proponentes, é possível fazer corresponder os passos da decisão por eles considerados relevantes e as alterações ora propostas, nos seguintes termos:

- para fazer face à falta de previsão legal de o armazenamento dos dados dever ocorrer no território da União Europeia, pondo em causa a efetividade dos direitos previstos nos 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 Carta dos Direitos Fundamentais da União Europeia, a iniciativa propõe que o n.º 1 do artigo 4.º da Lei passe a determinar que a conservação dos dados ocorra em Portugal ou em outro Estado-Membro da União Europeia;
- para expurgar a inconstitucionalidade da norma que permitia a conservação por um ano dos dados de tráfego e de localização, decorrente da conjugação dos artigos 4.º e 6.º da Lei n.º 32/2008, de 17 de julho, em violação dos n.ºs 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição, o proponente exclui desse prazo de conservação de um ano os dados de tráfego e localização, apenas conserváveis por 12 semanas a partir da data da conclusão da comunicação;
- para obviar à falta de previsão de 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 a integridade física de terceiros, o artigo 9.º da Lei n.º 32/2008, de 17 de julho, viola o disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição, a iniciativa estabelece a obrigatoriedade de notificação do titular dos dados acerca de qualquer transmissão dos dados «a partir do momento em que essa comunicação não seja suscetível de comprometer a investigação criminal ou de constituir risco para a integridade física ou vida de terceiros», competindo ao ao juiz de instrução que autorizou a transmissão dos dados informar o fornecedor de serviços de comunicações eletrónicas transmitente dos dados acerca do referido momento.

Porventura atenta a possibilidade de poder ficar comprometido o sucesso de processos-crime em curso em fase de investigação, julgamento ou recurso, os proponentes prevêem que, entrando a lei a aprovar em vigor no dia seguinte ao da sua publicação, a aplicação das novas normas aos dados que estejam a ser conservados e estabelecem a licitude da utilização de dados de tráfego e de localização conservados por prazo superior às 12 semanas agora propostas, desde que inferior a um ano, em processos pendentes em que já tenha sido deduzida acusação.

Projeto de Lei n.º 79/XV (CH)

O segundo Projeto de Lei em análise na presente nota preconiza a alteração da mesma Lei n.º 32/2008, de 17 de julho, que *transpõe para a ordem jurídica interna a Directiva 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações*, fazendo apelo *ao* Acordão do Tribunal Constitucional n.º 268/2022 e, bem assim, ao Acórdão de 8 de abril de 2014, *Digital Rights Ireland Ltd* e outros, C-293/12 e C-594/12, através do qual o Tribunal de Justiça da União Europeia declarou a invalidade da Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março de 2006; com base na violação do princípio da proporcionalidade, relativamente à restrição dos direitos ao respeito pela vida privada e familiar e à proteção dos dados pessoais, todos eles consagrados na Carta dos Direitos Fundamentais da União Europeia.

Os proponentes invocam ainda a Deliberação n.º 641/2017, de 9 de maio, da Comissão Nacional de Proteção de Dados, que confirma o seu entendimento sobre a violação dos direitos ao respeito pela vida privada e pelas comunicações e à proteção de dados pessoais, bem como constituir uma restrição desproporcionada face ao disposto no artigo 18.º da Constituição da República Portuguesa.

Impelidos por tais decisões, os proponentes defendem que o combate à criminalidade grave, que consideram necessário, "não pode ir tão longe que coloque em causa direitos fundamentais de todos os cidadãos, a todo o tempo", pelo que consideram justificar-se uma revisão da Lei que garanta que o Estado assegure os meios adequados à investigação criminal, salvaguardando a proporcionalidade e conjugando o direito à segurança com o direito à reserva da intimidade da vida privada e sigilo das comunicações.

Nesse sentido, a iniciativa preconiza a alteração dos artigos 3.º, 4.º, 6.º, 7.º, 9.º e 13.º da Lei n.º 32/2008, introduzindo regras mais restritivas para o acesso aos dados por parte dos órgãos de polícia criminal e de conservação dos dados por parte das operadoras de comunicação, apontando como questões normativas principais a superar:

- a possibilidade de conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização dos utilizadores de serviços de telecomunicações, ao abrigo dos artigos 4.º e 6.º da Lei;

- a falta de previsão, no artigo 7.º da mesma Lei, da obrigatoriedade de as autoridades que podem aceder aos dados informarem as pessoas em causa, no âmbito de uma investigação judicial, pelo menos a partir do momento em que tal informação não coloque em causa a referida investigação.

Assim, o Projeto de Lei em apreço passa a impor que a, a partir do dia seguinte ao da sua publicação, conservação ocorra "em território na União Europeia"; e mendianta decisão judicial, "relativo a pessoa concrtea e com efeitos para o futuro", pelo período de seis meses a partir "da data da conclusão da comunicação" (constituindo crime a conservação por período mais longo), e com notificação do acesso aos dados aos respetivos titulares "a partir do momento em que essa comunicação não seja suscetível de comprometer as investigações levadas a cabo por essas autoridades".

Informação adicional comum às duas iniciativas

Sobre a matéria objeto destas iniciativas[1], será relevante recordar, para além do Acórdão que, de acordo com os proponentes, constitui fundamento para a sua urgente apresentação, as recentes decisões do Tribunal Constitucional que responderam a pedidos da Senhora Procuradora-Geral da República – através da qual o Tribunal Constitucional decidiu não tomar conhecimento do requerimento da Senhora Procuradora-Geral da República que invocava a nulidade do Acórdão n.º 268/2022, por carecer de legitimidade processual e constitucional para a suscitar, tendo considerado, em qualquer caso, serem manifestamente improcedentes os argumentos invocados pela requerente - e do Partido Chega[2].

A matéria objeto das iniciativas em apreço tem sido amplamente noticiada, quer no que concerne à decisão do Tribunal Constitucional, como quanto aos seus efeitos, em

[1] Cujo teor fica evidenciado no quadro conmparativo que constitui o anexo desta nota técnica.
[2] Tal como noticiado pela Comunicação Social, de que é exemplo esta notícia

particular a sua retroatividade ou a sua eficácia retroativa, quer ainda quanto à necessidade de uma revisão constitucional suscetível de clarificar a possibilidade de utilização dos metadados em investigação criminal.

II. APRECIAÇÃO DOS REQUISITOS CONSTITUCIONAIS, REGIMENTAIS E FORMAIS

- **Conformidade com os requisitos constitucionais e regimentais**

Projeto de Lei n.º 70/XV (PSD)

A iniciativa em apreciação é apresentada pelo Grupo Parlamentar do Partido Social Democrata (PSD), ao abrigo e nos termos do n.º 1 do artigo 167.º da Constituição[3] e do n.º 1 do artigo 119.º do Regimento da Assembleia da República[4] (Regimento), que consagram o poder de iniciativa da lei. Trata-se de um poder dos Deputados, por força do disposto na alínea *b*) do artigo 156.º da Constituição e *b*) do n.º 1 do artigo 4.º do Regimento, bem como dos grupos parlamentares, por força do disposto na alínea *g*) do n.º 2 do artigo 180.º da Constituição e da alínea *f*) do artigo 8.º do Regimento.

Assumindo a forma de projeto de lei, em conformidade com o disposto no n.º 2 do artigo 119.º do Regimento, a iniciativa encontra-se redigida sob a forma de artigos, tem uma designação que traduz sinteticamente o seu objeto principal e é precedida de uma breve exposição de motivos, pelo que cumpre os requisitos formais previstos no n.º 1 do artigo 124.º do Regimento.

No que se refere aos limites à admissão da iniciativa estabelecidos no n.º 1 do artigo 120.º do Regimento, o projeto de lei define concretamente o sentido das modificações a introduzir na ordem legislativa, observando o disposto na alínea *b*) do preceito. Relativamente ao cumprimento do disposto na alínea *a*), que estabelece que «não são admitidos projetos e propostas de lei ou propostas de alteração que infrinjam a

[3] Hiperligação para o sítio da *Internet* da Assembleia da República.
[4] Hiperligação para o sítio da *Internet* da Assembleia da República.

Constituição ou os princípios nela consignados», cumpre fazer referência a alguns aspetos.

Em primeiro lugar, assinala-se que a iniciativa, no seu artigo 2.º, introduz alterações à Lei n.º 32/2008, de 17 de julho, nomeadamente aos artigos 4.º (Categoria de dados a conservar) e 6.º (Período de conservação), com o objetivo de a conformar com a decisão do Tribunal Constitucional (TC) vertida no Acórdão n.º 268/2022[5], no sentido de declarar a inconstitucionalidade, com força obrigatória geral, da interpretação conjugada destas normas.

Atendendo que as referidas normas restringem os direitos à reserva da intimidade da vida privada e à autodeterminação informativa (previstos nos n.ºs 1 e 4 do artigo 35.º e no n.º 1 do artigo 26.º da Constituição), o Tribunal apreciou se a obrigação de conservação dos dados respeita o princípio da proporcionalidade, previsto no n.º 2 do artigo 18.º da Constituição, atendendo aos outros valores constitucionalmente protegidos em causa — a segurança interna, a legalidade democrática e o exercício da ação penal no combate à criminalidade.

Neste âmbito, fazendo uma análise diferenciada dos tipos de dados conservados, no que respeita à obrigação de conservação dos dados de tráfego, o Tribunal é de opinião que «(…) materializam uma agressão mais intensa à intimidade da vida privada dos sujeitos privados do que a preservação dos dados de base, ao permitirem identificar, a todo o tempo, a posição e os movimentos dos utilizadores», o que «tem reflexos na proporcionalidade da restrição».

Focando a sua análise no âmbito subjetivo da norma, considera o TC que «Ao conservar todos os dados de localização e de tráfego de todos os assinantes, abrangem-se as comunicações eletrónicas da quase totalidade da população, sem qualquer diferenciação, exceção ou ponderação face ao objetivo perseguido». Conclui, assim, que «Neste quadro, por se ultrapassarem na medida fiscalizada os limites da proporcionalidade no que concerne ao respetivo âmbito subjetivo, viola-se o n.º 2 do artigo 18.º da Constituição na restrição aos direitos fundamentais à reserva da intimidade da vida privada e à autodeterminação informativa (artigos 26.º, n.º 1, e 35.º,

[5] Hiperligação para o sítio da Internet do Tribunal Constitucional.

n.º 1, da Constituição), perdendo relevância a questão de saber se os demais elementos de que dependeria a proporcionalidade da medida (o ajustamento do prazo de conservação ao estritamente necessário para os fins a alcançar; e a imposição de condições de segurança do respetivo armazenamento) são preenchidos pela regulamentação fiscalizada.»

Em face do exposto, será de equacionar se a solução preconizada na presente iniciativa, no sentido de restringir o período de conservação dos dados de tráfego e de localização a 12 semanas, sem prever uma definição ou limite do âmbito subjetivo da norma, respeita o princípio da proporcionalidade, previsto o n.º 2 do artigo 18.º da Constituição, na restrição aos direitos fundamentais à reserva da intimidade da vida privada e à autodeterminação informativa.

Por outro lado, assinala-se que o n.º 2 do artigo 3.º (Norma transitória) prevê a utilização, como meio de prova, de dados de tráfego e de localização, que tenham sido conservados pelas entidades previstas no n.º 1 do artigo 4.º por prazo superior a 12 semanas desde que inferior a um ano, nos processos pendentes e em que já tenha sido deduzida acusação no momento da entrada em vigor da lei que venha a resultar da presente iniciativa.

Esta norma pode suscitar algumas dúvidas quanto à sua compatibilidade com os efeitos da declaração de inconstitucionalidade com força obrigatória geral da «medida de conservação por um ano dos dados de tráfego e dos dados de localização, decorrente da conjugação do disposto do artigo 4.º com o artigo 6.º da Lei n.º 32/2008, de 17 de julho.»

De acordo com o n.º 1 do artigo 282.º da Constituição, «A declaração de inconstitucionalidade do TC com força obrigatória geral tem efeitos *ex tunc* (…). Produz um efeito de invalidação da norma porque faz remontar os efeitos à data da sua entrada em vigor. (…) Esta eficácia retroativa da declaração de inconstitucionalidade significa (…) proibição da aplicação das normas inconstitucionais a situações ou relações desenvolvidas à sombra da sua eficácia e ainda pendentes.»[6]

[6] CANOTILHO, J.J Gomes, Direito constitucional e teoria da Constituição, 7.ª ed., Edições Almedina, p. 1013.

Embora a Constituição permita ao TC fixar e restringir os efeitos da sua decisão, determinando que só produz efeitos para futuro (n.º 4 do artigo 282.º), não foi esta a opção do Tribunal no Acórdão em causa, pelo que as normas declaradas inconstitucionais «estão feridas de nulidade desde a sua entrada em vigor[7]».

Acrescenta ainda Gomes Canotilho, em anotação ao artigo 282.º da Constituição, que «A declaração de inconstitucionalidade (…) impõe-se também ao legislador, pelo que nenhuma lei pode vir a apagar os efeitos por ela produzidos, por exemplo, convalidando retroactivamente os actos administrativos praticados com base numa norma declarada inconstitucional (ou ilegal) sem limitação de efeitos (…)»[8]

Dever-se-á ter ainda em consideração, no que se refere à análise da possibilidade de utilização como meio de prova dos dados conservados ao abrigo das normas julgadas inconstitucionais, as garantias de processo penal consagradas no artigo 32.º da Constituição, que determina a nulidade das provas obtidas mediante abusiva intromissão na vida privada ou telecomunicações (n.º 8), «(…) devendo ter-se por abusiva a intromissão (…) quando desnecessária ou desproporcionada ou quando aniquiladora dos próprios direitos (cfr. Art. 18.º- 2 e 3).[9]»

Assim, assinalamos que, apesar de as normas acima referidas poderem suscitar dúvidas sobre a sua constitucionalidade, a análise do cumprimento das normas constitucionais em causa caberá, em concreto, à comissão competente.

Cumpre ainda referir que a matéria sobre a qual versa a presente iniciativa enquadra-se, por força do disposto na alínea *b*) do artigo 165.º da Constituição, no âmbito da reserva relativa de competência legislativa da Assembleia da República.

O projeto de lei em apreciação deu entrada a 11 de maio de 2022, tendo sido junta a ficha de avaliação prévia de impacto de género. Foi admitido a 12 de maio, data em que, por despacho do Presidente da Assembleia da República, baixou na generalidade à

[7] CANOTILHO, J.J Gomes e MOREIRA, Vital, Constituição da República Portuguesa Anotada, II vol., 4.ª ed., Coimbra Editora, p. 975.
[8] CANOTILHO, J.J Gomes e MOREIRA, Vital, Constituição da República Portuguesa Anotada, II vol., 4.ª ed., Coimbra Editora, p. 980.
[9] CANOTILHO, J.J Gomes e MOREIRA, Vital, Constituição da República Portuguesa Anotada, I vol., 4.ª ed., Coimbra Editora, p. 524.

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias (1.ª), tendo sido anunciado na sessão plenária do dia 23 de maio. A respetiva discussão na generalidade encontra-se agendada para a reunião plenária do dia 3 de junho (*cfr.* Súmula n.º 6 da Conferência de Líderes, de 18 de maio de 2022).

Projeto de Lei n.º 79/XV (CH)

A iniciativa em apreciação é apresentada pelo Grupo Parlamentar do partido Chega (CH), ao abrigo e nos termos da alínea *b)* do artigo 156.º e do n.º 1 do artigo 167.º da Constituição[10] e da alínea *b)* do n.º 1 do artigo 4.º e do n.º 1 do artigo 119.º do Regimento da Assembleia da República[11] (Regimento), que consagram o poder de iniciativa da lei.

Assumindo a forma de projeto de lei, em conformidade com o disposto no n.º 2 do artigo 119.º do Regimento, a iniciativa encontra-se redigida sob a forma de artigos, tem uma designação que traduz sinteticamente o seu objeto principal e é precedida de uma breve exposição de motivos, pelo que cumpre os requisitos formais previstos no n.º 1 do artigo 124.º do Regimento.

Respeita igualmente os limites à admissão da iniciativa estabelecidos no n.º 1 do artigo 120.º do Regimento, uma vez que parece não infringir a Constituição ou os princípios nela consignados e define concretamente o sentido das modificações a introduzir na ordem legislativa.

Cumpre ainda referir que a matéria sobre a qual versa a presente iniciativa enquadra-se, por força do disposto na alínea *b*) do artigo 165.º da Constituição, no âmbito da reserva relativa de competência legislativa da Assembleia da República.

O projeto de lei em apreciação deu entrada a 19 de maio de 2022, tendo sido junta a ficha de avaliação prévia de impacto de género. Foi admitido a 23 de maio, data em que, por despacho do Presidente da Assembleia da República, baixou na generalidade à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias (1.ª). Nesse mesmo dia foi anunciado em reunião plenária. A respetiva discussão na generalidade

[10] Hiperligação para o sítio da *Internet* da Assembleia da República.
[11] Hiperligação para o sítio da *Internet* da Assembleia da República.

encontra-se agendada para a reunião plenária do dia 3 de junho, por arrastamento com o Projeto de Lei n.º 70/XV/1.ª (PSD) (*cfr.* Boletim Informativo).

- **Verificação do cumprimento da lei formulário**

Projeto de Lei n.º 70/XV (PSD)

A Lei n.º 74/98, de 11 de novembro, conhecida como lei formulário[12] contém um conjunto de normas sobre a publicação, identificação e formulário dos diplomas que são relevantes em caso de aprovação da presente iniciativa.

O título da presente iniciativa legislativa - 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 - traduz sinteticamente o seu objeto, mostrando-se conforme ao disposto no n.º 2 do artigo 7.º da lei formulário.

Em caso de aprovação, esta iniciativa revestirá a forma de lei, nos termos do n.º 3 do artigo 166.º da Constituição, pelo que deve ser objeto de publicação na 1.ª série do Diário da República, em conformidade com o disposto na alínea *c)* do n.º 2 do artigo 3.º da lei formulário.

No que respeita ao início de vigência, o artigo 4.º deste projeto de lei estabelece que a sua entrada em vigor ocorrerá «no dia seguinte ao da sua publicação», mostrando-se

[12] Hiperligação para o sítio da Internet da Assembleia da República.

assim conforme com o previsto no n.º 1 do artigo 2.º da lei formulário, segundo o qual os atos legislativos «entram em vigor no dia neles fixado, não podendo, em caso algum, o início de vigência verificar-se no próprio dia da publicação».

Nesta fase do processo legislativo, a iniciativa em apreço não nos parece suscitar outras questões em face da lei formulário.

Projeto de Lei n.º 79/XV (CH)

A Lei n.º 74/98, de 11 de novembro[13], conhecida como lei formulário, contém um conjunto de normas sobre a publicação, identificação e formulário dos diplomas que são relevantes em caso de aprovação da presente iniciativa.

Antes de mais, assinala-se que o título da presente iniciativa legislativa - Altera a Lei n.º 32/2008, de 17 de julho, por forma a harmonizá-la com os preceitos constitucionais em vigor - traduz sinteticamente o seu objeto, mostrando-se conforme ao disposto no n.º 2 do artigo 7.º da lei formulário.

Cumpre referir que o diploma que a iniciativa visa alterar, ou seja, a Lei n.º 32/2008, de 17 de julho, foi modificado pela Lei n.º 79/2021, de 24 de novembro, tal como referido no articulado e confirmado pela consulta da base de dado *Digesto* (Diário da República Eletrónico). Assim, em caso de aprovação, esta constituirá a sua segunda alteração.

Em face do exposto, há que atender ao n.º 1 do artigo 6.º da lei formulário, que dispõe que «Os diplomas que alterem outros devem indicar o número de ordem da alteração introduzida e, caso tenha havido alterações anteriores, identificar aqueles diplomas que procederam a essas alterações (…)». No sentido do cumprimento desta norma, sugere-se que a iniciativa faça menção ao número de ordem de alteração à Lei n.º 32/2008, de 17 de julho, devendo as informações referidas constarem preferencialmente no artigo relativo ao objeto.

Em caso de aprovação, esta iniciativa revestirá a forma de lei, nos termos do n.º 3 do artigo 166.º da Constituição, pelo que deve ser objeto de publicação na 1.ª série do

[13] Hiperligação para o sítio da Internet da Assembleia da República.

Diário da República, em conformidade com o disposto na alínea *c)* do n.º 2 do artigo 3.º da lei formulário.

No que respeita ao início de vigência, o artigo 3.º deste projeto de lei estabelece que a sua entrada em vigor ocorrerá «no dia seguinte ao da sua publicação», mostrando-se assim conforme com o previsto no n.º 1 do artigo 2.º da lei formulário, segundo o qual os atos legislativos «entram em vigor no dia neles fixado, não podendo, em caso algum, o início de vigência verificar-se no próprio dia da publicação».

Nesta fase do processo legislativo, a iniciativa em apreço não nos parece suscitar outras questões em face da lei formulário.

- **Conformidade com as regras de legística formal**

Projeto de Lei n.º 79/XV (CH)

A elaboração de atos normativos da Assembleia da República deve atender às regras de legística formal, nomeadamente as constantes do Guia de Legística para a Elaboração de Atos Normativos[14], por forma a garantir a clareza dos textos normativos, mas também a certeza e a segurança jurídicas.

Neste sentido, em caso de aprovação da presente iniciativa, deverá ser ponderado o aditamento de uma norma revogatória, sendo criado um novo artigo para assinalar a revogação da alínea *f*) do n.º 1 do artigo 4.º da Lei n.º 32/2008, de 17 de julho, prevista no artigo 2.º do projeto de lei. De acordo com o referido Guia, «Quando a alteração de um artigo implicar a revogação não substitutiva de um dos seus números, a referida revogação deve ser evidenciada na norma de alteração e na norma revogatória final.»

Na presente fase do processo legislativo, a iniciativa em apreço não nos suscita outras questões pertinentes no âmbito da legística formal, sem prejuízo da análise mais detalhada a ser efetuada no momento da redação final.

[14] Hiperligação para o sítio da *Internet* da Assembleia da República.

III. ENQUADRAMENTO JURÍDICO NACIONAL

A Constituição[15] regula no seu artigo 35.º a utilização da informática, no âmbito dos direitos, liberdades e garantias pessoais; nomeadamente nos seus n. os 1: «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» e 4: «É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei».

Como estipula o n.º 2 do artigo 18.º da Constituição «A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos».

Por fim, ressalve-se 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», como referido no n.º 1 do artigo 26.º da Constituição.

Os preceitos constitucionais invocados devem ser interpretados em conformidade com o disposto nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia[16]. Os referidos artigos são relativos ao "Respeito pela vida privada e familiar" (artigo 7.º) e à "Proteção de dados pessoais" (artigo 8.º).

A Lei n.º 32/2008, de 17 de julho[17], transpõe para a ordem jurídica interna a Directiva 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

[15] Todas as referências legislativas à Constituição da República Portuguesa nesta parte da nota técnica são feitas para o portal oficial da Assembleia da República, salvo indicação em contrário. Consulta efetuada em 20.05.2022
[16] Todas as referências legislativas ao Direito da União Europeia são feitas para o sítio da *Internet* do *EUR-Lex*, salvo indicação em contrário. Consultas efetuadas a 20.05.2022
[17] Todas as referências legislativas são feitas para o sítio da *Internet* do *Diário da República Eletrónico*, salvo indicação em contrário. Consultas efetuadas a 20.05.2022.

comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.

A Diretiva n.º 2006/24/CE, foi declarada inválida pelo Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014[18]. Os pedidos apresentados perante o TJUE são relativos a um litígio acerca da legalidade de medidas legislativas e administrativas nacionais respeitantes à conservação de dados relativos a comunicações eletrónicas; e a recursos em matéria constitucional interpostos, acerca da compatibilidade da lei que transpõe a Diretiva 2006/24 para o direito interno austríaco com a lei constitucional federal (Bundes-Verfassungsgesetz).

A Lei n.º 32/2008, de 17 de julho, regula a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, detecção e repressão de crimes graves por parte das autoridades competentes, transpondo para a ordem jurídica interna a Directiva 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações.

A conservação de dados que revelem o conteúdo das comunicações é proibida, sem prejuízo do disposto na Lei n.º 41/2004, de 18 de Agosto, (Transpõe para a ordem jurídica nacional a Directiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas) e na legislação processual penal relativamente à intercepção e gravação de comunicações.

[18] Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014.
Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources e o. e Kärntner Landesregierung e o.
Pedidos de decisão prejudicial apresentados pela High Court (Irlanda) e pelo Verfassungsgerichtshof.
Comunicações eletrónicas — Diretiva 2006/24/CE — Serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações — Conservação de dados gerados ou tratados no contexto da oferta desses serviços — Validade — Artigos 7.°, 8.° e 11.° da Carta dos Direitos Fundamentais da União Europeia.
Processos apensos C-293/12 e C-594/12. Consulta efetuada a 20.05.2022

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 estabelecidos pela Portaria n.º 469/2009, de 6 de maio[19], alterada pelas Portarias n.ºs 915/2009, de 18 de agosto, e 694/2010, de 16 de agosto.

O Capítulo IV, do Livro III (Dos meios de obtenção da prova) do Código de Processo Penal (CPP), regula nos artigos 187.º a 190.º as "escutas telefónicas". «A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público», quanto aos crimes descritos no n.º 1 do artigo 187.º do CPP.

«A intercepção e a gravação de conversações ou comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respectivos requisitos de admissibilidade» (n.º 6 do artigo 187.º). «Sem prejuízo do disposto no artigo 248.º, a gravação de conversações ou comunicações só pode ser utilizada em outro processo, em curso ou a instaurar, se tiver resultado de intercepção de meio de comunicação utilizado por pessoa referida no n.º 4 e na medida em que for indispensável à prova de crime previsto no n.º 1» (n.º 7 do artigo 187.º).

O Acórdão do Tribunal da Relação de Coimbra[20], de 06.03.2013 (364/12.3TALRA-A.C1) relativo a escutas telefónicas, refere que «a transcrição da gravação de conversações ou comunicações telefónicas obtidas no decurso de um inquérito, conquanto não possam valer como meio de prova no âmbito de outro, quando o suspeito neste não integra qualquer alvo e não detém a referida qualidade naquele, têm sempre, na descrita situação, um valor residual para efeitos de notícia de outro crime a investigar, que é

[19] Texto consolidado. Consulta efetuada em 20.05.2022
[20] Informação disponível no site da DGSI em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/76c938fcd1fda3b880257b40004b79df?OpenDocument Consulta efetuada a 20.05.2022

salvaguardado pelo primeiro segmento do n.º 7 do artigo 187.º do CPP ("Sem prejuízo do disposto no artigo 248.º (…)"».

A Lei n.º 109/2009, de 15 de setembro – Lei do Cibercrime – ,"estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime [21][22] do Conselho da Europa" (artigo 1.º).

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".
O Tribunal Constitucional, em recente acórdão (cfr. infra), considera que esta lei «determina que o responsável pelo armazenamento dos dados é obrigado a facultar ao titular dos dados pessoais retidos, a seu pedido, informações sobre a sua transmissão (artigo 13.º e alínea c) do n.º 2 do artigo 15.º), bem como a apresentar queixa à autoridade de controlo de eventuais violações do regime jurídico (alínea f) do n.º 2 do artigo 15.º da Lei n.º 59/2019, de 8 de agosto). O que explica, aliás, a obrigação de os fornecedores de serviços de comunicações eletrónicas elaborarem «*registos da extração dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD*» (n.º 5 do artigo 9.º da Lei n.º 32/2008, de 17 de julho). Em conformidade, a informação de que os dados foram transmitidos só pode ser recusada para evitar prejuízos para investigações criminais, execução de sanções penais, proteção da segurança pública ou proteção de direitos, liberdades e garantias de terceiros (n.º 1 do artigo 16.º da Lei n.º 59/2019, de 8 de agosto), caso em que a rejeição da prestação dessa informação é judicialmente controlável, mediante ação judicial especialmente prevista e de cuja existência é o visado informado (n.º 2 do artigo 16.º e artigo 18.º, todos da Lei n.º 59/2019, de 8 de agosto). Nessa medida, o ordenamento

[21] Disponível em: https://rm.coe.int/16802fa428. Consulta efetuada a 20.05.2022
[22] A Convenção sobre o Cibercrime, ou Convenção de Budapeste, foi assinada por Portugal em 23 de novembro de 2001, data da sua conclusão, entrou em vigor na ordem internacional em 1 de julho de 2004 e foi aprovada para ratificação pela Resolução da Assembleia da República n.º 88/2009, de 15 de setembro. Consulta efetuada a 20.05.2022

vigente atribui ao titular dos dados o direito a conhecer que estes foram transmitidos às autoridades de investigação criminal quando essa informação não seja já necessária às investigações criminais em curso. Prevendo-se mecanismos judiciais (artigo 18.º, n.º 3 da Lei n.º 59/2019, de 8 de agosto) e administrativos (artigo 18.º, n.º 2 da Lei n.º 59/2019, de 8 de agosto) de controlo de eventuais recusas dessa transmissão».

A Lei n.º 79/2021, de 24 de novembro[23], procedeu à primeira alteração da Lei n.º 32/2008, modificando a definição de 'crime grave', prevista na alínea *g)* do n.º 1, do artigo 2.º.

Ressalve-se ainda a referência à Deliberação n.º 641/2017, de 9 de maio[24], da Comissão Nacional de Proteção de Dados, que recomendou a revisão da Lei n.º 32/2008.

Recentemente o Tribunal Constitucional, na sequência de pedido apresentado pela Senhora Provedora de Justiça, declarou através do Acórdão n.º 268/2022, de 19 de abril[25], a inconstitucionalidade, com força obrigatória geral, dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho.

O artigo 4.º identifica as categorias de dados a armazenar pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações; o artigo 6.º determina a obrigação da sua conservação pelo período de um ano, a contar da data da conclusão da comunicação; e o artigo 9.º estabelece as condições de transmissão de dados armazenados ao Ministério Público ou à autoridade de polícia criminal competente

Na Lei n.º 32/2008, de 17 de julho, são identificáveis dois regimes jurídicos em torno dos dados identificados no artigo 4.º: um relativo à obrigação de conservação pelos fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações, essencialmente contido nos artigos 4.º a 8.º; e outro atinente ao seu

[23] Transpõe a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, alterando o Código Penal, o Código de Processo Penal, a Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, e outros atos legislativos.
[24] Informação disponível no sítio Internet da CNPD, em https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/104933 Consulta efetuada a 25.05.2022
[25] Informação disponível no sítio Internet do Tribunal Constitucional. Consulta efetuada em 20.05.2022

acesso pelas autoridades competentes para a investigação e repressão criminal, estatuído nos artigos 9.º a 11.º.

A Provedora de Justiça solicitou a fiscalização da constitucionalidade do regime jurídico da conservação dos dados (quanto ao seu âmbito e duração) e, bem assim, da norma que disciplina a transmissão dos dados às autoridades competentes para a investigação, deteção e repressão de crimes graves.

Destacamos as seguintes considerações expressas no citado acórdão do Tribunal Constitucional: «No que tange ao regime de conservação dos dados, prevê-se uma obrigação, para os fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações, de preservação dos dados elencados no artigo 4.º, relativos a quaisquer utilizadores e assinantes.»

«O legislador previu um dever de conservação com a mesma segurança e proteção que os dados na rede (alínea b) do n.º 1 do artigo 7.º da Lei n.º 32/2008, de 17 de julho) e disciplinou que a sua transmissão eletrónica às autoridades ocorresse «*nos termos das condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados*» (n.º 3 do artigo 7.º), subordinando o controlo dessas regras à Comissão Nacional de Proteção de Dados [CNPD], nos termos do n.º 5 do artigo 7.º. Em conformidade, a Portaria n.º 469/2009, de 6 de maio, alterada pelas Portarias n.ºs 915/2009, de 18 de agosto, e 694/2010, de 16 de agosto, estabeleceu medidas relativas às condições técnicas e de segurança dos dados conservados. O ato regulamentar incide essencialmente sobre a segurança da transmissão dos dados às autoridades públicas, instituindo uma aplicação informática específica e prevendo regras para todo o procedimento de transmissão. Não versa, porém, sobre os requisitos de segurança da conservação de dados pelos operadores — aludindo-se apenas à obrigação de os sujeitar «à mesma segurança e proteção que os dados na rede» (alínea b) do n.º 1 do artigo 7.º da Lei n.º 32/2008, de 17 de julho).»

«Por outro lado, as disposições relativas à conservação de dados (essencialmente contidas no artigo 7.º da Lei n.º 32/2008, de 17 de julho) não impõem que o seu armazenamento ocorra em Portugal (ou em outro Estado-Membro da União Europeia).

Os dados referidos no artigo 4.º não abrangem o conteúdo das comunicações, dizendo respeito somente às suas circunstâncias — razão pela qual são usualmente designados por metadados (ou dados sobre dados) — cfr. Acórdãos n. os 403/2015 e 420/2017(…). O conjunto de metadados elencado no artigo 4.º abrange dados de diferente natureza, categorizados na jurisprudência constitucional como dados de base e dados de tráfego. A distinção é relevante, pois a tutela constitucional não é modelada nos mesmos termos para as duas espécies.»

«No que respeita ao acesso aos dados pelas autoridades competentes para investigação, deteção e repressão criminal, exige-se a autorização do juiz de instrução, requerida pelo Ministério Público ou pela autoridade de polícia criminal competente, ficando subordinada à existência de «razões para crer que a obtenção desses dados 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.ºs 1 e 2 do artigo 9.º da Lei n.º 32/2008, de 17 de julho)».

Entende ainda o TC que «Não restam dúvidas que as normas fiscalizadas se colocam no domínio de aplicação do Direito da União Europeia e, por isso, estão abrangidas pela Carta dos Direitos Fundamentais da União Europeia (CDFUE)».

Recorde-se que as normas em apreço haviam sido objeto de vasta jurisprudência, de que se refere, a título de exemplo:

1. Ac. TRL de 22-06-2016: - Solicitar a operadoras de telemóveis todos os dados de tráfego dos cartões SIM que operaram num determinado período de tempo em 19 antenas, mas não estando concretizados alvos determináveis, e atingindo a diligência pretendida um universo ilimitado e indiferenciado de cidadãos que não se integram no conceito jurídico-penal de “suspeitos” é proibido por lei e não respeita os princípios constitucionais da proporcionalidade e da adequação.

2. Ac. TRL de 03-05-2016: - Não é permitido, em inquérito, solicitar às operadoras de comunicações que forneçam todos os números de telefone que num determinado período de tempo se conectaram a uma determinada antena, sem que se determinem previamente os suspeitos, o que, em caso de desconhecimento da respetiva identificação, pressupõe a existência de dados factuais tendentes à sua

individualização, não sendo admissível que sejam consideradas suspeitas de determinada ação criminosa todas as pessoas que se encontrassem naquele local e tempo.

3. Ac. TRE de 19-05-2015 : I - A falta de suspeito ou suspeitos determinados contra quem dirigir as escutas telefónicas, os pedidos de obtenção de dados de tráfego ou os pedidos de localização celular, é obstáculo intransponível à realização deste tipo de meios de obtenção de prova. II - Recolher informações de pessoas inocentes, na esperança de, de entre estas, se "apanhar" algum suspeito, é desproporcional aos fins visados, sendo, pois, uma compressão inconstitucional e ilícita do direito à privacidade e à inviolabilidade das comunicações.

4. Ac. TRE de 25.10.2016 :1 - No caso de investigação e repressão de infrações penais relativas a comunicações, dados de comunicações e sua conservação existe legislação especial que secundariza o Código de Processo Penal e torna quase irrelevantes as Leis n.os 5/2004 e 41/2004 para efeitos processuais penais. 2 - Tal legislação especial são as Leis n.os 32/2008, de 17-07 (Lei relativa a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações) e 109/2009, de 15-09 (Lei do Cibercrime), assim como a Convenção do Conselho da Europa sobre o Cibercrime de 23/11/2001 (Resolução da AR n.º 88/2009, de 15 de Setembro), também designada Convenção de Budapeste. 3- Tratando-se de dados de comunicações conservadas ou preservadas já não é possível aplicar o disposto no artigo 189.º do Código de Processo Penal - a extensão do regime das escutas telefónicas - aos casos em que são aplicáveis as Leis n.os 32/2008 e 109/2009 e a Convenção de Budapeste. Isto é, para a prova de comunicações preservadas ou conservadas em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11.º a 19.º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pelos artigos 3.º a 11.º da Lei nº 32/2008, se for caso de dados previstos nesta última. 4 - A Lei n.º 32/2008 tem um regime processual privativo da matéria por si regulada, assente na existência de dados conservados nos termos do artigo 4.º, n.º 1, pelos fornecedores de serviços. 5 - O regime processual aplicável é o constante dessa lei, inclusive o catálogo de crimes permissivo que ela criou, os crimes graves referidos no artigo 3.º, n.º 1. 6- O conceito de "crime grave", abarcando a criminalidade violenta - artigo 2.º, n.º 1, al. *g)* do diploma -, abrange o crime de violência

doméstica previsto no n.º 1 do artigo 152.º do Código Penal por via da previsão do artigo 1.º, al. *j)* do C.P.P. 7 - De onde resulta a aplicabilidade ao caso dos autos do regime processual previsto nos artigos 3.º a 11.º da Lei n.º 32/2008. 8 - E, face ao n.º 2 da Lei 32/2008, a transmissão dos dados as autoridades competentes - Ministério Público ou autoridade de polícia criminal competente - só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º do diploma, que regula a "transmissão dos dados" e que apresenta como pressuposto substancial que haja 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. 9 - Esta transmissão ou processamento veio a ser regulada pela Portaria n.º 469/2009, de 06 de maio - Condições Técnicas e de Segurança, Tratamento de Dados de Tráfego - que mantém hoje a redação dada pela Portaria n.º 694/2010, de 16/08.

5. Ac. TRL de 07.03.2017 :I O regime dos artigos 187.º a 189.º, do CPP, aplica-se aos "dados sobre a localização celular", obtidos em tempo real e interceção das comunicações entre presentes, enquanto o consagrado na Lei n.º 32/2008, de 17/07, tem como âmbito de aplicação os dados que concernem a comunicações relativas ao passado, ou seja, arquivadas. II- Na densificação do conceito de suspeito aceita-se que pode ele não ser determinado - que se não conheça a sua identificação completa -, não pode, porém, dispensar-se a existência de dados factuais tendentes a essa identificação, com recurso aos quais possa ser identificável e tal desiderato não se satisfaz pela circunstância de dezenas ou mesmo centenas de pessoas terem efetuado comunicações telefónicas em três áreas geográficas em período temporal próximo ao momento da prática do crime de roubo em investigação, tendo feito ativar a mesma antena, quer no que respeita ao emissor, quer ao recetor. III- No decurso do inquérito deve o Juiz de Instrução Criminal indeferir o requerimento do Ministério Público em que impetra se ordenasse às operadoras de telemóveis a remessa para os autos, relativamente a dia concretizado, no período entre as 08:45 horas e as 09:15 horas, de "listagem - em suporte digital e formato *Excel* - com: identificação dos cartões telefónicos que tenham recebido ou realizado chamadas de voz ou texto de ou para cartões presentes na mesma célula em questão e a seguir identificada - n.º chamador e n.º chamado ativados na mesma célula; identificação dos IMEI em que esses cartões operavam na altura; identificação dos titulares desses cartões ou códigos de

carregamento Multibanco dos mesmos. Quanto às antenas que se identificam a Fls. 16 e vs. dos presentes autos", tendo em atenção o estabelecido nos artigos 1.º, n.º 1, 2.º, n.º 1, alínea *g)*, 4.º, 9.º, n.º 3, alínea *a)*, da Lei n.º 32/2008, de 17/07, 1.º, alínea *e)*, do CPP, 26.º, n.º 1 e 34.º, n.ºs 1 e 4, da Constituição da República Portuguesa.

6. Ac. TC n.º 420/2017, de 13.07.2017: Dados de tráfego. O TC decidiu não julgar inconstitucional a norma que estabelece o dever de os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações conservarem pelo período de um ano a contar da data da conclusão da comunicação, os dados relativos ao nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP estava atribuído no momento da comunicação, constante do disposto no artigo 6.º e do artigo 4.º, n.º 1, alínea *a)*, 2.ª parte, e n.º 2, alínea *b)*, subalínea *iii)*, ambos da Lei n.º 32/2008 de 17 de julho.

7. Ac. TRC de 08.11.2017: Obtenção de dados de tráfego. Requisitos. I - Os valores constitucionais da descoberta da verdade material e da realização da justiça, mesmo em matéria criminal, estão sujeitos aos limites impostos pela dignidade e pelos direitos fundamentais das pessoas e que processualmente se traduzem nas proibições de prova, em relação aos quais o artigo 32.º, n.º 8, da CRP, estabelece, quanto à questão que agora nos ocupa, que são nulas todas as provas obtidas mediante abusiva intromissão nas telecomunicações. II - A obtenção de dados de tráfego e de localização como aqueles que o Ministério Público pretende só pode ocorrer em relação às pessoas referidas no artigo 9.º, n.º 3, da Lei 32/2008, de 17-07, e no n.º 4 do artigo 187.º do CPP, ou seja, *a)* o suspeito ou arguido; *b)* a pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou *c)* a vítima de crime, mediante o respetivo consentimento, efetivo ou presumido. III - É também pressuposto que existam 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. IV - Exige-se ainda que a decisão judicial de transmitir os dados respeite os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados. V - Não é permitido que se aceda a dados de tráfego e de localização de um conjunto

indeterminado de pessoas que efetuaram comunicações, acionado células de antenas de comunicações, na expectativa de, entre elas, descortinar quem possa ter praticado o ilícito investigado. VI - Pretende-se, pois, obter dados de tráfego e de localização, desejavelmente de suspeitos, mas seguramente de muitos não suspeitos. VII - O que não é permitido pela salvaguarda do sigilo das telecomunicações, consubstanciada nos apertados limites estabelecidos na Lei n.º 32/2008 e nas exigências constitucionais de adequação, necessidade e proporcionalidade.

8. Ac. TRE de 20-01-2015 : 1. O regime processual das comunicações telefónicas previsto nos artigos 187.º a 190.º do Código de Processo Penal deixou de ser aplicável por extensão às "telecomunicações eletrónicas", "crimes informáticos" e "recolha de prova eletrónica (informática)" desde a entrada em vigor da Lei n.º 109/2009, de 15-09 (Lei do Cibercrime) como regime regra. 2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável à recolha de prova por "localização celular conservada" uma forma de "recolha de prova eletrónica - desde a entrada em vigor da Lei n.º 32/2008, de 17-07. 3. Para a prova eletrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11.º a 19.º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face à prova por «localização celular conservada". 4. Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11.º a 17.º e o regime dos artigos 18.º e 19.º do mesmo diploma. O regime processual dos artigos 11.º a 17.º surge como o regime processual "geral" do cibercrime e da prova eletrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18.º, n.º 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18.º e 19.º - são aplicáveis por remissão expressa os artigos 187.º, 188.º e 190.º do C.P.P. e sob condição de não contrariarem e Lei n.º 109/2009. 5. As normas contidas nos artigos 12.º a 17.º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n.º 1 do artigo 11.º, estão (a) previstos na lei n.º 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico. 6. A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12.º a 17.º se referirem à pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18.º do diploma se

refere à interceção de comunicações eletrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático. 7. Assim, o Capítulo III da Lei 109/2009, relativo às disposições processuais, deve ser encarado como um «escondido Capítulo V ("Da prova eletrónica"), do Título III ("Meios de obtenção de prova") do Livro III ("Da prova") do Código de Processo Penal» (Dá Mesquita). 8. Tratando-se de obter prova por «localização celular conservada», isto é, a obtenção dos dados previstos no artigo 4.º, n.º 1 da Lei n.º 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3.º e 9.º desta lei. 9. Em suma, numa interpretação conjugada das Leis n.os 32/2008 e 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República n.º 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n.º 1 do artigo 11.º da Lei n.º 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11.º a 17.º dessa Lei; - o catálogo de crimes do n.º 1 do artigo 18.º da Lei n.º 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18.º e no 19.º dessa Lei aos crimes previstos na al. a) do artigo 18.º; - o catálogo de crimes do n.º 1 do artigo 187.º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18.º e no 19.º dessa Lei para os crimes previstos na al. b) do artigo 18.º; - o catálogo de crimes ("crimes graves") do artigo 3.º da Lei n.º 32/2008 quanto a especiais "dados conservados" (localização celular), como requisito de aplicação dos artigos 3.º e 9.º da Lei n.º 32/2008. 10. O artigo 189.º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável. 11. O objeto de ambas as leis - de 2008 e 2009 - é parcialmente coincidente. Ambas se referem e regulam "dados conservados" (Lei n.º 32/2008) e "dados preservados" (Lei n.º 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (à exceção do correio eletrónico, especificamente previsto no seu artigo 17.º). 12. O regime processual da Lei n.º 32/2008 constitui relativamente aos dados "conservados" que prevê no seu artigo 4.º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11.º a 19.º da Lei n.º 109/2009. 13. Consequentemente devemos concluir que o regime processual da Lei n.º 32/2008, designadamente o artigo 3.º, n.os 1 e 2, e o artigo 9.º: - mostra-se

revogado e substituído pelo regime processual contido na Lei n.º 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4.º, n.º 1, da Lei n.º 32/2008, ou seja, dados conservados em geral; - revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4.º, n.º 1 da Lei n.º 32/2008, isto é, para os dados conservados relativos à localização celular. Só para este último caso ganha relevo o conceito de "crime grave". 14. Antes da entrada em vigor das Leis n.os 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis "processualmente úteis" de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252.º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189.º, n.º 2, do mesmo código, que se mantém em vigor para a localização celular em tempo real. 15. Agora coexistem três realidades distintas através do acrescento da obtenção de dados de localização celular "conservados" por via da Lei n.º 32/2008. 16. Os requisitos do n.º 3 do artigo 9.º da Lei n.º 32/2008 mostram-se de verificação alternativa. O conceito de "suspeito" dele constante exige "determinabilidade" e não "determinação". 17. A previsão do artigo 252.º-A do Código de Processo Penal é claramente uma previsão de carácter excecional para situações de carácter excecional.

9. Ac. TRE de 06-01-2015: - O regime processual da Lei n.º 32/2008 (designadamente o artigo 3.º, n.os 1 e 2, e o artigo 9.º) está revogado e substituído pelo regime processual contido na Lei n.º 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4.º, n.º 1, daquela lei, ou seja, dados conservados em geral; está em vigor para todos os dados que estejam especificamente previstos naquele artigo 4.º, n.º 1 (por exemplo para dados conservados relativos à localização celular).

IV. ENQUADRAMENTO JURÍDICO NA UNIÃO EUROPEIA E INTERNACIONAL

- **Âmbito da União Europeia**

A matéria relacionada com as comunicações eletrónicas é regida pelo Código Europeu das Comunicações Eletrónicas[26], adotado em novembro de 2018, que estabelece as

[26] Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas (reformulação)Texto relevante para efeitos do EEE. (europa.eu)

regras e objetivos comuns da União Europeia (UE) sobre a regulamentação do sector das telecomunicações e define como os prestadores de redes e/ou serviços podem ser regulamentados pelas autoridades nacionais. Nesta medida, pode ler-se no referido instrumento legal que «a presente diretiva cria um regime jurídico que assegura a liberdade de oferta de serviços e redes de comunicações eletrónicas, apenas sujeita às condições previstas na presente diretiva e a restrições de acordo com o artigo 52.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE), nomeadamente medidas relativas à ordem pública, à segurança pública e à saúde pública, e em consonância com o artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia» (considerando 5).

Este novo Código substituiu e revogou quatro das diretivas que integram o chamado «pacote telecomunicações», nomeadamente a Diretiva Autorização[27], a Diretiva Acesso[28], a Diretiva Serviço Universal[29] e a Diretiva-Quadro[30], de acordo com as orientações constantes do programa de simplificação legislativa REFIT[31], integrando-as num novo texto único.[32]

A Diretiva relativa à privacidade e às comunicações eletrónicas (Directiva 2002/58/CE)[33] também integra o pacote supra referido e «estabelece regras para garantir a segurança no que diz respeito ao tratamento de dados pessoais, à notificação da violação de dados pessoais e à confidencialidade das comunicações», e proíbe «as comunicações não solicitadas nos casos em que o utilizador não tenha dado o seu consentimento».

[27] EUR-Lex - 32002L0020 - EN - EUR-Lex (europa.eu)
[28] EUR-Lex - 32002L0019 - EN - EUR-Lex (europa.eu)
[29] EUR-Lex - 32002L0022 - EN - EUR-Lex (europa.eu)
[30] EUR-Lex - 32002L0021 - EN - EUR-Lex (europa.eu)
[31] REFIT – Tornar a legislação europeia mais simples e menos onerosa | Comissão Europeia (europa.eu)
[32] Através deste instrumento, procedeu-se, também, à revisão do Regulamento (UE) 2018/1971, que cria o Organismo de Reguladores Europeus das Comunicações Eletrónicas (ORECE)[32] e a Agência de Apoio ao ORECE (Gabinete ORECE), do Regulamento (CE) n.º 1211/2009[32] que cria o Organismo de Reguladores Europeus das Comunicações Eletrónicas (ORECE) e do Regulamento (UE) n.º 531/2012[32] relativo à itinerância nas redes de comunicações móveis públicas da União.
[33] EUR-Lex - 32002L0058 - EN - EUR-Lex (europa.eu)

Este instrumento foi alterado pela Directiva 2006/24/CE[34] 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Directiva 2002/58/CE, tendo , todavia, sido declarado inválido[35][36] pelo Tribunal de Justiça (TJUE), nos termos do Acórdão de 8 de abril de 2014, *Digital Rights Ireland Ltd e outros*, C-293/12 e C-594/12. Tal declaração teve por fundamento a violação do princípio da proporcionalidade pela restrição que a Diretiva opera dos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia. Em outubro de 2020, o TJUE proferiu os seus mais recentes acórdãos sobre a temática relacionada com conservação de dados e, para além de confirmar a proibição da conservação generalizada e indiscriminada de dados como princípio, estabeleceu uma série de exceções a esse princípio que os Estados-Membros pretendem agora explorar, tendo em conta o importante papel dos metadados das comunicações na preservação da segurança nacional, na imputação de crimes e na identificação de criminosos.

De referir ainda que o Grupo de Trabalho "*Proteção de dados*" criado pelo artigo 29.º da Diretiva n.º 95/46/CE, se pronunciara, através do Parecer n.º 3/2006, de 25 de março, sobre a Diretiva n.º 2006/24/CE, manifestando reservas relativamente às soluções nela consagradas. Com efeito, o parecer refere que "*as disposições da directiva terão implicações muito profundas para todos os cidadãos da Europa, bem como para a vida privada*", sendo "*susceptível de pôr em perigo os valores e as liberdades fundamentais de que gozam e beneficiam todos os cidadãos europeus*".

Por isso, o Grupo de Trabalho considerou "*extremamente importante que a directiva seja acompanhada e transposta em cada Estado-membro por medidas que limitem a sua incidência sobre a vida privada*", apresentando algumas sugestões no sentido de estabelecer garantias adequadas e específicas, nomeadamente em matéria de

[34] EUR-Lex - 32006L0024 - EN - EUR-Lex (europa.eu)
[35] CURIA - List of results (europa.eu)
[36] Adicionalmente, o TJUE proibiu, ainda, no âmbito dos processos Digital Rights Ireland (2014) e Tele2 (2016), a UE e os seus Estados-Membros de estabelecerem regras que impliquem a conservação de dados de forma geral e indiscriminada, estabelecendo limites ao regime de conservação de dados praticado até essa data, o que levou os Estados-Membros a alegar que a decisão do tribunal tornaria mais difícil a realização de investigações criminais eficazes.

finalidade, limitação do acesso, impossibilidade de extracção de dados, exame judicial, finalidade de conservação dos dados pelos fornecedores, separação dos sistemas e medidas de segurança.

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)[37], que se encontra em fase discussão no Conselho.

Neste contexto, a 11 de dezembro de 2020, o Parlamento Europeu adotou uma resolução sobre a «Estratégia da UE para a União da Segurança», na qual se pode ler que «apenas é permitida a conservação orientada de dados limitada a pessoas específicas ou a uma área geográfica específica; contudo, o Tribunal especificou que os endereços IP atribuídos à fonte de uma comunicação, podem ser sujeitos a uma conservação generalizada e indiscriminada para efeitos de combate a crimes graves e ameaças graves à segurança pública, sujeita a salvaguardas rigorosas».

Na reunião informal de 11 de março de 2021, os Ministros da Justiça «procederam a uma troca de pontos de vista sobre a conservação de dados de comunicações eletrónicas pelos prestadores de serviços, que podem revelá-los às autoridades policiais e judiciárias em certas condições estritas. Os ministros ponderaram, em especial, se se deveria adotar a nível da UE legislação para assegurar um regime jurídico harmonizado ou se a cooperação policial e judiciária se deverá basear exclusivamente no direito nacional em matéria de conservação de dados».

Na sequência da reunião informal de 25 de março de 2021, os membros do Conselho Europeu adotaram uma declaração, na qual se apela a «que se explore melhor o potencial dos dados e das tecnologias digitais, em benefício da sociedade, do ambiente e da economia, sem deixar de respeitar a proteção de dados, a privacidade e outros direitos fundamentais, e assegurando a conservação de dados necessária para que as

[37] A presente iniciativa foi escrutinada pela Assembleia da República.

autoridades policiais e judiciárias exerçam os seus poderes legais no combate à criminalidade grave».

De acordo com a comunicação «Estratégia da UE para lutar contra a criminalidade organizada (2021-2025)» de 14 de abril de 2021, a Comissão Europeia « analisará e delineará possíveis soluções, em consonância com os acórdãos do Tribunal, que satisfaçam as necessidades das autoridades responsáveis pela aplicação da lei e do sistema judiciário de uma forma que seja operacionalmente útil, tecnicamente possível e juridicamente sólida, o que inclui respeitar plenamente os direitos fundamentais». Mais se pode ler na referida comunicação que «Nos seus recentes acórdãos sobre a conservação de dados[38], o Tribunal de Justiça da União Europeia confirmou a sua jurisprudência anterior, segundo a qual os dados das comunicações eletrónicas são confidenciais e, em princípio, os dados de tráfego e de localização não podem ser conservados de forma generalizada e indiferenciada». Mais se previa no documento que, antes do final de junho de 2021, a Comissão Europeia consultaria os Estados-Membros visando definir os próximos passos.

- **Âmbito internacional**

Países analisados

Apresenta-se, de seguida, o enquadramento internacional referente a: Alemanha e Espanha.

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*[39] (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

[38] Acórdãos no processo C-623/17, *Privacy International*, e nos processos apensos C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e outros*, de 6 de outubro de 2020, e no processo C-746/18, *H.K./Prokuratuur*, de 2 de março de 2021.
[39] Diploma retirado do portal da imprensa oficial alemã (*Bundesgesetzblatt)*.

Telekommunikationsgesetz[40] (lei das telecomunicações) e o *Strafprocessordnung*[41] (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[42].

Em 2015 foi aprovada nova lei sobre conservação de dados das comunicações – a *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten*[43] *(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[44] 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[45] 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.

---

[40] 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 em 18/05/2022.

[41] Diploma consolidado na sua redação atual.

[42] A decisão pode ser consultada no portal do Tribunal Constitucional em https://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html.

[43] Diploma retirado do portal da imprensa oficial alemã (*Bundesgesetzblatt).*

[44] Na numeração atual; era o §113 aquando da aprovação da *VerkDSpG.*

[45] 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 da Internet 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 do Protocolo da Internet 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* [46](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 que a lei alemã é 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[47].

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

Também o *Bundesverwaltungsgericht* (Tribunal Administrativo Federal, que julga em última instânica) entendeu, a propósito da transposição da Diretiva *e-Privacy*[48], haver

[46] Para detalhes sobre a organização judiciária alemã, veja-se a síntese informativa «organização judiciária», elaborada pela DILP.
[47] 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.
[48] Directiva 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

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 que haja decisão deste[49].

Por outro lado, foram também apresentadas queixas por inconstitucionalidade junto do Tribunal Constitucional, cuja decisão também se aguarda.

Segundo notícias na comunicação social[50], o atual Ministro Federal da Justiça ter-se-á manifestado contrário ao armazenamento de dados de forma tão genérica, considerando preferível uma solução que passe pela conservação rápida de dados em casos específicos por ordem judicial, para que a polícia e o Ministério Público possam então avaliá-los, e apenas nos casos de suspeita da existência de crimes graves – um procedimento designado como «*Quick-Freeze*».

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*[51], 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, para identificar o destino de uma

[49] A fundamentação desta decisão do Tribunal Administrativo Federal encontra-se explicada nesta nota de imprensa no respetivo sítio da *internet.*
[50] De 21 de dezembro de 2021 - https://www.spiegel.de/netzwelt/netzpolitik/marco-buschmann-bundesjustizminister-will-vorratsdatenspeicherung-kippen-a-9de4fead-9873-4230-b342-7b19def9f425
[51] Diploma consolidado, na sua redação atual, retirado do portal oficial *boe.es*. Todas as referências relativas à legislação da Alemanha devem considerar-se remetidas para o referido portal, salvo indicação expressa em contrário. Consultas efetuadas a 20/05/2022.

comunicação, 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.
Em qualquer caso, está expressamente excluída a conservação do conteúdo de qualquer comunicação.
Por outro lado, prevê-se a necessidade de 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 terá feito por entender que estava estabelecido um controlo judicial eficaz e, portanto, os direitos humanos em causa não estavam limitados[52].

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* [53]

Contudo, nos processos em que a questão foi suscitada, o *Tribunal Supremo*[54] 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 o fins nela previstos e autorização judicial prévia', o que não constituía uma garantia imposta pela

[52] De acordo com notícia publicada pela *Asociacíon de Internautas*, organização sem fins lucrativos de defesa dos direitos dos utilizadores de telefone e internet.
[53] 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.
[54] Tribunal de última instância em todas as ordens jurisdicionais, com com exceção do previsto para as garantias constitucionais, que é competência do Tribunal Constitucional.

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 por isso idêntico nível de tutela, como são os consagrados no artigo 18.3 [da Constituição], interferência no conteúdo de conversas telefónicas e transmissão de dados de tráfego eletrónico 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 interferência em 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 infrações graves), acaba por considerar que «deve partir-se da premissa segundo a qual os dados em causa no processo principal foram conservados em conformidade com a legislação nacional, no respeito dos requisitos estabelecidos no artigo 15.º, n.º 1, da Diretiva 2002/58 (…)»[55].

[55] Recorde-se que aquele artigo da Diretiva 2002/58/CE (conhecida como Diretiva *e-Privacy*) prevê a possibilidade de os Estados-Membros adoptarem medidas legislativas para restringir o

Refra-se finalmente que se encontra em apreciação no Parlamento espanhol, apresentada pelo Governo, uma iniciativa tendente à aprovação de uma nova *Ley General de Telecomunicaciones*, que mantém a remissão para a LCD constante da *Ley General de Telecomunicaciones* atualmente em vigor (cfr. *artículo 61* do *Proyecto de Ley General de Telecomunicaciones*, cuja tramitação parlamentar pode ser consultada aqui, e o *artículo 42* da atual *Ley General de Telecomunicaciones*), 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 rege-se pelo disposto na LCD.

Organizações internacionais

CONSELHO DA EUROPA

O relatório *Data retention in the States Parties to the Budapest Convention on Cybercrime*, de setembro de 2020, dá nota dos resultados de um inquérito realizado aos Estados-Parte da Convenção sobre o Cibercrime relativamente à questão específica da retenção de dados.

A Convenção sobre o Cibercrime do Conselho da Europa, também conhecida como Convenção de Budapeste, vigora na ordem internacional desde 2004 (e em Portugal desde 2010, tendo sido aprovada[56] pela Resolução da Assembleia da República n.º 88/2009 e ratificada pelo Decreto do Presidente da República n.º 91/2009, ambos de 15

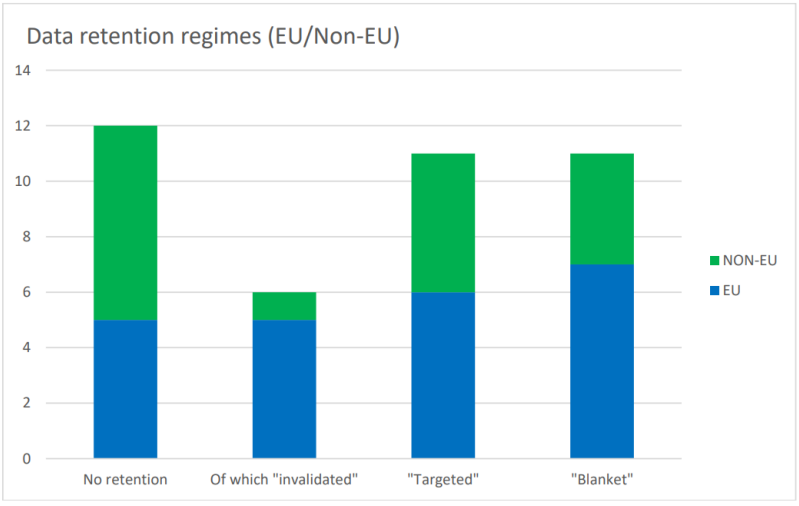
âmbito dos direitos e obrigações previstos na mesma diretiva «sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas (…) 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 (…)».

[56] Com reserva em matéria de extradição.

de setembro), constituindo o primeiro e mais relevante instrumento internacional no âmbito do combate ao cibercrime.

Esta Convenção preconiza a preservação de dados informáticos já existentes para fins de investigação criminal (*v.d.* o respetivo artigo 16.º), bem como a recolha, em tempo real, de dados de tráfego (cfr. artigo 20.º). Com o estudo referido, co-financiado pela União Europeia e pelo Conselho da Europa, pretendia-se recolher informação sobre a existência ou não de regras sobre retenção de dados (e, em caso afirmativo, com que alcance, se generalizada ou direccionada) nos Estados-Parte da Convenção, designadamente tendo em conta a invalidação da Diretiva 2006/24/CE (embora nem todos sejam membros de ambas ou mesmo uma das organizações promotoras do estudo).

Responderam 33 países, concluindo-se, entre outros aspetos, que, à data, cerca de dois terços dos Estados que responderam tinham prevista na respetiva legislação alguma forma de retenção de dados (tendo cinco Estados-Membros da União Europeia que previam a retenção de dados visto a respetiva legislação ser invalidada em consequência de decisões do TJUE), como se reflete no quadro abaixo.



Fonte: *Data retention in the States Parties to the Budapest Convention on Cybercrime*

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU)

Através da Resolução 74/247, de 21 de dezembro de 2019, a ONU determinou a constituição de uma comissão ad-hoc composta por peritos de todas as regiões do mundo com vista à preparação de uma convenção internacional abrangente sobre combate ao uso de tecnologias de informação e comunicação para fins criminais. Um projeto daquela que será a primeira convenção da ONU nesta matéria deverá ser apresentado a tempo de ser discutido na 78.ª Assembleia Geral (setembro de 2023 a setembro de 2024).

V. ENQUADRAMENTO PARLAMENTAR

- **Iniciativas pendentes (iniciativas legislativas e petições)**

Consultada a base de dados da Atividade Parlamentar (AP), verificou-se estarem em apreciação sobre a matéria, nesta data, as duas iniciativas objeto desta nota, as quais baixaram à Comissão de Assuntos Constitucionais, para além das seguintes, que foram apresentadas em 27 de maio, na presente data ainda sem baixa à Comissão:

- Proposta de Lei n.º 11/XV/1.ª (GOV) - Regula o acesso a metadados referentes a Comunicações Eletrónicas para fins de investigação criminal;
- Projeto de Lei n.º 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.

- **Antecedentes parlamentares (iniciativas legislativas e petições)**

Consultada a mesma base de dados, verifica-se que a Lei n.º 32/2008 teve origem na Proposta de Lei n.º 161/X/3.ª (GOV) - *Transpõe para a ordem jurídica interna a Directiva n.º 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações*, aprovado em votação final global, com votos a favor do PS, PSD, CDS-PP e contra do PCP, BE, PEV e Luísa Mesquita (Ninsc).

Esta Proposta de Lei baixara à Comissão de Obras Públicas, Transportes e Comunicações em 27 de setembro de 2017, tendo sido redistribuída, em 9 de novembro seguinte, à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias para emissão do respetivo parecer, por se tratar de matéria "*mais diretamente relacionada com a política de investigação criminal do que, propriamente com a política de comunicações*".

Duas das normas ora objeto de alteração – os artigos 4.º e 6.º - correspondem, na sua exata redação, às constantes da referida Proposta de Lei: o artigo 4.º não foi objeto de propostas de alteração e o artigo 6.º viu a proposta de alteração apresentada pelo Grupo Parlamentar do BE[57] rejeitada, com votos contra do PS e do PSD e votos a favor do PCP, registando-se as ausências do CDS-PP, do BE e do PEV.

O artigo 9.º - cuja alteração também é preconizada - foi objeto de diferentes propostas de alteração e corresponde, na sua redação:
- N.º 1: à proposta de substituição apresentada pelo Grupo Parlamentar do BE (em formulação alterada pelo Grupo Parlamentar do PS, no sentido de substituir o inciso final "dos crimes previstos na alínea *g)* do n.º 1 do artigo 2.º." pela expressão "de crimes graves";
- N.os 2, 3 e 5: ao texto da Proposta de Lei;
- N.os 4 e 6: às propostas de substituição apresentadas pelo Grupo Parlamentar do PSD.

Dos trabalhos preparatórios da Lei é possível retirar, com relevância para a apreciação destas iniciativas, o que a seguir se consigna.

Na exposição de motivos da Proposta de Lei n.º 161/X, o proponente Governo explicitava: "*A presente proposta de lei reconhece a sensibilidade dos valores em presença e da conservação dos dados em causa. Por essa razão, são adotadas especiais restrições, cautelas e medidas de segurança em sede de acesso e tratamento dos dados e de supervisão e fiscalização do cumprimento das obrigações aqui previstas*", especificando, designadamente, que "*o acesso aos dados apenas pode ser*

[57] A proposta do GP do BE era do seguinte teor: "*As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de* ***seis meses*** *a contar da data da conclusão da comunicação.*"

solicitado pelo Ministério Público ou por certas autoridades de polícia criminal e depende sempre da decisão do juiz (...). Por outro lado, o acesso aos dados é limitado ao adequado, necessário e proporcional face ao caso concreto." E acrescentava que "*os dados em causa não podem ser conservados eternamente. Estabelece-se que o período de conservação é de um ano, que corresponde a metade do período de conservação máximo permitido pela Diretiva que agora se transpõe."*

No final, mencionava-se que "*Foram ouvidos o Conselho Superior da Magistratura, o Conselho Superior do Ministério Público, a Ordem dos Advogados, a Comissão Nacional de Proteção de Dados e o Instituto de Comunicações de Portugal - Autoridade Nacional das Comunicações."* Não foram, no entanto, remetidas à Assembleia da República quaisquer cópias de pareceres ou contributos resultantes das audições indicadas na exposição de motivos.

Destacava o parecer da Comissão da Assuntos Constitucionais sobre esta iniciativa legislativa, no que se refere ao seu enquadramento constitucional, que "Nos termos do disposto no artigo 26.º, n.ºs 1 e 2, da Constituição da República Portuguesa (CRP) a todos é reconhecido o direito '*à palavra' e 'à reserva da intimidade da vida privada e familiar*', sendo que a '*lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias*'. E ainda: "Por seu turno, o artigo 34.º, n.ºs 1 e 4, da CRP dispõe que '*o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis*' e que '*É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação social, salvo nos casos previstos na lei em matéria de processo penal.',* acrescentando a referência ao "artigo 35.º da Lei Fundamental, que consagra a protecção dos cidadãos perante o tratamento de dados pessoais informatizados". E concluía: "Estamos, pois, no domínio dos direitos, liberdades e garantias, cuja restrição está, portanto, sujeita aos princípios jurídico-constitucionais referidos no artigo 18.º, designadamente os princípios da necessidade, da adequação e da proporcionalidade."

De referir que, nas conclusões da sua pronúncia escrita sobre a Proposta de Lei n.º 161/X, emitida a pedido da CACDLG, a Comissão Nacional de Proteção de Dados

(CNPD)[58] indicava que "*Constituindo um facto a publicação da Diretiva 2006/24/CE – apesar das objeções oportunamente apesentadas pelo Grupo de Trabalho do Artigo 29.º -, afigura-se correto, no essencial, o modo como através da Proposta de Lei n.º 161/X/3.ª se intenta transpô-la.*

Considera-se ajustado, designadamente, o prazo anual de retenção de dados previsto, bem como a precisão que nela se faz quanto à caracterização dos crimes a que se reporta.
Reitera-se, nessa medida, o parecer positivo emitido, na generalidade, em relação à última versão do respetivo anteprojeto." [59]

Da discussão na generalidade desta iniciativa, ocorrida na sessão plenária de 4 de janeiro de 2008 [*vd*. *DAR I série N.º 31/ X/ 3 2008-01-05 (Pág. 19-26)*] permitimo-nos destacar, por se reportarem especificamente à matéria em apreço, as intervenções do Senhor Secretário de Estado da Justiça (João Tiago Silveira) e dos Senhores Deputados Nuno Teixeira de Melo (CDS-PP), Fernando Negrão (PSD), Vítor Pereira (PS), António Filipe (PCP) e Helena Pinto (BE).

Na generalidade, a Proposta de Lei n.º 161/X/3.ª foi aprovada, com votos a favor do PS, do PSD e do CDS-PP e votos contra do PCP, do BE, do PEV e da Deputada Luísa Mesquita (Ninsc).

Para a preparação da respetiva discussão e votação na especialidade, a Comissão de Assuntos constitucionais constituiu um Grupo de Trabalho, que integrou os Senhores Deputados Vítor Pereira (PS), que coordenou, Luís Pais Antunes (PSD), Nuno Melo (CDS-PP), António Filipe (PCP) e as Senhoras Deputadas Helena Pinto (BE) e Heloísa Apolónia (PEV).

O Grupo de Trabalho recebeu em audiência a APRITEL – Associação dos Operadores de Telecomunicações, e o Sindicato dos Jornalistas, em 6 de maio de 2008, e procedeu

[58] Parecer n.º 61/2007, de 20 de dezembro de 2007.
[59] Refere a CNPD que "Esta Comissão teve já oportunidade de se pronunciar – no parecer n.º 38/07, de 16 de julho de 2007 – sobre o inicial Anteprojeto de Proposta de Lei de transposição da Diretiva em causa. O Governo veio a elaborar novo Anteprojeto da Proposta de Lei de transposição, no qual atendeu à generalidade das observações suscitadas pela CNPD – o que esta de resto reconheceu no seu parecer 47/07, de 29 de agosto de 2017 (ratificado por deliberação n.º 39/07, de 17 de setembro de 2007)."

à discussão e votação indiciárias de todos os artigos da Proposta de Lei e respetivas propostas de alteração, votações que foram ratificadas na reunião da Comissão de 21 de maio de 2008, registando-se as ausências do BE e do PEV.

O contributo escrito do Sindicato dos Jornalistas, enviado em 22 de novembro de 2007 à Comissão de Assuntos Constitucionais, dava nota de que o conteúdo da Proposta de Lei poderia "*contender com direitos e garantias dos jornalistas protegidos pela CRP e pelo Estatuto do Jornalista, mormente a garantia do sigilo profissional, designadamente quanto à confidencialidade das fontes de informação*", considerando que era "*evidente o risco de comunicações efetuadas ou recebidas por jornalistas no exercício da sua profissão (…) virem a cair indiscriminadamente na alçada da investigação de autoridades sem a adequada proteção*", razão pela qual apresentava "*as seguintes alternativas de redação para o artigo 9.º da referida Proposta de Lei:*

1 – A transmissão de dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz, quando tal se mostre necessário à investigação, detecção e repressão de crimes graves e não ponha em causa o sigilo profissional dos jornalistas.

2 – Os fornecedores de serviços de comunicações electrónicas ou de uma rede pública de comunicações ficam impedidos de fornecer quaisquer dados quando o assinante for uma empresa de comunicação social ou o nome e/ou o nome do utilizador registado constar na lista oficial de jornalistas disponível no site da Comissão da Carteira Profissional de Jornalistas que, para o efeito, deve ser consultada.
3 – redacção do n.º 2
3 – redacção do n.º 3
4 – redacção do n.º 4
5 – redação do n.º 5
6 – redacção do n.º 6."

Em 6 de maio de 2008, em pronúncia escrita complementar à audiência que requereu à Comissão, essa mesma entidade apresentou "*uma versão alternativa para o texto do n.º 2 do artigo 9.º então proposto pelo Sindicato dos Jornalistas:*
1 - …

2 – Antes de proferir o despacho referido no n.º 1 do presente artigo, o juiz toma conhecimento do nome da pessoa ou entidade que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido, após o que promove a consulta à lista oficial dos jornalistas disponível no sítio electrónico da Comissão da Carteira Profissional de Jornalista e, se essa pessoa for jornalista, é notificada para, querendo, dizer se a comunicação em causa está sob protecção do sigilo profissional, caso em que se observará o disposto nos artigos 135.º do Código de Processo Penal e 11.º do Estatuto do Jornalista.

3 – Se tomar conhecimento de que a entidade titular do suporte de comunicação usado para transmitir ou receber mensagens de suspeito ou arguido é uma entidade colectiva titular de um órgão de informação, o juiz manda notificar esta para que informe se a comunicação em causa envolve ou não um jornalista, seguindo-se, em caso afirmativo, o procedimento previsto no número anterior.

(…)"

Para além da já referida proposta de alteração apresentada pelo BE para o artigo 6.º, que foi rejeitada (tendo o Deputado Vítor Pereira (PS) recordado que o prazo de conservação de um ano, contante da Proposta de Lei, era o que vigorava em ordenamentos próximos como os de Espanha e Itália, para além de se tratar do mesmo prazo do direito de queixa), cumpre recordar a proposta de alteração apresentada pelo Grupo Parlamentar do BE para o artigo 9.º da Proposta de Lei (que foi rejeitada, aprovação parcial da redação proposta para o n.º 1):

Artigo 9.º

Transmissão de dados

1 – A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz **de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão dos crimes previstos na alínea *g)* do n.º 1 do artigo 2.º.**

2 — A transmissão dos dados referentes às categorias previstas no artigo 4.º não pode, quer directa, quer indirectamente, colocar em causa, qualquer vertente ou conteúdo do segredo profissional, de funcionário, ou de Estado dos envolvidos

3 – Caso os dados a transmitir se refiram, directa ou indirectamente, a pessoas que estejam abrangidas pelo segredo profissional, de funcionário, ou de Estado, devem observar-se previamente os requisitos para a eventual quebra desse segredo, tal como previstos no Código de Processo Penal ou em legislação específica.

4 – Os fornecedores de serviços de comunicações electrónicas ou de uma rede pública de comunicações ficam impedidos de fornecer quaisquer dados quando o assinante for uma empresa de comunicação social ou o nome e/ou o nome do utilizador registado constar na lista oficial de jornalistas disponível no site da Comissão da Carteira Profissional de Jornalistas que, para o efeito, deve ser consultada.

5 – A autorização prevista no n.º 1 só pode ser requerida pelo Ministério Público, de forma fundamentada e indicando expressamente quais as categorias de dados a transmitir.

6 – Anterior n.º 3

a) (...);

b) Eliminado

c) (...).

7 – Anterior n.º 4.

8 – Anterior n.º 5.

9 – Anterior n.º 6

10 – À transmissão de dados prevista no presente diploma aplica-se o regime legal das escutas telefónicas.

Do mesmo modo, recorda-se que a proposta de alteração apresentada pelo Grupo Parlamentar do PCP para o mesmo artigo 9.º (que foi retirada pelo proponente), era a seguinte:

"Artigo 9.º

Transmissão de dados

1 – A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz, quando tal se mostre necessário à investigação, detecção e repressão de crimes graves **e não ponha em causa o segredo profissional de funcionários ou dos jornalistas.**

2 – (...).

3 – (...).

4 – (...).

5 – Quando os dados solicitados forem referentes a empresas de comunicação social ou jornalistas constantes da lista oficial disponibilizada pela Comissão da Carteira Profissional dos Jornalistas que, para o efeito, deve ser consultada, o juiz deve tomar as medidas adequadas à salvaguarda do sigilo profissional, observando, com as devidas adaptações, o disposto no artigo 135.º do Código de Processo Penal e 11.º do Estatuto dos jornalistas.

6 – (Actual n.º 5 da PPL).

7– (Actual n.º 6 da PPL).”

Em votação final global, o texto final apresentado pela Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias foi aprovado, com votos a favor do PS, do PSD e do CDS-PP e votos contra do PCP, do BE, do PEV e da Deputada Luísa Mesquita (Ninsc.)

Esta Lei foi recentemente objeto de alteração pela Lei n.º 79/2021, de 24.11 - *Transpõe a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, alterando o Código Penal, o Código de Processo Penal, a Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, e outros atos legislativos*, com origem na Proposta de Lei n.º 98/XIV/2.ª (GOV), a qual foi aprovada em votação final global com votos a favor de PS, PSD, PAN, IL, Cristina Rodrigues (Ninsc), Joacine Katar Moreira (Ninsc) e as abstenções de BE, PCP, CDS-PP, PEV, CH. Esta alteração incidiu apenas, no que releva para a apreciação das iniciativas ora em apreço, na alteração da definição de ‘crime grave’, prevista na alínea *g)* do n.º 1, do artigo 2.º.

VI. CONSULTAS E CONTRIBUTOS

- **Consultas obrigatórias e facultativas**

Quando se proceder à distribuição das iniciativas e nomeação do respetivo relator, a Comissão poderá promover a consulta escrita do Conselho Superior da Magistratura, do Conselho Superior do Ministério Público e da Ordem dos Advogados e, bem asism, da Comissão Nacional de Proteção de Dados, atenta a matéria objeto de alteração.

A serem solicitados e emitidos, os pareceres serão disponibilizados no *site* da Assembleia da República nas páginas eletrónicas das duas iniciativas (PJL 70 e PJL 79).

VII. AVALIAÇÃO PRÉVIA DE IMPACTO

- **Avaliação sobre impacto de género**

O preenchimento, pelos proponentes, das fichas de avaliação prévia de impacto de género (PJL 70 e PJL 79) da presente iniciativa, em cumprimento do disposto na Lei n.º 4/2018, de 9 de fevereiro, devolve como resultado uma valoração neutra do impacto de género.

VIII. ENQUADRAMENTO BIBLIOGRÁFICO

FERREIRA, Pedro – A retenção de dados pessoais nas comunicações electrónicas. In **Estudos comemorativos dos 10 anos da Faculdade de Direito da Universidade Nova de Lisboa** [Em linha]. Coimbra : Almedina, 2008. ISBN 978-972-40-3426-3. V. 2, p. 417-447. [Consult. 17 mai. 2022]. Disponível na internat da AR em: <URL: https://catalogobib.parlamento.pt:82/images/winlibimg.aspx?skey=&doc=120879&img=28350&save=true>.

Resumo: Como se lê neste artigo, «a entrada em vigor da Directiva 2006/24/CE inicia uma nova abordagem aos direitos fundamentais suscitada pela Sociedade de Comunicação: passa a vigorar um quadro jurídico que legitima a vigilância generalizada da "vida digital" e avança-se para um novo balanceamento entre o direito à protecção de dados pessoais e o direito à segurança, com preferência deste último», no que se considera ser a «resposta legislativa à nova criminalidade». Considerando que «a

conservação de dados de comunicações com o objectivo de reprimir crimes graves não tem precedentes e terá uma importância histórica», são apresentados os vários pontos críticos da Diretiva, salientando-se os principais cuidados e reservas a ter na sua transposição para a legislação nacional. Para o autor, «a primeira pergunta que se coloca é se a comunidade aceita o balanceamento, não somente na sua construção legislativa, mas sobretudo nas consequências a médio e longo prazo. Até que ponto as sociedades democráticas conseguem conviver com regimes de excepção que, a pouco e pouco, em nome da defesa dessa mesma democracia, vão escavando em redor dos alicerces dos direitos fundamentais e das garantias que lhe dão sustentação.»

GUERRA, Clara ; CALVÃO, Filipa Urbano – Anotação [ao Acórdão do Tribunal de Justiça (Grande Secção), 8 de abril de 2014]. **Fórum de Proteção de Dados** [Em linha]. Nº 1 (jul. 2015), p. 77-80. [Consult. 25 mai. 2022]. Disponível em WWW: <URL: https://catalogobib.parlamento.pt:82/images/winlibimg.aspx?skey=&doc=139531&img=28240 >.

Resumo: As autoras procuram aferir a conformidade da Lei n.º 32/2008 com o Direito da União Europeia, com base nos fundamentos expostos no acórdão do Tribunal de Justiça da União Europeia em relação às várias disposições da Diretiva 2006/24/CE e verificando se todos ou alguns deles se justificam quanto às normas da Lei portuguesa. Concluem que «a Lei n.º 32/2008 contém normas que preveem a restrição ou ingerência nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais (artigos 7.º e 8.º da Carta dos Direitos Fundamentais da UE) com grande amplitude e intensidade em clara violação do princípio da proporcionalidade.» Acrescentam que «a idêntica conclusão se chega se o padrão de avaliação for a Constituição da República Portuguesa: com os mesmos fundamentos, verifica-se uma restrição desproporcionada dos direitos à reserva da intimidade da vida privada e à proteção de dados pessoais, em violação do disposto no n.º 2 do artigo 18.º da Constituição.»

PINHO, Carlos – Lei de retenção de dados de comunicações electrónicas : aposentar ou reformar?. **Revista do Ministério Público** [Em linha]. Nº 154 (abr./jun. 2018), p. 167-192. [Consult. 16 mai. 2022]. Disponível em WWW: <URL: https://catalogobib.parlamento.pt:82/images/winlibimg.aspx?skey=&doc=125457&img=28292&save=true>.

Resumo: Este artigo de Carlos Pinho, Procurador-adjunto do Ministério Público, pretende avaliar a pertinência da Lei n.º 32/2008 no ordenamento jurídico nacional, a necessidade da sua reforma e em que sentidos deve essa mesma reforma apontar. Descreve brevemente o regime derivado desta lei e algumas questões levantadas quanto à sua inserção no ordenamento jurídico português. Analisa os argumentos que levaram à decisão de invalidade pelo Tribunal de Justiça da União Europeia, centrando-se na questão do princípio da proporcionalidade e no problema da obrigação de conservação e da transterritorialidade dos dados gerados no âmbito de comunicações eletrónicas. Aborda ainda o impacto derivado da entrada em vigor do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, retificado em 23 de Maio de 2018: o Regulamento Geral de Proteção de Dados. Conclui com uma síntese de propostas de reforma da Lei n.º 32/2008.

PORTUGAL. Centro Nacional de Cibersegurança. Observatório de Cibersegurança – **Relatório cibersegurança em Portugal** [Em linha] : **Ética & Direito**. Lisboa : CNCS, 2020. [Consult. 16 mai. 2022]. Disponível em WWW: <URL: https://catalogobib.parlamento.pt:82/images/winlibimg.aspx?skey=&doc=137836&img=26439&save=true>.

Resumo: O presente Relatório analisa os principais problemas éticos e jurídicos associados à (in)segurança no ciberespaço e as soluções que têm vindo a ser adotadas a nível internacional e nacional para resolver ou minorar estes problemas. A análise é dividida em três capítulos, incidindo sucessivamente sobre os desafios ético-morais, a genealogia legal e a aplicação prática do quadro normativo. Como instrumento legal fundamental neste domínio, a Lei n.º 32/2008 é analisada nesses três vetores, sendo salientadas as dúvidas que suscita na jurisprudência e na doutrina portuguesas, quer em torno da sua constitucionalidade, quer da conformidade com o Direito da União Europeia.

RAMALHO, David Silva ; COIMBRA, José Duarte – A declaração de invalidade da Diretiva 2006/24/CE : presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves. **O Direito** [Em linha]. A. 147, nº 4 (2015), p. 997-1045. [Consult. 16 mai. 2022] Disponível em WWW: <URL:

https://catalogobib.parlamento.pt:82/images/winlibimg.aspx?skey=&doc=119627&img=28291&save=true>

Resumo: O artigo analisa, no seu teor, efeitos e implicações, o Acórdão Digital Rights Ireland, do Tribunal de Justiça da União Europeia, que declarou inválida, em 8 de abril de 2014, a Diretiva 2006/24/CE. Os autores perspetivam o tema à luz do «equilíbrio entre, por um lado, o respeito pelo direito à reserva da intimidade da vida privada e à proteção dos dados pessoais e, por outro, a necessidade de conservação de alguns desses dados para fins de prevenção, investigação e repressão criminal», equilíbrio que «tem sido particularmente dificil de alcançar devido à oscilação periódica da prevalência atribuida a cada um desses conjuntos de interesses por parte do legislador e da opinião pública.» A Diretiva surgiu na sequência dos atentados terroristas de 2001, 2004 e 2005, e já depois de vários Estados-Membros terem criado, autonomamente, «legislação destinada a permitir ou impor a conservação de dados de tráfego e/ou localização por parte de fornecedores de serviços, precisamente para fins de prevenção, investigação, deteção e repressão de infrações penais». A contestação ao texto da Diretiva precedeu a sua entrada em vigor, e «intensificou-se durante o seu período de vigência, primeiro com a impugnação da respetiva base jurídica junto do TJ, depois com a resistência de alguns Estados-Membros em transpô-la a tempo ou de forma completa, e, por fim, com as sucessivas declarações de inconstitucionalidade, total ou parcial, das suas leis de transposição.» No caso de transposição para a legislação nacional, na Lei n.º 32/2008, ainda que os autores considerem que «num louvável – e, de resto, incomum – exercício de transposição crítica da Diretiva, o legislador português antecipou a generalidade das omissões e insuficiências agora identificadas pelo TJ no texto comunitário e criou um diploma significativarnente mais exigente», a mesma «não escapa ao principal fundamento aduzido pelo TJ para invalidar a Diretiva».

Anexo

Quadro comparativo

Lei n.º 32/2008	Projeto de Lei n.º 70/XV	Projeto de Lei n.º 79/XV
	Artigo 1.º **Objeto** A presente lei 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.	**Artigo 1.º** **Objeto** A presente Lei procede à alteração Lei n.º 32/2008, de 17 de julho, que aprova a Conservação de Dados Gerados ou Tratados no Contexto de oferta de Serviços de Comunicações Eletrónicas, por forma a harmonizá-la com os preceitos constitucionais em vigor.
	Artigo 2.º **Alteração à Lei n.º 32/2008, de 17 de julho** Os artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho, alterada pela Lei n.º 79/2021, de 24 de	**Artigo 2.º** **Alteração à Lei n.º 32/2008, de 17 de julho** São alterados os artigos 3.º, 4.º, 6.º, 7.º, 9.º e 13.º, Lei n.º 32/2008, de 17 de julho, alterada pela Lei n.º

	novembro, passam a ter a seguinte redação:	79/2021, de 24 de novembro, os quais passam a ter a seguinte redação:
Artigo 3.º Finalidade do tratamento 1 - A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes. 2 - A transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º 3 - Os ficheiros destinados à conservação de dados no âmbito da presente lei têm que, obrigatoriamente, estar separados de quaisquer outros ficheiros para outros fins. 4 - O titular dos dados não pode opor-se à respectiva conservação e transmissão.		«Artigo 3.º (…) 1 – (…). 2 – (…). 3 – (…). 4 - O titular dos dados não pode opor-se à respectiva conservação e transmissão, **desde que esta ocorra no estrito cumprimento da lei.**
Artigo 4.º	«Artigo 4.º	Artigo 4.º

Categorias de dados a conservar 1 - Os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar as seguintes categorias de dados: a) Dados necessários para encontrar e identificar a fonte de uma comunicação; b) Dados necessários para encontrar e identificar o destino de uma comunicação; c) Dados necessários para identificar a data, a hora e a duração de uma comunicação; d) Dados necessários para identificar o tipo de comunicação; e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento; f) Dados necessários para identificar a localização do	[…] 1 – Os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar**, em Portugal ou em outro Estado-Membro da União Europeia,** as seguintes categorias de dados: a) […]; b) […]; c) […]; d) […]; e) […]; f) […]; 2 – […]. 3 – […]. 4 – […]. 5 – […]. 6 – […]. 7 – […].	(…) 1 - Os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar, **em território na União Europeia**, as seguintes categorias de dados: a) Dados necessários para encontrar e identificar a fonte de uma comunicação; b) Dados necessários para encontrar e identificar o destino de uma comunicação; c) Dados necessários para identificar a data, a hora e a duração de uma comunicação; d) Dados necessários para identificar o tipo de comunicação; e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento; **f) Revogado.**

equipamento de comunicação móvel. 2 - Para os efeitos do disposto na alínea a) do número anterior, os dados necessários para encontrar e identificar a fonte de uma comunicação são os seguintes: a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel: i) O número de telefone de origem; ii) O nome e endereço do assinante ou do utilizador registado; b) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet: i) Os códigos de identificação atribuídos ao utilizador; ii) O código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública; iii) O nome e o endereço do assinante ou do utilizador registado, a quem o endereço do		2 – (…). 3 – (…). 4 – (…). 5 – (…). 6 – (…). 7 – **Os dados relativos à identificação da localização do equipamento de comunicação móvel não podem ser conservados de forma generalizada, mas somente após despacho fundamentado de juiz, relativo a pessoa concreta e com efeitos para o futuro.** **8 – Para os efeitos do disposto no número que antecede, os dados necessários para identificar a localização do equipamento de comunicação móvel são os seguintes:** **a) O identificador da célula no início da comunicação;** **b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respetivos**

protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação. 3 - Para os efeitos do disposto na alínea b) do n.º 1, os dados necessários para encontrar e identificar o destino de uma comunicação são os seguintes: a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel: i) Os números marcados e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada; ii) O nome e o endereço do assinante, ou do utilizador registado; b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:		**identificadores de célula durante o período em que se procede à conservação de dados.**

i) O código de identificação do utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da Internet; ii) Os nomes e os endereços dos subscritores, ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação. 4 - Para os efeitos do disposto na alínea c) do n.º 1, os dados necessários para identificar a data, a hora e a duração de uma comunicação são os seguintes: a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação; b) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:		

i) A data e a hora do início (log in) e do fim (log off) da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado; ii) A data e a hora do início e do fim da ligação ao serviço de correio electrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário. 5 - Para os efeitos do disposto na alínea d) do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes: a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, o serviço telefónico utilizado;		

b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet, o serviço de Internet utilizado. 6 - Para os efeitos do disposto na alínea e) do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, são os seguintes: a) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino; b) No que diz respeito às comunicações telefónicas na rede móvel: i) Os números de telefone de origem e de destino; ii) A Identidade Internacional de Assinante Móvel (International Mobile Subscriber Identity, ou IMSI) de quem telefona;		

iii) A Identidade Internacional do Equipamento Móvel (International Mobile Equipment Identity, ou IMEI) de quem telefona; iv) A IMSI do destinatário do telefonema; v) A IMEI do destinatário do telefonema; vi) No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da activação inicial do serviço e o identificador da célula a partir da qual o serviço foi activado; c) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet: i) O número de telefone que solicita o acesso por linha telefónica; ii) A linha de assinante digital (digital subscriber line, ou DSL), ou qualquer outro identificador terminal do autor da comunicação. 7 - Para os efeitos do disposto na alínea f) do n.º		

1, os dados necessários para identificar a localização do equipamento de comunicação móvel são os seguintes: a) O identificador da célula no início da comunicação; b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respectivos identificadores de célula durante o período em que se procede à conservação de dados.		
Artigo 6.º Período de conservação As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação.	Artigo 6.º […] **1 – Sem prejuízo do disposto no número seguinte,** as entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação. **2 – Os dados de tráfego e de localização são conservados pelas entidades referidas no**	Artigo 6.º Período **e local de armazenamento** 1 - As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de **seis meses** a contar da data da conclusão da comunicação, **sem prejuízo do disposto no número 7, do mesmo artigo, no que diz respeito aos dados de identificação do**

	n.º 1 do artigo 4.º pelo período de 12 semanas a contar da data da conclusão da comunicação.	**equipamento de comunicação móvel.** **2 – Os dados devem ser armazenados em local compatível com o exercício das garantias constitucionais de proteção e com a intervenção da CNPD.**
Artigo 7.º Proteção e segurança dos dados 1 - As entidades referidas no n.º 1 do artigo 4.º devem: a) Conservar os dados referentes às categorias previstas no artigo 4.º por forma a que possam ser transmitidos imediatamente, mediante despacho fundamentado do juiz, às autoridades competentes; b) Garantir que os dados conservados sejam da mesma qualidade e estejam sujeitos à mesma protecção e segurança que os dados na rede; c) Tomar as medidas técnicas e organizativas		Artigo 7.º (…) 1 - As entidades referidas no n.º 1 do artigo 4.º devem: a) (…); b) (…); c) (…); d) (…); e) (…); f) Destruir **imediatamente** os dados que tenham sido preservados, quando tal lhe seja determinado por ordem do juiz; 2 – (…). 3 – (…). 4 – (…). 5 – (…).

adequadas à protecção dos dados previstos no artigo 4.º contra a destruição acidental ou ilícita, a perda ou a alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito; d) Tomar as medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados referentes às categorias previstas no artigo 4.º; e) Destruir os dados no final do período de conservação, excepto os dados que tenham sido preservados por ordem do juiz; f) Destruir os dados que tenham sido preservados, quando tal lhe seja determinado por ordem do juiz. 2 - Os dados referentes às categorias previstas no artigo 4.º, com excepção dos dados relativos ao		

nome e endereço dos assinantes, devem permanecer bloqueados desde o início da sua conservação, só sendo alvo de desbloqueio para efeitos de transmissão, nos termos da presente lei, às autoridades competentes. 3 - A transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação electrónica, nos termos das condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, que devem observar um grau de codificação e protecção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados.		

4 - O disposto nos números anteriores não prejudica a observação dos princípios nem o cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados, previstos nas Leis n.os 67/98, de 26 de Outubro, e 41/2004, de 18 de Agosto. 5 - A autoridade pública competente para o controlo da aplicação do disposto no presente artigo é a Comissão Nacional de Protecção de Dados (CNPD).		
Artigo 9.º Transmissão dos dados 1 - A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova	Artigo 9.º […] 1 – […]. 2 – […]. 3 – […]. 4 – […]. 5 – […]. 7 – […].	Artigo 9.º (…) 1 – A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz de instrução**, onde este admite a transmissão apenas na medida do estritamente necessário para as finalidades que**

seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves. 2 - A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente. 3 - Só pode ser autorizada a transmissão de dados relativos: a) Ao suspeito ou arguido; b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou c) A vítima de crime, mediante o respectivo consentimento, efectivo ou presumido. 4 - A decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade,		**visa alcançar e** se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves. 2 - (…). 3 - (…). 4 - (…). 5 - (…). 6 - (…).

designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à protecção do segredo profissional, nos termos legalmente previstos. 5 - O disposto nos números anteriores não prejudica a obtenção de dados sobre a localização celular necessários para afastar perigo para a vida ou de ofensa à integridade física grave, nos termos do artigo 252.º-A do Código de Processo Penal. 6 - As entidades referidas no n.º 1 do artigo 4.º devem elaborar registos da extracção dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD.	**7 – As entidades referidas no n.º 1 do artigo 4.º notificam o titular dos dados de qualquer transmissão dos dados referentes às categorias previstas no artigo 4.º, a partir do**	7 - **As autoridades competentes devem informar imediatamente os titulares dos dados a que tenham acedido, a partir do momento em que essa comunicação**

	momento em que essa comunicação não seja suscetível de comprometer a investigação criminal ou de constituir risco para a integridade física ou vida de terceiros. **8 – Para efeitos do cumprimento da obrigação prevista no número anterior, compete ao juiz de instrução que autorizou a transmissão dos dados informar o fornecedor de serviços de comunicações eletrónicas transmitente dos dados do momento a partir do qual a comunicação a que se refere o número anterior não é suscetível de comprometer a investigação criminal ou de constituir risco para a integridade física ou vida de terceiros.** **9 – É proibida a transmissão dos dados referentes às categorias previstas no artigo 4.º a**	**não seja suscetível de comprometer as investigações levadas a cabo por essas autoridades.**

	autoridades judiciárias e autoridades de polícia criminal de Estado que não seja membro da União Europeia.»	
Artigo 13.º Crimes 1 - Constituem crime, punido com pena de prisão até dois anos ou multa até 240 dias: a) O incumprimento de qualquer das regras relativas à protecção e à segurança dos dados previstas no artigo 7.º; b) O não bloqueio dos dados, nos termos previstos no n.º 2 do artigo 7.º; c) O acesso aos dados por pessoa não especialmente autorizada nos termos do n.º 1 do artigo 8.º. 2 - A pena é agravada para o dobro dos seus limites quando o crime: a) For cometido através de violação de regras		Artigo 13.º (…) 1 - Constituem crime, punido com pena de prisão até dois anos ou multa até 240 dias: a) (…); b) (…); c) (…); d) **A conservação dos dados por período mais longo que o definido no artigo 6.º.** 2 – (…). 3 – (…).»

técnicas de segurança; b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais; ou c) Tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial. 3 - A tentativa e a negligência são puníveis.		
	Artigo 3.º **Norma transitória** 1 - A presente lei aplica-se imediatamente, também aos dados que no momento da sua entrada em vigor estejam a ser conservados pelas entidades referidas no n.º 1 do artigo 4.º. 2 – Em processos pendentes e em que já tenha sido deduzida acusação no momento da entrada em vigor presente lei, é lícita a utilização como meio de prova de dados de tráfego e de localização que tenham sido conservados pelas entidades referidas no n.º 1 do artigo 4.º por prazo superior ao indicado no n.º	

	2 do artigo 6.º da Lei n.º 32/2008, de 17 de julho, na redação introduzida pela presente lei, desde que inferior a um ano.	
	Artigo 4.º **Entrada em vigor** A presente lei entra em vigor no dia seguinte ao da sua publicação.	**Artigo 3.º** **Entrada em vigor** A presente Lei entra em vigor no dia seguinte à sua publicação.