CONSELHO DA UNIÃO EUROPEIA

Bruxelas, 19 de Abril de 2011 (02.05)
(OR. en)

9324/11

DAPIX 38
TELECOM 47
COPEN 85

NOTA DE ENVIO

Origem:	Secretário-Geral da Comissão Europeia, assinado por Jordi AYET PUIGARNAU, Director
Data de recepção:	18 de Abril de 2011
Destinatário:	Pierre de BOISSIEU, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	COM(2011) 225 final
Assunto:	Relatório da Comissão ao Conselho e ao Parlamento Europeu – Relatório de Avaliação sobre a Directiva relativa à conservação de dados (2006/24/CE)

Envia-se em anexo, à atenção das delegações, o documento da Comissão – COM(2011) 225 final.

Anexo: COM(2011) 225 final

COMISSÃO EUROPEIA

Bruxelas, 18.4.2011
COM(2011) 225 final

RELATÓRIO DA COMISSÃO AO CONSELHO E AO PARLAMENTO EUROPEU

Relatório de Avaliação sobre a Directiva relativa à conservação de dados (2006/24/CE)

RELATÓRIO DA COMISSÃO AO CONSELHO E AO PARLAMENTO EUROPEU

Relatório de Avaliação sobre a Directiva relativa à conservação de dados (2006/24/CE)

1. INTRODUÇÃO

A Directiva relativa à conservação de dados[1] (a seguir designada por «Directiva»), exige que os Estados-Membros obriguem os prestadores de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações (a seguir designados por «operadores») a conservarem os dados relativos ao tráfego e os dados de localização durante um período que pode ir de seis meses a dois anos, para efeitos de investigação, detecção e repressão de crimes graves.

O presente relatório da Comissão avalia, em conformidade com o disposto no artigo 14.º da Directiva, a sua aplicação pelos Estados-Membros e os seus efeitos nos operadores económicos e nos consumidores, tendo em conta os progressos da tecnologia das comunicações electrónicas e as estatísticas transmitidas à Comissão, a fim de apurar se é necessário alterar as suas disposições, nomeadamente no que respeita aos dados abrangidos e aos períodos em que estes devem ser conservados. O presente relatório analisa também as implicações da Directiva em matéria de direitos fundamentais, tendo em conta as críticas que, em termos gerais, têm sido formuladas relativamente à conservação de dados, e analisa se serão necessárias medidas para fazer face às preocupações relacionadas com a utilização de cartões SIM anónimos para fins criminosos[2].

Em termos globais, a avaliação demonstrou que a conservação de dados é um instrumento importante para o funcionamento dos sistemas de justiça penal e para efeitos de aplicação da lei na União Europeia. O contributo da Directiva para a harmonização da conservação de dados tem sido algo limitado, nomeadamente no que se refere à delimitação das finalidades do tratamento desses dados, aos períodos de conservação ou ao reembolso dos custos suportados pelos operadores, que se situa fora do seu âmbito de aplicação. Tendo em conta as implicações e os riscos para a mercado interno e para o respeito do direito à vida privada e à protecção dos dados de carácter pessoal, a UE deve continuar a garantir, mediante a adopção de regras comuns, a aplicação sistemática de normas rigorosas em matéria de conservação, recuperação e utilização dos dados de tráfego e de localização. Em função destas conclusões, a Comissão tenciona propor alterações à Directiva, com base numa avaliação do seu impacto.

---

1 Directiva 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, e que altera a Directiva 2002/58/CE, JO L 105 de 13.4.2006, pp. 54-63.

2 Conclusões do Conselho sobre a luta contra a utilização abusiva e a utilização anónima de comunicações electrónicas, 2 908ª Reunião do Conselho «Justiça e Assuntos Internos», Bruxelas, 27 e 28 de Novembro de 2008.

2. ANTECEDENTES

O presente relatório de avaliação foi elaborado na sequência de debates aprofundados com os Estados-Membros, os peritos e outras partes interessadas, e com base nas observações por estes formuladas.

Em Maio de 2009, a Comissão organizou uma conferência intitulada *Towards the Evaluation of the Data Retention Directive* («Para uma avaliação da Directiva relativa à conservação de dados») em que participaram autoridades responsáveis pela protecção de dados, o sector privado, a sociedade civil e várias universidades. Em Setembro de 2009, a Comissão enviou um questionário aos participantes nestes grupos, tendo recebido cerca de 70 respostas[3]. Em Dezembro de 2010, a Comissão organizou uma segunda conferência, intitulada *Taking on the Data Retention Directive* («Ponto de situação da Directiva relativa à conservação de dados»), que contou com a participação de um leque de interessados semelhante, a fim de partilhar as avaliações preliminares da Directiva e debater os desafios futuros neste campo.

Entre Outubro de 2009 e Março de 2010, a Comissão encontrou-se com representantes dos vários Estados-Membros e dos países associados do Espaço Económico Europeu, a fim de debater mais detalhadamente as questões relativas à aplicação da Directiva. Os Estados-Membros começaram a aplicar a Directiva mais tarde do que o previsto, nomeadamente no que respeita aos dados relativos à Internet. Esse atraso na transposição da Directiva significou que nove Estados-Membros forneceram à Comissão os dados estatísticos completos, relativos aos anos de 2008 ou 2009, tal como exigido pelo artigo 10.° da Directiva, embora, no total, dezanove Estados-Membros tenham fornecido apenas dados estatísticos parciais (ver ponto 4.7). Em Julho de 2010, a Comissão escreveu aos Estados-Membros, solicitando-lhes informações quantitativas e qualitativas adicionais quanto à necessidade de conservação de dados para efeitos da aplicação da lei. Dez Estados-Membros responderam à Comissão, tendo fornecido mais pormenores sobre casos específicos em relação aos quais eram necessários mais dados[4].

O presente relatório assenta nos documentos de síntese adoptados pela Plataforma relativa à conservação de dados electrónicos para efeitos de investigação, detecção e repressão de crimes graves, desde a criação deste grupo, em 2008[5]. A Comissão teve em conta os relatórios do Grupo de Trabalho do Artigo 29.º para a Protecção dos Dados[6], nomeadamente o relatório sobre a segunda acção comum de controlo da aplicação da legislação, ou seja, a sua avaliação

---

3 As respostas foram publicadas no sítio *Web* da Comissão (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm).

4 Bélgica, República Checa, Chipre, Lituânia, Hungria, Países Baixos, Polónia, Eslovénia e Reino Unido. A Suécia também transmitiu dados sobre vários casos de crimes graves específicos em que os dados de tráfego históricos – que estavam disponíveis embora não existisse obrigação de os conservar – se revelaram determinantes para a condenação dos seus autores.

5 Este grupo de peritos foi instituído pela Decisão 2008/324/CE da Comissão, JO L 111 de 23.4.2008, p. 11-14. A Comissão reúne-se regularmente com este Grupo. O seus documentos de síntese estão publicados em: http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm

6 O Grupo de protecção das pessoas no que diz respeito ao tratamento de dados pessoais foi criado nos termos do artigo 29.º da Directiva relativa à protecção de dados (Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24.10.1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31)).

da conformidade da legislação dos Estados-Membros com as exigências em matéria de protecção e de segurança dos dados formuladas pela Directiva[7].

3. CONSERVAÇÃO DE DADOS NA UNIÃO EUROPEIA

3.1. Conservação de dados para efeitos da justiça penal e da aplicação da lei

Os fornecedores de serviços e de redes (a seguir designados por «operadores») têm, no âmbito da sua actividade, de tratar dados pessoais para efeitos da transmissão de comunicações, facturação, pagamentos de interligação, *marketing* e outros serviços de valor acrescentado. Esse tratamento envolve dados que indicam a origem, o destino, a data, a hora, a duração e o tipo de comunicação, bem como o equipamento de comunicação dos utilizadores e, no caso dos telemóveis, dados sobre a localização do equipamento. Por força da Directiva 2002/58/CE, relativa à protecção da privacidade no sector das comunicações electrónicas (a seguir designada por «Directiva relativa à privacidade e às comunicações electrónicas»)[8], os dados de tráfego originados pela utilização de serviços de comunicações electrónicas devem, em princípio, ser apagados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação, salvo se forem necessários para efeitos de facturação – apenas durante o período em que sejam necessários - ou se tiver sido obtido o consentimento do assinante ou utilizador. Os dados de localização só podem ser tratados se forem tornados anónimos ou com o consentimento do utilizador em causa, na medida e durante o tempo necessário para o fornecimento de um serviço de valor acrescentado.

Antes da entrada em vigor da Directiva as autoridades nacionais podiam, em determinadas condições, solicitar aos operadores o acesso a estes dados, por exemplo, para identificar os assinantes que utilizavam um determinado endereço IP, analisar comunicações anteriores ou localizar um determinado telemóvel.

A nível da UE, a conservação e a utilização de dados para efeitos de aplicação da lei foi abordada, pela primeira vez, pela Directiva 97/66/CE, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações. Essa Directiva previa inicialmente a possibilidade de os Estados-Membros adoptarem as medidas legislativas necessárias para a protecção da segurança pública, a defesa ou a manutenção da ordem pública, incluindo o bem-estar económico do Estado quando as actividades se relacionavam com questões de segurança do Estado e a aplicação do direito penal[9].

---

7 Relatório 1/2010, sobre a segunda acção comum de controlo da aplicação da legislação: Cumprimento a nível nacional, pelos operadores de telecomunicações e fornecedores de serviços de Internet das obrigações previstas na legislação nacional em matéria de conservação de dados de tráfego, tendo por base jurídica os artigos 6.º e 9.º da Directiva relativa à privacidade e às comunicações electrónicas (2002/58/CE) e a Directiva relativa à conservação de dados (2006/24/CE), que altera a Directiva relativa à privacidade e às comunicações electrónicas (WP 172) de 13.7.2010 (ver http://ec.europa.eu/Justice/policies/Privacy/workinggroup/wpdocs/2010_en.htm).

8 Directiva 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 (Directiva relativa à privacidade e às comunicações electrónicas, JO L 201 de 31.7.2002, pp. 37-47).

9 Artigo 14.º, n.º 1, da Directiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações (JO L 24 de 30.1.1998, pp. 1–8).

Esta disposição foi desenvolvida na Directiva relativa à privacidade e às comunicações electrónicas, que permite aos Estados-Membros adoptarem medidas legislativas em derrogação do princípio da confidencialidade das comunicações, incluindo, sob certas condições, a conservação, o acesso e a utilização dos dados para efeitos de aplicação da lei. O artigo 15.º, n.º 1, permite aos Estados-Membros restringirem o âmbito das obrigações e direitos, incluindo através da conservação de dados por um período limitado, sempre que «a medida seja 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».

O papel que os dados conservados desempenham no âmbito dos sistemas de justiça penal e de aplicação da lei é abordado com maior profundidade na Secção 5.

3.2. Objectivo e base jurídica da Directiva relativa à conservação de dados

Em consequência das disposições da Directiva 97/66/CE e da Directiva relativa à privacidade e às comunicações electrónicas, que autorizam os Estados-Membros a adoptarem legislação em matéria de conservação de dados, os operadores de alguns Estados-Membros foram obrigados a adquirir equipamento para a conservação de dados e a empregar pessoal para obter esses dados em nome das autoridades responsáveis pela aplicação da lei, enquanto os operadores de outros Estados-Membros não estavam sujeitos a essa obrigação, o que provocou distorções no mercado interno. Além disso, a evolução dos modelos comerciais e dos serviços oferecidos, como o aumento das tarifas com taxas fixas e dos serviços de comunicações electrónicas pré-pagas ou gratuitas, fez com que os operadores deixassem progressivamente de armazenar os dados de tráfego e de localização para fins de facturação, reduzindo assim a disponibilidade desses dados para efeitos da justiça penal ou de aplicação da lei. Os ataques terroristas em Madrid, em 2004, e em Londres, em 2005, acentuaram a urgência de debater, a nível da UE, a melhor forma de abordar estas questões.

Neste contexto, a Directiva relativa à conservação de dados exige que os Estados-Membros obriguem os prestadores de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações a conservarem os dados relativos às comunicações para efeitos de investigação, detecção e repressão de crimes graves, tal como definidos por cada Estado-Membro na sua legislação nacional, tendo procurado harmonizar algumas questões conexas em toda a União Europeia.

A Directiva alterou o artigo 15.º, n.º 1, da Directiva relativa à privacidade e às comunicações electrónicas, tendo aditado um número que determina que o artigo 15.º, n.º 1, não se aplica aos dados conservados ao abrigo da Directiva relativa à conservação de dados[10]. Como resultado, os Estados-Membros (como referido no considerando n.º 12 da Directiva) continuam a poder introduzir derrogações ao princípio da confidencialidade das

[10] Artigo 11.° da Directiva: «No artigo 15.° da Directiva 2002/58/CE é inserido o seguinte número: 1-A. O n.º 1 não é aplicável aos dados cuja conservação seja especificamente exigida pela Directiva 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, para os fins mencionados no n.º 1 do artigo 1.º dessa directiva».

comunicações. A Directiva (relativa à conservação de dados) regulamenta apenas a conservação de dados para os efeitos, mais limitados, de investigação, detecção e repressão de crimes graves.

Esta complexa relação jurídica entre a Directiva relativa à conservação de dados e a Directiva relativa à privacidade e às comunicações electrónicas, juntamente com a falta de definição em qualquer das directivas do conceito de «crimes graves», dificulta a distinção entre, por um lado, as medidas adoptadas pelos Estados-Membros para transpor as obrigações de conservação de dados fixadas na Directiva e, por outro, a prática mais geral de conservação de dados nos Estados-Membros, permitida pelo artigo 15.º, n.º 1 da Directiva relativa à privacidade e às comunicações electrónicas[11]. Esta temática é abordada mais aprofundadamente na Secção 4.

A Directiva baseia-se no artigo 95.º do Tratado que institui a Comunidade Europeia (substituído pelo artigo 114.º do Tratado sobre o Funcionamento da União Europeia), relativo à criação e ao funcionamento do mercado interno. Após a adopção da Directiva, a sua base jurídica foi contestada no Tribunal de Justiça Europeu, com base no facto de ter por principal objectivo a investigação, detecção e repressão de crimes graves. O Tribunal considerou que a Directiva regulamentava operações que eram independentes da concretização de qualquer acção de cooperação policial ou judiciária em matéria penal e que não se destinava a harmonizar o acesso aos dados pelas autoridades nacionais competentes ou a utilização e o intercâmbio desses dados entre as referidas autoridades. O Tribunal concluiu, pois, que a Directiva visava, no essencial, as actividades dos fornecedores de serviços no sector em causa do mercado interno, decidindo, assim, confirmar a sua base jurídica[12].

3.3. Preservação de dados

A conservação de dados é distinta da preservação de dados (também conhecida por «congelamento rápido» ou «*quick freeze*») através da qual os operadores, por ordem de um tribunal, são obrigados a conservar os dados relativos exclusivamente a determinados indivíduos suspeitos de actividades criminosas, a partir da data da ordem de preservação. A preservação de dados é um dos instrumentos de investigação previstos e utilizados pelos Estados participantes na Convenção do Conselho da Europa sobre a Cibercriminalidade[13]. Quase todos os Estados participantes criaram pontos de contacto, cujo papel é garantir a prestação de assistência imediata em matéria de investigações ou de processos por cibercrime. No entanto, afigura-se que nem todas as Partes na Convenção previram a preservação de dados, não tendo sido ainda efectuada qualquer avaliação da eficácia deste modelo na luta contra a cibercriminalidade[14]. Recentemente, foi desenvolvido um novo tipo de preservação de dados, intitulado «*quick freeze plus*». Este modelo vai mais longe do que a preservação dos dados, na medida em que o juiz pode também autorizar o acesso a dados que ainda não

---

11 O Grupo de Trabalho do Artigo 29.° questiona se a Directiva [relativa à conservação de dados] pretendia constituir uma derrogação à obrigação geral de apagar os dados de tráfego no final da comunicação electrónica ou ordenar a conservação de todos os dados que os operadores já estavam autorizados a conservar para fins comerciais.

12 TJE, processo C-301/6, Irlanda / Parlamento Europeu e Conselho, Colectânea, 2009, p. I-00593.

13 Artigo 16. ° da Convenção sobre a Cibercriminalidade (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm).

14 Fonte: Conselho da Europa.

tenham sido apagados pelos operadores. Além disso, existia uma derrogação muito limitada, prevista na lei, à obrigação de apagar, durante um curto período de tempo, determinados dados das comunicações que não são normalmente armazenados (como os dados de localização, os dados de ligação à Internet ou endereços IP dinâmicos) relativamente aos utilizadores com assinaturas a preço fixo, em relação aos quais não existe necessidade de armazenar dados para efeitos de facturação.

Os defensores da preservação de dados consideram-na menos invasiva da privacidade do que a conservação de dados. Contudo, a maioria dos Estados-Membros não concorda que qualquer das variantes da preservação de dados possa substituir adequadamente a conservação de dados, porque esta última resulta na disponibilidade de dados históricos enquanto a preservação dos dados não garante a possibilidade de estabelecer pistas de investigação antes de ser dada a ordem de preservação, não permite investigações cujo alvo seja desconhecido nem permite recolher provas relativas, por exemplo, a movimentações das vítimas ou testemunhas de um crime[15].

4. TRANSPOSIÇÃO DA DIRECTIVA RELATIVA À CONSERVAÇÃO DE DADOS

Os Estados-Membros tinham de transpor a Directiva até 15 de Setembro de 2007, podendo optar por adiar até 15 de Março de 2009 a imposição das obrigações de conservação relacionadas com o acesso à Internet, ao correio electrónico e às comunicações telefónicas através da Internet.

A análise a seguir efectuada tem por base as notificações de transposição enviadas à Comissão por 25 Estados-Membros, incluindo a Bélgica, que apenas transpôs a Directiva parcialmente[16]. Na Áustria e na Suécia o projecto de legislação está em discussão. Nesses dois Estados-Membros, não existe qualquer obrigação de conservação de dados, mas as autoridades responsáveis pela aplicação da lei podem pedir – pedindo e obtendo de facto – dados de tráfego dos operadores, na medida em que esses dados se encontrem disponíveis. Após a notificação inicial da transposição pela República Checa, Alemanha e Roménia, os respectivos tribunais constitucionais revogaram a legislação nacional que transpunha a Directiva[17], e estes três países estão neste momento a estudar a forma como irão proceder novamente à sua transposição.

---

15 Este facto foi igualmente reconhecido pelo Tribunal Constitucional da Alemanha no seu acórdão que revoga a legislação alemã de transposição da Directiva. (ver ponto 4.9): (Bundesverfassungsgericht, 1 BvR 256/08 de 2 de Março de 2010, par. 208).

16 Os 25 Estados-Membros que notificaram à Comissão a transposição da directiva são: Bélgica, Bulgária, República Checa, Dinamarca, Alemanha, Grécia, Estónia, Irlanda, Espanha, França, Itália, Chipre, Letónia, Lituânia, Luxemburgo, Hungria, Malta, Países Baixos, Polónia, Portugal, Roménia, Eslovénia, Eslováquia, Finlândia e Reino Unido. A Bélgica informou a Comissão de que o seu projecto de legislação que conclui a transposição ainda se encontra em debate no parlamento.

17 Decisão n.º 1258, de 8 de Outubro de 2009, do Tribunal Constitucional da Roménia, jornal oficial da Roménia, n.° 789, de 23 de Novembro de 2009; acórdão 1 BvR 256/08, de 2 de Março de 2010, do Tribunal Constitucional da Alemanha (*Bundesverfassungsgericht*); jornal oficial de 1 de Abril de 2011; acórdão do Tribunal Constitucional de 22 de Março relativo às disposições do artigo 97º, n.^{os} 3 e 4, da Lei n.° 127/2005 Coll. sobre as comunicações electrónicas, que altera determinadas leis conexas, e decreto n.° 485/2005 Coll. sobre a conservação e a transmissão de dados às autoridades competentes.

A presente secção analisa a forma como os Estados-Membros transpuseram as disposições pertinentes da Directiva. Analisa ainda se os Estados-Membros optaram por reembolsar os operadores pelos custos suportados com a obtenção e conservação dos dados, aspecto em relação ao qual a Directiva é omissa, bem como as implicações para a Directiva das sentenças proferidas pelos tribunais constitucionais da Alemanha, da Roménia e da República Checa.

4.1. Objectivo de conservação de dados (Artigo 1.º)

A Directiva obriga os Estados-Membros a adoptarem as medidas necessárias para assegurar que os dados são conservados e estão disponíveis para efeitos de investigação, detecção e repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro. Contudo, os objectivos da conservação e/ou acesso aos dados nas diversas legislações nacionais continuam a variar consoante os Estados-Membros. Assim, dez Estados-Membros (Bulgária, Estónia, Irlanda, Grécia, Espanha, Lituânia, Luxemburgo, Hungria, Países Baixos e Finlândia) definiram «crime grave», tomando como referência uma pena de prisão mínima, a possibilidade de ser aplicada uma pena privativa de liberdade ou uma lista de infracções penais previstas na legislação nacional. Oito Estados-Membros (Bélgica, Dinamarca, França, Itália Letónia, Polónia, Eslováquia e Eslovénia) exigem que os dados sejam conservados não apenas para efeitos de investigação, detecção e repressão de crimes graves, mas também em relação a quaisquer infracções penais ou para efeitos de prevenção da prática de crimes ou, de um modo geral, para salvaguardar a segurança nacional e/ou a segurança pública. A legislação de quatro Estados-Membros (Chipre, Malta, Portugal e Reino Unido) faz referência a «crimes graves» ou a «infracções graves» sem avançar uma definição. O quadro seguinte apresenta a situação por país:

Quadro 1: Limitação das finalidades em matéria de conservação de dados previstas nas legislações nacionais	
Bélgica	Para a investigação e repressão de infracções penais, a repressão do abuso de números telefónicos de emergência, a investigação de abusos nas redes ou serviços de comunicações electrónicas, assim como para fins de recolha de informações pelos serviços de informações e de segurança do Estado[18].
Bulgária	Para a investigação de crimes graves e dos crimes previstos no artigo 319º, alíneas a) a f), do Código Penal, assim como para a busca de pessoas[19].
República Checa	Ainda não transpôs a Directiva.
Dinamarca	Para a investigação e repressão de infracções penais[20].
Alemanha	Ainda não transpôs a Directiva.
Estónia	Pode ser autorizada a conservação de dados se a recolha de provas por outros actos processuais for excluída ou particularmente difícil e o objecto do processo penal for uma infracção penal [de primeiro grau ou uma infracção penal de segundo grau cometida com dolo, punida com pena de prisão de pelo menos três anos][21].

18 Artigo 126.º, n.º 1, da Lei de 13 de Junho de 2005 relativa às comunicações electrónicas.
19 Artigo 250.º- a, n.º 2, da Lei das Comunicações Electrónicas (alterada), 2010.
20 Artigo 1.º, Ordem relativa à Conservação de Dados.
21 Artigo 110.°, n.º 1, do Código de Processo Penal.

Quadro 1: Limitação das finalidades em matéria de conservação de dados previstas nas legislações nacionais	
Irlanda	Para a prevenção de infracções graves [ou seja, puníveis com pena de prisão de 5 ou mais anos, ou das infracções previstas na legislação de transposição], para a salvaguarda da segurança do Estado ou para salvar uma vida humana[22].
Grécia	Para a detecção de crimes particularmente graves[23].
Espanha	Para a detecção, investigação e repressão dos crimes graves previstos no Código Penal ou em legislação penal especial[24].
França	Para a detecção, investigação e repressão de infracções penais, e unicamente para prestar as informações necessárias às autoridades judiciais, bem como para a prevenção de actos de terrorismo e a protecção da propriedade intelectual[25].
Itália	Para a detecção e a repressão de infracções penais[26].
Chipre	Para a investigação de infracções penais graves[27].
Letónia	Para proteger a segurança nacional e/ou a segurança pública ou para garantir a investigação de crimes, acções penais e processos-crime[28].
Lituânia	Para a investigação, detecção e repressão de crimes graves ou muito graves, tal como definidos no Código Penal da Lituânia[29].
Luxemburgo	Para a detecção, investigação e repressão de infracções penais punidas com pena de prisão igual ou superior a um ano[30].
Hungria	Para permitir que os organismos de investigação, o Ministério Público, os tribunais e as agências de segurança nacional possam desempenhar as suas funções, bem como para permitir à polícia e às autoridades aduaneiras e fiscais investigar crimes dolosos sancionados com pena de prisão de pelo menos dois anos[31].
Malta	Para a investigação, detecção e repressão de crimes graves[32].
Países Baixos	Para a investigação e repressão de infracções graves, passíveis de penas privativas da liberdade.[33]

22 Artigo 6.º Lei das Comunicações (Conservação de Dados) de 2011.

23 Trata-se dos crimes definidos no artigo 4.º da Lei 2225/1994; Artigo 1.º da Lei 3917/2011.

24 Artigo 1. °, n. ° 1, da Lei 25/2007.

25 As normas legislativas que regulamentam a utilização dos dados conservados, respectivamente, para as infracções penais, para a prevenção de actos de terrorismo e a para a protecção da propriedade intelectual são as seguintes: Artigo L.34-1(II), CPCE, Lei n.º 2006-64 de 23 de Janeiro de 2006 e Lei nº 2009-669 de 12 de Junho de 2009.

26 Artigo 132.°, n.° 1, do Código de Protecção de Dados.

27 Artigo 4.º, n.º 1, da Lei n.º 183 (I)/2007.

28 Artigo 71. °, n. ° 1), Lei das Comunicações Electrónicas.

29 Artigo 65.º da Lei X-1835

30 Artigo 1.°, n.° 1, da Lei de 24 de Julho de 2010.

31 Para efeitos gerais de conservação de dados: artigo 159.º/A da Lei C/2003, com a última redacção que lhe foi dada pela Lei CLXXIV/2007. Para efeitos de acesso pela Polícia: artigo 68.º da Lei XXXIV/1994. Para efeitos de acesso pela Administração Fiscal e Aduaneira Nacional: artigo 59º da Lei CXXII/2010.

32 Artigo 20.º, n.º 1, Aviso Legal 198/2008.

33 Artigo 126.º do Código de Processo Penal.

Quadro 1: Limitação das finalidades em matéria de conservação de dados previstas nas legislações nacionais	
Áustria	Ainda não transpôs a Directiva.
Polónia	Para a prevenção ou detecção de crimes, prevenção e detecção de infracções fiscais, utilização pelos magistrados do Ministério Público e dos tribunais quando relevante para acções judiciais em curso, assim como no âmbito da Agência de Segurança Interna, da Agência de Informações, dos Serviços Centrais de Combate à Corrupção e dos Serviço Militares de Contra-Informação[34].
Portugal	Para a investigação, detecção e repressão de crimes graves[35].
Roménia	Ainda não transpôs a Directiva.
Eslovénia	Para salvaguardar a segurança nacional, as normas constitucionais e os interesses económicos, políticos e de segurança do Estado... assim como para efeitos de defesa nacional[36].
Eslováquia	Para a prevenção, investigação, detecção e repressão de infracções penais[37].
Finlândia	Para a investigação, detecção e repressão de crimes graves, como os definidos no capítulo 5-A, artigo 3.°, nº 1, da lei relativa às medidas de coerção[38].
Suécia	Ainda não transpôs a Directiva.
Reino Unido	Para a investigação, detecção e repressão de crimes graves[39].

A maior parte dos Estados-Membros que já efectuou a transposição da Directiva para a respectiva legislação autoriza o acesso e a utilização dos dados conservados para fins que vão mais além dos previstos na Directiva, incluindo a prevenção e o combate à criminalidade em geral e a prevenção de riscos para a vida e a integridade física da pessoas. Embora tal seja permitido pela Directiva relativa à privacidade e às comunicações electrónicas, o grau de harmonização da legislação da UE neste domínio continua a ser muito reduzido. As diferenças quanto às finalidades para as quais os dados podem ser conservados podem afectar o volume e a frequência dos pedidos e, deste modo, os custos suportados para satisfazer as obrigações impostas pela Directiva. Além disso, esta situação não garante uma previsibilidade suficiente, que constitui uma das exigências de qualquer medida legislativa que restrinja o direito à vida privada[40]. A Comissão irá analisar a necessidade de assegurar uma maior harmonização neste domínio e as modalidades a utilizar para o efeito[41].

---

34 Artigo 180.º-A, da Lei das Telecomunicações, de 16 de Julho de 2004, com a redacção que lhe foi dada pelo artigo 1.° da Lei de 24 de Abril de 2009.

35 Artigos 1.° e 3.º, n.° 1, da Lei 32/2008.

36 Artigo 170.º-A, n.º 1, da Lei relativa às Comunicações Electrónicas.

37 Artigo 59.º-A, n.º 6, da Lei relativa às Comunicações Electrónicas.

38 Artigo 14.º-A, n.º 1, da Lei relativa às Comunicações Electrónicas.

39 Regulamento sobre a Conservação de Dados (Directiva CE) de 2009 (2009 n.° 859).

40 Acórdão do Tribunal de Justiça Europeu de 20 de Maio de 2003 nos processos apensos C-465/00, C-138/01 e C-139/01 (pedido de decisão prejudicial apresentado pelo Verfassungsgerichtshof e Oberster Gerichtshof): Rechnungshof (C-465/00) contra Österreichischer Rundfunk e o. e entre Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) e Österreichischer Rundfunk (Protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais — Directiva 95/46/CE —

4.2. Obrigações dos operadores em matéria de conservação de dados (Artigo 1º)

A Directiva é aplicável aos «fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou a uma rede pública de comunicações» (artigo 1.º, n.º 1). Dois Estados-Membros (Finlândia e Reino Unido) não exigem aos pequenos operadores que conservem os dados, porque, segundo argumentam, os custos tanto para o prestador do serviço como para o Estado seriam superiores aos benefícios retirados em matéria de aplicação da lei e da justiça penal. Quatro Estados-Membros (Letónia, Luxemburgo, Países Baixos e Polónia) indicaram que haviam adoptado regimes administrativos alternativos. Embora os grandes operadores presentes em vários Estados-Membros beneficiem de economias de escala em termos de custos, os operadores de menor dimensão de alguns Estados-Membros criam normalmente empresas comuns ou externalizam essas funções para empresas especializadas em programas de conservação e de extracção de dados, a fim de reduzirem os seus custos. Essa externalização das tarefas técnicas não afecta a obrigação dos operadores de controlarem adequadamente as operações de tratamento dos dados e de garantirem que são adoptadas as necessárias medidas de segurança, o que pode ser particularmente problemático para os operadores de menor dimensão. A Comissão irá analisar a questão da segurança dos dados e do impacto sobre as pequenas e médias empresas quando se debruçar sobre as diferentes alternativas para modificar o quadro legislativo aplicável à conservação de dados.

4.3. Acesso aos dados: autoridades, procedimentos e condições (Artigo 4.º)

Os Estados-Membros devem «tomar medidas para assegurar que os dados conservados […] só sejam transmitidos às autoridades nacionais competentes em casos específicos e de acordo com a legislação nacional». Incumbe aos Estados-Membros definir no respectivo direito nacional «os procedimentos que devem ser seguidos e as condições que devem ser respeitadas para se ter acesso a dados conservados de acordo com os requisitos da necessidade e da proporcionalidade, sob reserva das disposições pertinentes do direito da União Europeia ou do direito internacional público, nomeadamente a Convenção Europeia dos Direitos do Homem, na interpretação que lhe é dada pelo Tribunal Europeu dos Direitos do Homem».

Em todos os Estados-Membros, as forças de polícia e, com excepção das jurisdições de direito comum (Irlanda e Reino Unido), os magistrados do Ministério Público podem ter acesso aos dados conservados. Catorze Estados-Membros incluem os serviços de informações, de segurança ou militares entre as autoridades competentes. Seis Estados-Membros enumeram autoridades fiscais e/ou aduaneiras e três identificam as autoridades de controlo das fronteiras. Um Estado-Membro permite a outras autoridades públicas acederem aos dados desde que estejam autorizadas para fins específicos no âmbito do direito derivado. Onze Estados-Membros exigem uma autorização judicial para cada pedido de acesso aos dados conservados. Em três Estados-Membros é necessária, na maior parte dos casos, uma autorização judicial. Quatro Estados-Membros exigem a autorização de uma autoridade

---

Protecção da vida privada — Divulgação de dados sobre os rendimentos de assalariados de entidades sujeitas à auditoria do Rechnungshof).

[41] Quando adoptou a Directiva, a Comissão emitiu uma declaração em que sugeria que fosse tida em conta a lista de crimes do mandado de detenção europeu. (Decisão-Quadro do Conselho 2002/584/JHA, de 13 de Junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros.)

superior mas não de um juiz. Em 2 Estados-Membros a única condição é que o pedido seja apresentado por escrito.

Quadro 2: Acesso aos dados de telecomunicações conservados		
	Autoridades nacionais competentes	*Procedimentos e condições*
Bélgica	Unidade de coordenação judicial, magistrados, Ministério Público, polícia judiciária.	O acesso tem de ser autorizado por um magistrado ou por um procurador do Ministério Público. Mediante pedido, os operadores devem fornecer em «tempo real» dados relativos aos assinantes, assim como dados de tráfego e de localização, para as chamadas efectuadas no último mês. Os dados relativos às chamadas anteriores devem ser apresentadas o mais rapidamente possível.
Bulgária[42]	Direcções e serviços específicos do Organismo Estatal para a Segurança Nacional, Ministério da Administração Interna, Serviço de Informações Militares, Polícia Militar, Ministro da Defesa, serviços de investigação nacionais; autoridades judiciais e de instrução, mediante certas condições.	O acesso só é possível com ordem do presidente de um tribunal regional.
República Checa	Ainda não transpôs a Directiva.	
Dinamarca[43]	Polícia	O acesso requer autorização judicial; o tribunal pode autorizar se o pedido satisfizer critérios rigorosos em matéria de suspeita, necessidade e proporcionalidade.
Alemanha	Ainda não transpôs a Directiva.	
Estónia[44]	Polícia e Guarda de Fronteiras, Direcção da Polícia de Segurança e, para os objectos e as comunicações electrónicas, a Direcção dos Serviços Aduaneiros e Fiscais.	O acesso requer a autorização de um juiz de instrução. Os operadores devem «apresentar [os dados conservados] dentro de 10 horas e, nos outros casos, no prazo de 10 dias úteis [a contar da data de recepção do pedido]».
Irlanda[45]	Membros da *Garda Síochána* (polícia) de categoria *Chief Superintendant* ou superior; agentes das Forças de Defesa Permanentes de categoria equivalente ou superior a coronel; funcionários da Administração Fiscal de categoria equivalente a «responsável principal» ou superior.	Os pedidos devem ser apresentados por escrito.
Grécia[46]	Autoridades judiciais, militares ou de polícia.	O acesso requer uma decisão judicial que declare que a investigação por outros meios é impossível ou extremamente difícil.
Espanha[47]	Forças policiais responsáveis pela detecção, investigação e repressão de crimes graves,	O acesso aos dados pelas autoridades nacionais competentes requer autorização judicial prévia.

42 Artigo 250.º-B, n.º 1, da Lei das Comunicações Electrónicas (alterada) de 2010 (autoridades); Artigo 250.º- B, n.º 2, e 250.º- C, n.º 1, da Lei das Comunicações Electrónicas (alterada) de 2010 (acesso).

43 Capítulo 71 da Lei de Administração da Justiça.

44 Artigo 112.º, n.os 2 e 3, do Código de Processo Penal (Autoridades e Procedimentos); Artigo 111.º, n.º 9, da Lei relativa às Comunicações Electrónicas (Condições);

45 Artigo 6.º da Lei das Comunicações (Conservação de Dados) de 2009.

46 Artigos 3.º e 4.º da Lei 2225/94

Quadro 2: Acesso aos dados de telecomunicações conservados		
	Autoridades nacionais competentes	*Procedimentos e condições*
	Serviços de Informação Nacional e Agência Aduaneira.	
França[48]	Ministério Público, determinados agentes de polícia e *gendarmes*.	A polícia tem de apresentar uma justificação para cada pedido de acesso a dados conservados e obter autorização da parte da pessoa designada junto do Ministério da Administração Interna pela *Commission nationale de contrôle des interceptions de sécurité*. Os pedidos de acesso são tramitados por um funcionário designado que trabalha para o operador.
Itália[49]	Procuradores do Ministério Público; Polícia; advogados de defesa do réu ou da pessoa investigada.	Acesso sujeito a um «despacho fundamentado» do Ministério Público
Chipre[50]	Tribunais, Ministério Público e Polícia.	O acesso deve ser autorizado por um procurador se este considerar que pode fornecer elementos de prova da prática de um crime grave. Um juiz pode emitir ordens deste tipo se houver suspeita razoável da prática de uma infracção penal grave e se os dados forem susceptíveis de lhe estar associados.
Letónia[51]	Funcionários autorizados das autoridades de instrução; pessoas que executam funções de investigação; funcionários autorizados dos organismos de segurança nacional; Ministério público; tribunais.	Os funcionários autorizados, o Ministério Público e os tribunais têm de avaliar a «adequação e pertinência» do pedido, registá-lo e garantir a protecção dos dados obtidos. As instâncias autorizadas podem assinar acordos com os operadores, nomeadamente para cifragem dos dados fornecidos.
Lituânia[52]	Autoridades de instrução, Ministério Público, tribunais (juízes) e agentes dos serviços de informações.	As autoridades públicas autorizadas devem solicitar por escrito os dados conservados. Para ter acesso durante as investigações em fase de instrução é necessário um mandado judicial.
Luxemburgo[53]	Autoridades judiciais (magistrados de instrução e procuradores), autoridades responsáveis pela salvaguarda da segurança nacional, pela defesa, pela segurança pública e pela prevenção, investigação, detecção e repressão de infracções penais.	Acesso sujeito a autorização judicial.
Hungria[54]	Polícia, Administração Fiscal e Aduaneira, serviços de segurança nacional, Ministério público, tribunais.	A Polícia e a Administração Fiscal e Aduaneira devem obter autorização do Ministério Público. O Ministério Público e os serviços de segurança nacional podem ter acesso aos dados sem uma decisão judicial.

47 Artigos 6.º e 7.º da Lei 25/2007.

48 Artigos 60.º, n.º 1, e 60.º, n.º 2, do Código de Processo Penal (autoridades); Artigo L.31-1-1 (condições).

49 Artigo 132.°, n.° 3, do Código de Protecção de Dados.

50 Artigo 4.º, n.os 2 e 4, da Lei 183 (I)/2007.

51 Artigo 71.°, n.° 1, da Lei das Comunicações Electrónicas (autoridades). Regulamento do Governo n.º 820 (procedimentos).

52 Artigo 77.° nos 1 e 2 da Lei X-1835; relatório oral à Comissão.

53 Artigos 5.º-2, n.º 1, e 9.º, n.º 2, da Lei de 24 de Julho de 2010 (autoridades); Artigo 67.º-1 do Código de Instrução Criminal (condições).

Quadro 2: Acesso aos dados de telecomunicações conservados		
	Autoridades nacionais competentes	*Procedimentos e condições*
Malta[55]	Forças Policiais de Malta; Serviços de segurança.	Os pedidos devem ser apresentados por escrito.
Países Baixos[56]	Agentes da polícia judiciária.	O acesso deve ser autorizado por um magistrado do Ministério Público ou pelo juiz de instrução.
Áustria	Ainda não transpôs a Directiva.	
Polónia[57]	Polícia, polícia de fronteiras, inspectores fiscais, Agência de Segurança Interna, Serviço de Informações, Serviços Centrais de Luta contra a Corrupção, serviços militares de informação e contra-informação, tribunais e Ministério Público	Os pedidos devem ser apresentados por escrito e, no caso da polícia, da polícia de fronteiras e dos inspectores fiscais, devem ser autorizados pelo funcionário superior da organização.
Portugal[58]	Polícia Judiciária, Guarda Nacional Republicana, Polícia de Segurança Pública, Polícia Judiciária Militar, Serviço de Estrangeiros e Fronteiras, Polícia Marítima.	A transmissão dos dados deve ser autorizada por despacho judicial, 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. A decisão judicial de transmitir os dados deve respeitar os princípios da necessidade e proporcionalidade.
Roménia	Ainda não transpôs a Directiva.	
Eslovénia[59]	Polícia, serviços de informações e de segurança, serviços de Defesa responsáveis pela informação e contra-informação e missões de segurança.	O acesso está sujeito a autorização judicial.
Eslováquia[60]	Autoridades responsáveis pela aplicação da lei, tribunais.	Os pedidos devem ser apresentados por escrito.
Finlândia[61]	Polícia, Serviço de Fronteiras, autoridades aduaneiras (para os dados conservados relativos a assinantes, ao tráfego e a dados de localização). Centros de Resposta de Emergência, serviços de salvamento marítimo, Sub-Centro de Salvamento Marítimo (para os dados de identificação e localização em situações de emergência)	Os dados dos assinantes podem ser consultados por todas as autoridades competentes sem autorização judicial. Os outros dados requerem uma decisão judicial.
Suécia	Ainda não transpôs a Directiva.	
Reino Unido[62]	Polícia, Serviços de informações, autoridades fiscais e aduaneiras, outras entidades públicas designadas pelo direito derivado.	O acesso é possível desde que seja autorizado por uma «pessoa designada» e desde que sejam respeitados os critérios da necessidade e da proporcionalidade, em casos específicos e em

54 Artigos 68.º, n.º 1, e 69.º, n.º 1, alíneas c) e d), da Lei XXXIV de 1994; Artigos 9.º/A(1) da Lei V de 1972; Artigos 71.º, n^{os} 1, 3, 4, 178.º/A, n.º 4), 200.º, 201.º, 268.º, n.º 2, da Lei XIX de 1998; artigo 40.°, n.^{os} 1 e 2.º, artigo 53.º, n.º 1, e artigo 54.º, n.º 1, alínea j), da Lei CXXV de 1995.

55 Artigo 20.º, n.º 1 e n.º 3, Aviso Legal 198/2008.

56 Artigo 126.º-NI do Código de Processo Penal.

57 Artigo 179.º, n.º 3, da Lei das Telecomunicações, de 16 de Julho de 2004, com a redacção que lhe foi dada pelo artigo 1.° da Lei de 24 de Abril de 2009.

58 Artigos 2.°, n.º 1, 3.º , n.º 2, e 9.º da Lei 32/2008.

59 Artigo 107.º-C da Lei relativa às Comunicações Electrónicas; Artigo 149.º-B do Código de Processo Penal; Artigo 24.º, alínea b), da Lei relativa aos Serviços de Segurança. Artigo 32.º da Lei da Defesa.

60 Artigo 59.º-A, nº 8, da Lei relativa às Comunicações Electrónicas.

61 Artigos 35.º, n.º 1, e 36.º da Lei relativa às Comunicações Electrónicas; Artigos 31.º-33.º da Lei da Polícia; Artigo 41.º, da Lei relativa ao Serviço de Fronteiras.

Quadro 2: Acesso aos dados de telecomunicações conservados		
Autoridades nacionais competentes		*Procedimentos e condições*
		circunstâncias em que a divulgação dos dados seja autorizada ou exigida por lei. Foram acordados procedimentos específicos com os operadores.

A Comissão irá avaliar a necessidade de um maior grau de harmonização e as e modalidades para o conseguir, no que se refere às autoridades que têm acesso aos dados conservados, assim como aos procedimentos para a sua obtenção. Entre estas modalidades figuram a elaboração de listas mais claras das autoridades competentes , o controlo judicial e/ou independente dos pedidos de dados e normas processuais mínimas para os operadores concederem acesso às autoridades competentes.

4.4. Âmbito da conservação dos dados e categorias de dados abrangidos (artigo 1.º, n.º 2, artigo 3.º, nº 2 e artigo 5.º)

A Directiva é aplicável às comunicações telefónicas das redes fixa e móvel, ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet. A Directiva especifica, no seu artigo 5.°, as categorias de dados a conservar, designadamente os dados necessários para identificar:

(a) a origem de uma comunicação;

(b) o destino de uma comunicação;

(c) a data, hora e duração de uma comunicação;

(d) o tipo de comunicação;

(e) o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento; ou

(f) a localização do equipamento de comunicação móvel.

Abrange ainda (artigo 3.º, n.º 2) as chamadas telefónicas falhadas, ou seja, as comunicações em que a ligação telefónica foi estabelecida, mas que não obteve resposta, ou em que houve uma intervenção do gestor da rede, quando os dados relativos a essas chamadas são gerados, tratados, armazenados ou registados pelos operadores. Nos termos da Directiva, não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações. Foi também posteriormente clarificado que as consultas efectuadas na Internet, ou seja, os registos de pesquisa gerados devido à disponibilização de um serviço de motor de pesquisa, estão

---

62 Artigo 25.º, Apêndice 1, da Lei relativa às competências de investigação, de 2000; Artigo 7.º do Regulamento relativo à conservação de dados. O artigo 22.º, n.º 2, da Lei relativa às competências de investigação define os fins para os quais as autoridades podem obter dados.

igualmente fora do âmbito de aplicação da Directiva, pois são considerados conteúdo e não dados de tráfego[63].

21 Estados-Membros contemplam a conservação de cada uma destas categorias de dados na sua legislação de transposição. A Bélgica não especifica o tipo de dados telefónicos a conservar nem adoptou qualquer disposição em matéria de dados relacionados com a Internet. Os inquiridos que responderam ao questionário da Comissão não consideraram necessário alterar as categorias de dados que devem ser conservados, embora o Parlamento Europeu tenha enviado à Comissão uma declaração escrita em que solicitava que a Directiva fosse tornada extensível aos «motores de pesquisa, a fim de reprimir, de formas rápida e eficaz, a pornografia infantil e os abusos sexuais em linha»[64]. No seu relatório sobre a segunda acção comum de controlo da aplicação da legislação, o Grupo de Trabalho do «Artigo 29.º» para a Protecção dos Dados alegou que a enumeração das categorias efectuada na Directiva deveria ser considerada exaustiva, não podendo ser impostas aos operadores quaisquer outras obrigações suplementares em matéria de conservação de dados. A Comissão vai avaliar a necessidade efectiva de cada uma destas categorias.

4.5. Períodos de conservação dos dados (artigos 6.º e 12.º)

Os Estados-Membros devem assegurar que as categorias de dados referidos no artigo 5.º sejam conservados por períodos não inferiores a seis meses e não superiores a dois anos. O período máximo de conservação pode ser prorrogado se um Estado-Membro tiver de «fazer face a circunstâncias especiais que justifiquem a prorrogação por um prazo limitado»; essa prorrogação deve ser notificada à Comissão que, no prazo de seis meses, a aprovará ou rejeitará. Embora o período máximo possa ser prorrogado, nenhuma disposição prevê a redução da duração do período de conservação para menos de seis meses. Com excepção de um, todos os Estados-Membros que transpuseram a directiva definiram períodos de conservação dos dados dentro destes limites, não tendo a Comissão recebido quaisquer notificações de eventuais prorrogações. Não existe, todavia, uma abordagem coerente em toda a UE.

Quinze Estados-Membros especificaram um prazo único para todas as categorias de dados: um Estado-Membro (Polónia) especifica um período de conservação dos dados de dois anos, outro Estado-Membro especifica um ano e meio (Letónia), dez especificam um ano (Bulgária, Dinamarca, Estónia, Grécia, Espanha, França, Países Baixos, Portugal, Finlândia e Reino Unido) e três especificam seis meses (Chipre, Luxemburgo e Lituânia). Cinco Estados-Membros definiram períodos de conservação distintos para as diferentes categorias de dados: dois Estados-Membros (Irlanda e Itália) especificam dois anos para os dados das comunicações telefónicas (redes fixa e móvel) e um ano para os dados de acesso à Internet, correio electrónico através da Internet e comunicações telefónicas através da Internet; um Estado-Membro (Eslovénia) especifica 14 meses para os dados das comunicações telefónicas e 8 meses para os relativos à Internet; um Estado-Membro (Eslováquia) especifica um ano para os dados das comunicações telefónicas (fixas e móveis) e 6 meses para os dados relativos à Internet; Um Estado-Membro (Malta) especifica 1 ano para os dados das

---

63 Parecer do Grupo de Trabalho do «Artigo 29.º» sobre questões de protecção de dados relacionadas com motores de pesquisa, de 4 de Abril de 2008.

64 Declaração Escrita, nos termos do artigo 123.º do Regimento de Parlamento Europeu, sobre a criação de um sistema de alerta rápido europeu contra a pedofilia e os abusos sexuais, 19.4.2010, 0029/2010.

comunicações telefónicas (redes fixa e móvel) e por Internet, e 6 meses para o acesso à Internet e o correio electrónico através da Internet. Um Estado-Membro (Hungria) conserva todos os dados durante um ano, excepto os das chamadas telefónicas falhadas, que só são conservados durante seis meses. Um Estado-Membro (Bélgica) não especificou qualquer período de conservação dos dados para as categorias de dados previstas na Directiva. O quadro seguinte apresenta a situação em pormenor.

Quadro 3: Períodos de conservação previstos nas legislações nacionais	
Bélgica[65]	Entre 1 ano e 36 meses para os serviços telefónicos «acessíveis ao público». Não existe qualquer disposição em matéria de dados da Internet.
Bulgária	1 ano. Os dados que tenham sido consultados podem, mediante pedido, ser conservados por um período suplementar de 6 meses.
República Checa	Ainda não transpôs a Directiva.
Dinamarca	1 ano
Alemanha	Ainda não transpôs a Directiva.
Estónia	1 ano
Irlanda	2 anos no caso dos dados das comunicações telefónicas (redes fixa e móvel), 1 ano para o acesso à Internet, correio electrónico através da Internet e comunicações telefónicas através da Internet.
Grécia	1 ano
Espanha	1 ano
França	1 ano
Itália	2 anos no caso dos dados das comunicações telefónicas (redes fixa e móvel), 1 ano para o acesso à Internet, correio electrónico através da Internet e comunicações telefónicas através da Internet.
Chipre	6 meses
Letónia	18 meses
Lituânia	6 meses
Luxemburgo	6 meses
Hungria	6 meses para as chamadas falhadas e 1 ano para todos os outros dados
Malta	1 ano para as chamadas telefónicas (redes fixa e móvel) e comunicações telefónicas através da Internet, 6 meses para os dados de acesso à Internet e de correio electrónico através da Internet.
Países Baixos	1 ano
Áustria	Ainda não transpôs a Directiva.
Polónia	2 anos
Portugal	1 ano
Roménia	Ainda não transpôs a Directiva (6 meses no quadro da legislação de transposição anterior que foi revogada).
Eslovénia	14 meses para os dados das comunicações telefónicas e 8 meses para os relativos à Internet.
Eslováquia	1 ano para as comunicações telefónicas (redes fixa e móvel), 6 meses para os dados de acesso à Internet, correio electrónico através da Internet e comunicações telefónicas através da Internet.
Finlândia	1 ano
Suécia	Ainda não transpôs a Directiva.
Reino Unido	1 ano

Embora esta diversidade de abordagens seja permitida pela Directiva, implica que a Directiva proporcione apenas uma segurança jurídica e uma previsibilidade limitadas em toda a UE para

[65] Artigo 126.º, n.º 2, da Lei de 13 de Junho de 2005 relativa às comunicações electrónicas.

os operadores que trabalham em mais do que um Estado-Membro e para os cidadãos cujos dados de comunicação possam ser armazenados em diferentes Estados-Membros. Tendo em conta a crescente internacionalização dos serviços de tratamento de dados e a externalização do seu armazenamento, importa analisar as possibilidades de harmonizar os períodos de conservação de dados em toda a UE. A fim de assegurar o respeito do princípio da proporcionalidade e tendo em conta os elementos quantitativos e qualitativos que comprovam o valor dos dados conservados nos Estados-Membros, assim como as tendências no sector das comunicações e das tecnologias e a evolução da criminalidade e do terrorismo, a Comissão irá estudar a possibilidade de definir períodos distintos em função das diferentes categorias de dados ou das categorias de crimes graves, ou de uma combinação de ambos[66]. Os dados quantitativos fornecidos até à data pelos Estados-Membros quanto à antiguidade dos dados conservados indicam que cerca de 90 % desses dados tinham seis meses ou menos e que cerca de 70 % tinham três meses ou menos quando foi introduzido o pedido de acesso (inicial) pelas autoridades responsáveis pela aplicação da lei (ver ponto 5.2).

4.6. Protecção e segurança dos dados; autoridades de controlo (artigos 7.º e 9.º)

A Directiva exige aos Estados-Membros que assegurem que os operadores respeitam, no mínimo, quatro princípios em matéria de segurança dos dados e que os dados conservados devem ser:

(a) da mesma qualidade e estar sujeitos à mesma protecção e segurança que os dados na rede [pública de comunicações];

(b) objecto de medidas técnicas e organizativas adequadas que os protejam da destruição acidental ou ilícita, da perda ou alteração acidental ou do armazenamento, tratamento, acesso ou divulgação não autorizado ou ilícito;

(c) objecto de medidas técnicas e organizativas adequadas para garantir que apenas pessoas especialmente autorizadas tenham acesso aos dados; e

(d) destruídos no final do período de conservação, excepto os dados que tenham sido facultados e conservados [para efeitos da Directiva].

Em conformidade com a Directiva relativa à protecção dos dados e com a Directiva relativa à privacidade e às comunicações electrónicas, os operadores estão proibidos de utilizar para outros fins os dados conservados ao abrigo da Directiva, desde que esses dados não tenham sido conservados para outros fins[67]. Os Estados-Membros são obrigados a designar uma autoridade pública para controlar, com absoluta independência, a aplicação destes princípios. Essas autoridades podem ser as exigidas pela Directiva relativa à protecção dos dados[68].

Quinze Estados-Membros transpuseram todos estes princípios para a sua legislação nacional. Quatro Estados-Membros (Bélgica, Estónia, Espanha e Letónia) transpuseram dois ou três destes princípios mas não prevêem expressamente a destruição dos dados no final do período

---

66 A proposta de directiva relativa à conservação de dados apresentada pela Comissão em 2005 previa períodos de conservação de dados de um ano para os dados telefónicos e de seis meses para os dados da Internet.

67 Artigo 13.º, n.º 1, da Directiva 95/46/CE.

68 Artigo 28º da Directiva 95/46/CE.

de conservação. Dois Estados-Membros (Itália e Finlândia) prevêem a destruição dos dados. Não é claro quais as medidas de segurança técnicas e organizativas, como a autenticação fidedigna ou a gestão pormenorizada dos registos de acesso[69], que foram efectivamente aplicadas. 22 Estados-Membros dispõem de uma autoridade de controlo responsável por verificar a aplicação dos princípios. Na maior parte dos casos, esta autoridade é a responsável pela protecção dos dados. O quadro seguinte fornece mais pormenores.

Quadro 4: Protecção e segurança dos dados; autoridades de controlo		
Estado-Membro	*Disposições da legislação nacional em matéria de protecção e segurança dos dados*	*Autoridade de controlo*
Bélgica	Os operadores têm de assegurar que a transmissão de dados não pode ser interceptada por terceiros, bem como respeitar as normas de segurança e de intercepção lícita das telecomunicações do Instituto Europeu de Normas de Telecomunicações[70]. Aparentemente, a legislação não consagra o princípio da destruição obrigatória dos dados no final do período de conservação.	Instituto dos Serviços Postais e das Telecomunicações
Bulgária	A legislação de transposição prevê a obrigação de aplicar os quatro princípios[71].	A Comissão de Protecção dos Dados Pessoais controla o tratamento e o armazenamento dos dados, assegurando o cumprimento das obrigações. Uma comissão parlamentar da Assembleia Nacional supervisiona os procedimentos de autorização e de acesso aos dados.
República Checa[72]	Ainda não transpôs a Directiva.	
Dinamarca	Os quatro princípios estão previstos[73].	A Agência Nacional para as TI e as Telecomunicações supervisiona se os fornecedores de redes e serviços de comunicações electrónicas asseguram que o equipamento técnico e os sistemas permitem que a polícia aceda à informação sobre tráfego de telecomunicações.
Alemanha	Ainda não transpôs a Directiva.	

69 A autenticação fidedigna («*strong authentication*») exige mecanismos duplos de autenticação, como uma senha acrescida dos dados biométricos ou uma senha mais um testemunho de autenticação («*token*»), de modo a assegurar a presença física da pessoa responsável pelo tratamento dos dados de tráfego. A gestão pormenorizada dos acessos exige o acompanhamento exaustivo do acesso e das operações de tratamento de dados, através da manutenção dos registos da identidade dos utilizadores, hora e data do acesso e ficheiros consultados.

70 Artigo 6.º do Decreto Real de 9 de Janeiro de 2003.

71 Artigo 4.º, n.º 1, da Lei das Comunicações Electrónicas (alterada), 2010.

72 Artigos 87º, n.º 3, e 88.º da Lei 127/2005, com a redacção que lhe foi dada pela Lei n.º 247/2008; artigo 2.º da Lei 336/2005; artigo 3.º, n.º 4, da Lei 485/2005; artigo 28.º, n.º 1, da Lei 101/2000.

73 Lei sobre o Tratamento dos Dados Pessoais; Decreto n.º 714 de 26 de Junho de 2008, relativo aos serviços de redes e de comunicações electrónicas.

Quadro 4: Protecção e segurança dos dados; autoridades de controlo		
Estado-Membro	*Disposições da legislação nacional em matéria de protecção e segurança dos dados*	*Autoridade de controlo*
Estónia	A legislação de transposição prevê três dos quatro princípios. Não existe qualquer disposição específica relativa ao quarto princípio mas todas as pessoas cuja privacidade seja violada por actividades de vigilância podem solicitar a destruição desses dados, mediante decisão judicial[74].	A autoridade responsável é a Autoridade de Fiscalização Técnica.
Irlanda[75]	A legislação de transposição prevê a obrigação de aplicar os quatro princípios.	O juiz designado tem competência para averiguar e fazer relatórios sobre o cumprimento pelas autoridades nacionais competentes do disposto na legislação de transposição.
Grécia[76]	A legislação de transposição prevê a obrigação de aplicar os quatro princípios, bem como a exigência suplementar de os operadores prepararem e aplicarem um plano para assegurar o seu cumprimento, sob a supervisão de um responsável pela segurança dos dados.	Autoridade responsável pela Protecção dos Dados Pessoais e pela Privacidade das Comunicações.
Espanha[77]	As disposições em vigor em matéria de protecção dos dados abrangem três dos quatro princípios (qualidade e segurança dos dados conservados, acesso por pessoas autorizadas e protecção contra tratamento não autorizado).	A autoridade responsável é a Agência de Protecção dos Dados.
França[78]	A legislação de transposição prevê a obrigação de aplicar os quatro princípios.	A Comissão Nacional da Informática e das Liberdades supervisiona o cumprimento das obrigações.
Itália	Não existem disposições específicas em matéria de segurança dos dados conservados, embora exista uma obrigação geral de destruição ou anonimização dos dados de tráfego e de tratamento consensual dos dados de localização[79].	A Autoridade de Protecção dos Dados supervisiona o cumprimento da Directiva pelos operadores
Chipre[80]	A legislação de transposição contempla os quatro princípios.	O Comissário para a Protecção dos Dados Pessoais supervisiona a aplicação da legislação de transposição.

74 Artigo 111.º, n.º 9, da Lei relativa às Comunicações Electrónicas; Artigo 122.°, n.º 2, do Código de Processo Penal.

75 Artigos 4.º, 11.º e 12.º da Lei relativa às Comunicações (Conservação de Dados) de 2009.

76 Artigo 6.º da Lei 3917/2011.

77 Artigo 8.º da Lei 25/2007, artigo 38.º, n.º 3, da Lei Geral das Telecomunicações. O artigo 9.º prevê derrogações ao acesso e direitos de cancelamento prescritos na Lei Orgânica 15/1999 sobre a protecção dos dados pessoais (artigos 22.º e 23.º).

78 Artigo D.98-5, CPCE; Artigo L-34-1 (V), CPCE; Artigo 34.º da Lei 78-17; Artigo 34-1, CPCE; Artigo 11.º da Lei n.º 78-17 de 6 de Janeiro de 1978.

79 Artigos 123.° e 126.º do Código de Protecção de Dados.

80 Artigos 14.º e 15.º da Lei 183 (I) /2007.

Quadro 4: Protecção e segurança dos dados; autoridades de controlo		
Estado-Membro	*Disposições da legislação nacional em matéria de protecção e segurança dos dados*	*Autoridade de controlo*
Letónia[81]	A legislação de transposição prevê dois dos princípios: a confidencialidade e a autorização do acesso aos dados conservados e a destruição dos dados no final do período de conservação.	A Inspecção Nacional para a Protecção dos Dados supervisiona a protecção dos dados pessoais no sector das comunicações electrónicas, mas não o acesso e o tratamento dos dados conservados.
Lituânia[82]	A legislação de transposição contempla os quatro princípios.	A Inspecção Nacional para a Protecção dos Dados supervisiona a aplicação da legislação de transposição, sendo responsável por fornecer dados estatísticos à Comissão Europeia.
Luxemburgo[83]	A legislação de transposição contempla os quatro princípios.	Autoridade responsável pela Protecção dos Dados
Hungria[84]	A legislação de transposição contempla os quatro princípios.	Comissário Parlamentar para a Protecção dos Dados e a Liberdade de Informação
Malta[85]	A legislação de transposição contempla os quatro princípios.	Comissário para a Protecção dos Dados
Países Baixos[86]	A legislação de transposição contempla os quatro princípios.	A Agência das Radiocomunicações supervisiona o cumprimento das obrigações de acesso à Internet e a actividade dos operadores de telecomunicações; a Autoridade de Protecção dos Dados controla o tratamento geral dos dados pessoais; a cooperação entre estas duas autoridades é regida por um protocolo.
Áustria	Ainda não transpôs a Directiva.	
Polónia	A legislação de transposição contempla os quatro princípios[87].	Autoridade responsável pela Protecção dos Dados
Portugal	A legislação de transposição contempla os quatro princípios[88].	Comissão Nacional de Protecção de Dados (CNPD)
Roménia	Ainda não transpôs a Directiva.	
Eslovénia[89]	A legislação de transposição contempla os quatro princípios.	Comissário para a Informação
Eslováquia[90]	A legislação de transposição contempla os quatro princípios.	A autoridade de fixação dos preços e regulador nacional em matéria de comunicações electrónicas supervisiona a protecção dos dados pessoais.

81 Artigos 4.º, n.º 4, e 71.°, n^{os} 6-8, da Lei das Comunicações Electrónicas.

82 Artigos 12.º, n.º 5, 66.º, n^{os} 8 e 9 da Lei das Comunicações Electrónicas, com a redacção que lhe foi dada em 14 de Novembro de 2009.

83 Artigo 1.°, n.° 5, da Lei de 24 de Julho de 2010.

84 Artigo 157.º da Lei C/2003, com a última redacção que lhe foi dada pela Lei CLXXIV/2007; artigo 2.° do Decreto 226/2003; Lei LXIII/1992 sobre a Protecção dos Dados.

85 Artigos 24.º e 25.º da Lei 198/2008; artigo 40.º, alínea b), da Lei sobre a Protecção dos Dados (Cap. 440).

86 Artigo 13.º, n.º 5, da Lei das Telecomunicações; título completo do protocolo de cooperação: *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens.*

87 Artigo 180.º-A e 180.º-E da Lei das Telecomunicações.

88 Artigos 7.°, n.^{os} 1 e 5, e 11.° da Lei 32/2008; artigos 53.º e 54.º da Lei sobre a Protecção dos Dados Pessoais.

89 Artigo 107.º-A (n.º 6) e 107.º-C da Lei das Comunicações Electrónicas.

Quadro 4: Protecção e segurança dos dados; autoridades de controlo		
Estado-Membro	*Disposições da legislação nacional em matéria de protecção e segurança dos dados*	*Autoridade de controlo*
Finlândia	A legislação de transposição apenas prevê expressamente a obrigação de destruição dos dados no final do período de conservação[91].	A Autoridade Reguladora das Comunicações supervisiona o cumprimento pelos operadores das normas em matéria de conservação de dados pessoais. O Provedor para a Protecção de Dados supervisiona o cumprimento das normas em matéria de tratamento dos dados pessoais.
Suécia	Ainda não transpôs a Directiva.	
Reino Unido	A legislação de transposição contempla os quatro princípios[92].	O Comissário para a Informação supervisiona a conservação e/ou o tratamento dos dados das comunicações (e quaisquer outros dados pessoais), assegurando o controlo adequado em matéria de protecção dos dados. O Comissário para as Intercepções de Comunicações (um magistrado superior em funções ou já aposentado) supervisiona a recolha de dados das comunicações pelas autoridades públicas ao abrigo da lei RIPA. Um tribunal com competências de inquérito investiga as queixas por utilização abusiva dos dados adquiridos ao abrigo da legislação de transposição (lei RIPA).

A transposição do artigo 7.° para as legislações dos vários Estados-Membros foi efectuada de forma incoerente. Na medida em que os dados conservados constituem, potencialmente, informações de carácter extremamente pessoal e sensível, devem ser observadas, ao longo de todo o processo de conservação dos dados, normas rigorosas quanto à protecção e à segurança dos mesmos, bem como ao seu armazenamento, extracção e utilização, de forma coerente e visível, de modo a minimizar os riscos de violação da privacidade e preservar a confiança dos cidadãos. A Comissão vai analisar as possibilidades de reforçar as normas em matéria de protecção e segurança dos dados, nomeadamente a introdução de soluções de «segurança e privacidade de raiz» (*privacy-by-design*) de forma a assegurar o cumprimento dessas normas, tanto a nível da conservação como da transmissão dos dados. A Comissão terá igualmente em conta as recomendações efectuadas no relatório sobre a segunda acção comum de controlo da aplicação da legislação pelo Grupo de Trabalho «Artigo 29.°» para a Protecção dos Dados, no sentido de serem adoptadas normas mínimas e medidas de salvaguarda e de segurança técnica e organizacional[93].

4.7. Estatísticas (artigo 10.º)

Os Estados-Membros devem fornecer à Comissão dados estatísticos anuais sobre a conservação de dados, nomeadamente sobre:

---

90 Artigo 59.º-A da Lei relativa às Comunicações Electrónicas; Artigo S-33.º da Lei 428/2002 sobre a Protecção dos Dados Pessoais.

91 Artigo 16.º, n.º 3, da Lei sobre as Comunicações Electrónicas.

92 Artigo 6.º do Regulamento relativo à Conservação de Dados.

93 Parecer n.º 3/2006 (wp119) do Grupo de Trabalho do «Artigo 29.º» para a Protecção dos Dados; Relatório 01/2010.

– os casos em que foram transmitidas informações às autoridades competentes em conformidade com o direito nacional aplicável;

– o período de tempo decorrido entre a data a partir da qual os dados foram conservados e a data em que as autoridades competentes solicitaram a sua transmissão (ou seja, a antiguidade dos dados); e

– os casos em que os pedidos de dados não puderam ser satisfeitos.

Ao solicitar dados estatísticos nos termos do artigo 10.º da Directiva, a Comissão convidou os Estados-Membros a fornecerem pormenores sobre os casos concretos de pedidos de dados. Os dados estatísticos fornecidos divergiam, todavia, quanto ao seu âmbito e pormenor: nas suas respostas, alguns Estados-Membros efectuavam uma distinção entre os diferentes tipos de comunicações, outros indicavam a antiguidade dos dados no momento do pedido, enquanto outros apenas forneceram estatísticas anuais sem qualquer discriminação. 19 Estados-Membros[94] forneceram dados estatísticos sobre o número de pedidos de dados em 2009 e/ou 2008. Entre estes figuravam a Irlanda, a Grécia e a Áustria, países a que foram solicitados dados não obstante o facto de a legislação não ter ainda sido transposta na altura, assim como a República Checa e a Alemanha, cuja legislação de conservação dos dados foi anulada. 7 Estados-Membros que transpuseram a Directiva não forneceram quaisquer dados estatísticos, embora a Bélgica tenha fornecido uma estimativa do volume anual dos pedidos de dados telefónicos (300 000).

A disponibilidade de dados quantitativos e qualitativos fidedignos é essencial para demonstrar a necessidade e a importância de medidas de segurança como a conservação de dados. Essa importância foi reconhecida no plano de acção de 2006 para a avaliação estatística da criminalidade e da justiça penal[95], que previa a definição de uma metodologia de recolha regular de dados, em conformidade com as disposições da Directiva, assim como a inclusão dessas estatísticas na base de dados do Eurostat (desde que satisfizessem as normas de qualidade). Não foi possível satisfazer este objectivo pois a maior parte dos Estados-Membros apenas concluiu a transposição integral da Directiva nos últimos dois anos, tendo utilizado diferentes interpretações para a fonte das estatísticas. Na sua futura proposta de revisão da Directiva relativa à conservação de dados, juntamente com a revisão do plano de acção sobre as estatísticas, a Comissão irá procurar definir procedimentos viáveis para a medição e a apresentação de relatórios, que permitam controlar, de uma forma transparente e adequada, a conservação dos dados, sem impor encargos desnecessários aos sistemas de justiça penal e às autoridades responsáveis pela aplicação da lei.

4.8. Transposição nos países do Espaço Económico Europeu

Já foi adoptada legislação em matéria de conservação de dados na Islândia, no Liechtenstein e na Noruega[96].

---

94 República Checa, Dinamarca, Alemanha, Estónia, Irlanda, Grécia, Espanha, França, Chipre, Letónia, Lituânia, Malta, Países Baixos, Áustria, Polónia, Eslovénia, Eslováquia, Finlândia e Reino Unido,

95 Comunicação da Comissão (COM(2006) 437, «Elaboração de uma estratégia europeia global e coerente para a avaliação estatística da criminalidade e da justiça penal: Plano de Acção da UE para 2006-2010»

96 Na Islândia, a lei que transpõe a Directiva é a Lei das Telecomunicações 81/2003 (com a redacção que lhe foi dada em Abril de 2005); no Liechtenstein é a Lei das Telecomunicações de 2006. Na Noruega a lei de transposição foi votada em 5 de Abril de 2011 e aguarda actualmente a aprovação real.

4.9. Decisões dos Tribunais Constitucionais sobre as legislações de transposição

Os tribunais constitucionais da Roménia, em Outubro de 2009, da Alemanha, em Março de 2010, e da República Checa, em Março de 2011, anularam a legislação de transposição da Directiva para as respectivas jurisdições, tendo-as considerado inconstitucionais. O Tribunal Constitucional da Roménia[97] reconheceu que a interferência com os direitos fundamentais pode ser autorizada se respeitar determinadas normas e assegurar salvaguardas suficientes para proteger os cidadãos contra eventuais intervenções arbitrárias por parte do Estado. Contudo, com base na jurisprudência do Tribunal Europeu dos Direitos do Homem[98], o tribunal considerou que a legislação de transposição era ambígua quanto ao seu âmbito de aplicação e finalidade, não proporcionando suficientes garantias, questionando se a «obrigação jurídica contínua» de conservar todos os dados de tráfego durante 6 meses seria compatível com os direitos à privacidade e à liberdade de expressão consagrados no artigo 8º da Convenção Europeia dos Direitos do Homem.

O Tribunal Constitucional da Alemanha[99] considerou que a conservação de dados gerava um sentimento de vigilância que poderia prejudicar o livre exercício dos direitos fundamentais. Reconheceu expressamente que a conservação de dados para fins estritamente limitados e com um nível suficientemente elevado de segurança dos dados não violaria, necessariamente, a Constituição da Alemanha. Contudo, salientou que a conservação desses dados constituía uma grave restrição ao direito à vida privada e que, consequentemente, só seria admissível em circunstâncias muito limitadas, e que um período de conservação de dados de seis meses seria o limite máximo (*«an der Obergrenze»)* do que poderia ser considerado proporcionalmente adequado (ponto 215). Os dados só podem ser pedidos nos casos em que exista já a suspeita da prática de uma infracção penal grave ou elementos que provem a existência de riscos para a segurança pública, devendo a sua extracção ser proibida relativamente a determinadas comunicações privilegiadas (nomeadamente as relacionadas com necessidades emocionais ou sociais) que têm por base a confidencialidade. Os dados deveriam também ser cifrados, com uma supervisão transparente da sua utilização.

O Tribunal Constitucional da República Checa[100] anulou a legislação de transposição com fundamento no facto de, tratando-se de uma medida que diz respeito a direitos fundamentais, a sua formulação não ser suficientemente clara e precisa. O Tribunal criticou a insuficiente limitação dos objectivos atendendo à escala e ao âmbito das exigências de conservação de dados. Alegou também a falta de uma definição rigorosa na legislação de transposição das autoridades competentes para aceder e utilizar os dados conservados, assim como os procedimentos adoptados para garantir a integridade e a confidencialidade dos dados. Os cidadãos, por conseguinte, não dispunham de garantias suficientes contra eventuais abusos de poder por parte das autoridades públicas. O Tribunal não criticou a Directiva em si mesma, tendo considerado que esta deixava uma margem suficiente à República Checa para efectuar a transposição respeitando a Constituição. Não obstante, numa observação incidental (*obter dictum)*, o Tribunal expressou as suas dúvidas quanto à necessidade, eficácia e adequação da conservação de dados de tráfego, dadas as novas formas de criminalidade através da utilização de cartões SIM anónimos.

---

97 Decisão n.º 1 258, de 8 de Outubro de 2009, do Tribunal constitucional da Roménia.

98 Tribunal Europeu dos Direitos do Homem: Processos Rotaru / Roménia, 2000, Sunday Times / Reino Unido, 1979, e Príncipe Hans-Adam do Liechtenstein / Roménia, 2001.

99 Bundesverfassungsgericht, 1 BvR 256/08 de 2 de Março de 2010, pontos 1 – 345.

100 Acórdão do Tribunal Constitucional da República Checa de 22 de Março relativo à lei n.° 127/2005 e ao decreto n.° 485/2005; ver, nomeadamente, os pontos 45 a 48, 50 a 51 e 56.

Estes três Estados-Membros estão agora a analisar a forma como irão proceder a uma nova transposição da Directiva. Foram também intentadas acções judiciais em matéria de conservação de dados perante o tribunal constitucional da Bulgária, que deu origem a uma alteração da legislação de transposição, perante o Tribunal Constitucional de Chipre que considerou as sentenças judiciais proferidas ao abrigo da legislação de transposição inconstitucionais, e perante o Tribunal Constitucional da Hungria, onde se encontra pendente um processo relativo à omissão da finalidade jurídica do tratamento dos dados na legislação de transposição[101].

Na sua futura proposta de revisão da Directiva relativa à conservação de dados, a Comissão irá ter em consideração as questões suscitadas pela jurisprudência dos Estados-Membros.

4.10. Aplicação actual da Directiva

A Comissão espera que os Estados-Membros que ainda não transpuseram integralmente a Directiva, ou que ainda não adoptaram legislação que substitua a legislação de transposição anulada pelos tribunais nacionais, o façam o mais rapidamente possível. Se tal não suceder, a Comissão reserva-se o direito de exercer os poderes que lhe foram conferidos pelos Tratados da UE. Até à data, dois Estados-Membros que ainda não transpuseram a Directiva (Áustria e Suécia) foram considerados culpados pelo Tribunal de Justiça de incumprimento das obrigações que lhes incumbem por força da legislação da UE[102]. Em Abril de 2011, a Comissão decidiu intentar um segundo recurso contra a Suécia perante o Tribunal, por incumprimento do acórdão proferido no processo C-185/09, solicitando a imposição de sanções financeiras a título do artigo 260.º do Tratado sobre o Funcionamento da União Europeia, na sequência da decisão do Parlamento sueco de adiar por 12 meses a adopção da legislação de transposição. A Comissão continua a acompanhar de perto a situação na Áustria, que já transmitiu um calendário para a adopção, em breve, da legislação de transposição.

5. PAPEL DOS DADOS CONSERVADOS NA JUSTIÇA PENAL E NA APLICAÇÃO DA LEI

A presente secção resume as funções desempenhadas pelos dados conservados, tal como descritas pelos Estados-Membros nas suas contribuições para o processo de avaliação da aplicação da Directiva.

5.1. Volume dos dados conservados a que as autoridades nacionais competentes tiveram acesso

O volume do tráfego de telecomunicações e dos pedidos de acesso a esses dados tem vindo a aumentar. As estatísticas fornecidas por dezanove Estados-Membros em relação aos anos de 2008 e/ou 2009 indicam que, na totalidade da UE, são anualmente formulados mais de dois milhões de pedidos de dados, havendo uma variação considerável entre os diferentes Estados-Membros: desde menos de cem (Chipre) e mais de um milhão (Polónia) por ano. Segundo as informações sobre o tipo de dados solicitados fornecidas por doze Estados-Membros em

---

101 Supremo Tribunal administrativo da Bulgária, Decisão n.º 13627 de 11 de Dezembro de 2008; Supremo Tribunal de Chipre, processos n.os 65/2009, 78/2009, 82/2009 e 15/2010-22/2010, de 1 de Fevereiro de 2011; a apreciação da constitucionalidade foi suscitada pela União das Liberdades Civis da Hungria, em 2 de Junho de 2008.

102 Processos C-189/09 e C-185/09, respectivamente.

relação a 2008 ou a 2009, os tipos de dados mais frequentemente solicitados dizem respeito às chamadas telefónicas da rede móvel (ver quadros 5, 8 e 12). Os dados estatísticos não indicam o objectivo preciso dos diferentes pedidos apresentados. A República Checa, a Letónia e a Polónia afirmaram que, no caso dos dados relativos à rede telefónica móvel, as autoridades competentes tinham de apresentar o mesmo pedido a cada um dos principais operadores da rede móvel, e que, por conseguinte, o número efectivo de pedidos por cada caso fora consideravelmente inferior ao que as estatísticas sugeriam.

Não existe uma explicação óbvia para estas variações, embora a dimensão da população, a evolução das tendências da criminalidade, as limitações quanto às finalidades e as condições de acesso ou os custos de extracção dos dados sejam factores a ter conta.

5.2. Antiguidade dos dados conservados que foram objecto de acesso

Com base na repartição estatística dos dados fornecidos por nove Estados-Membros[103] para 2008 (ver resumo no Quadro 5 e outros pormenores no Anexo), cerca de 90 % dos dados acedidos pelas autoridades competentes nesse ano tinham seis meses ou menos e cerca de 70 % três meses ou menos quando foi introduzido o pedido de acesso (inicial).

Quadro 5: Antiguidade dos dados conservados acedidos nos nove Estados-Membros que forneceram dados estatísticos discriminados por tipos de dados em 2008

Antiguidade	*Rede fixa*	*Rede móvel*	*Dados da Internet*	*Total*
Menos de 3 meses	61%	70%	56%	67%
3-6 meses	28%	18%	19%	19%
6-12 meses	8%	11%	18%	12%
Mais de 1 ano	3%	1%	7%	2%

Segundo a maior parte dos Estados-Membros, a utilização dos dados conservados com mais de três meses, ou mesmo seis meses, é menos frequente, mas pode revelar-se fundamental. Em termos de utilização podem ser distinguidas três categorias. Em primeiro lugar, os dados relativos à Internet são normalmente solicitados mais tarde do que os outros meios de prova no âmbito das investigações criminais. A análise dos dados das comunicações telefónicas (redes fixa e móvel) gera, muitas vezes, potenciais pistas de investigação, que podem dar origem a novos pedidos de dados mais antigos. Por exemplo, se, durante uma investigação é identificado um nome a partir das comunicações da rede fixa ou da rede móvel, os investigadores podem querer identificar também o endereço do Protocolo Internet (IP) que essa pessoa utilizava ou identificar as pessoas com quem ela entrou em contacto durante um determinado período de tempo através desse endereço IP. Nesse caso, os inspectores podem solicitar dados que permitam identificar também as comunicações com outros endereços IP e a identidade das pessoas que utilizaram esses endereços.

Em segundo lugar, a investigação dos crimes particularmente graves, dos crimes em série, do crime organizado e dos atentados terroristas implica normalmente o recurso a dados mais antigos, nomeadamente os relativos ao período de tempo necessário para planear esses crimes, de modo a permitir identificar padrões de comportamento criminoso e apurar quais são as relações entre os cúmplices, assim como a existência de dolo. Muitas vezes, as actividades relacionadas com crimes financeiros complexos só são detectadas após vários meses.

[103] República Checa, Dinamarca, Estónia, Irlanda, Espanha, Chipre, Letónia, Malta e Reino Unido.

Em terceiro lugar, e excepcionalmente, alguns Estados-Membros solicitaram dados de tráfego detidos por outro Estado-Membro, os quais só podem, normalmente, ser disponibilizados mediante uma autorização judicial, em resposta a uma carta rogatória emitida por um juiz do Estado-Membro requerente. Este tipo de assistência jurídica mútua pode ser morosa, o que explica por que razão alguns dos dados solicitados tinham mais de seis meses de antiguidade.

5.3. Pedidos transnacionais de dados conservados

As investigações e os processos-crime podem envolver elementos de prova ou testemunhas provenientes de diversos Estados-Membros, ou eventos que tiveram lugar em mais do que um Estado-Membro. Segundo as estatísticas fornecidas pelos Estados-Membros, menos de 1% de todos os pedidos de dados diziam respeito a dados detidos por outro Estado-Membro. As autoridades responsáveis pela aplicação da lei indicaram que preferem pedir os dados aos operadores nacionais, que podem ter esses dados armazenados, em vez de recorrer ao processo de assistência jurídica mútua, que pode ser moroso e não fornece quaisquer garantias de que o acesso aos dados será autorizado. A Decisão-Quadro 2006/960/JAI, relativa à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia[104], que define os prazos para a apresentação de informações na sequência de um pedido apresentado por um outro Estado-Membro, não é aplicável neste caso porque os dados conservados são considerados informações obtidas por meios coercivos, que não são abrangidas pelo seu âmbito de aplicação. Todavia, nenhum Estado-Membro ou autoridade responsável pela aplicação da lei preconizou alguma vez a simplificação do intercâmbio transnacional de dados.

5.4. Valor dos dados conservados em investigações penais ou em processos-crime

Embora o número absoluto de pedidos de dados não reflicta necessariamente o valor dos dados para as investigações criminais concretas, os Estados-Membros indicaram geralmente que a conservação de dados é, no mínimo, importante e, em alguns casos, indispensável[105], para prevenir e combater a criminalidade, incluindo a protecção das vítimas e a absolvição de inocentes em processos-crime. As condenações efectivas assentam na confissão de culpa, em testemunhos ou em provas forenses. Foi referido que os dados de tráfego conservados são necessários para contactar testemunhas que, de outro modo, não poderiam ser identificadas, e para fornecer elementos de prova ou pistas para se apurar a cumplicidade na prática de um crime. Alguns Estados-Membros[106] alegaram ainda que a utilização dos dados conservados permitiu ilibar pessoas suspeitas da prática de crimes, sem ter sido necessário recorrer a outros métodos de vigilância, como as escutas telefónicas ou as buscas domiciliárias, considerados mais intrusivos.

Embora sejam regularmente publicados dados sobre a criminalidade e a justiça na União Europeia, não existe uma definição geral de «crime grave» e, por conseguinte, não existem

---

104 Decisão-Quadro 2006/960/JAI do Conselho, de 18 de Dezembro de 2006, relativa à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia, JO L 386 de 29.12.2006. pp. 89-100 e JO L 200 de 1.8.2007. pp. 637-648.

105 A República Checa considerou a conservação de dados como «absolutamente indispensável num grande número de processos»; a Hungria indicou que é «indispensável para a actividade normal [dos organismos responsáveis pela aplicação da lei]»; a Eslovénia indicou que a falta de dados conservados «paralisaria a actividade dos organismos responsáveis pela aplicação da lei»; os serviços de polícia do Reino Unido consideraram a disponibilidade dos dados de tráfego como «absolutamente fundamental ... para investigar as ameaças terroristas e os crimes graves.»

106 Alemanha, Polónia, Eslovénia e Reino Unido.

estatísticas da UE sobre a incidência da criminalidade grave ou sobre as investigações ou processos relativos a este tipo de crimes. O volume global dos pedidos de dados conservados comunicados pelos dezanove Estados-Membros que forneceram informações em relação a 2009 e/ou 2008 foi de, aproximadamente, 2,6 milhões. Tendo em conta as últimas estatísticas em matéria de criminalidade e justiça penal disponíveis para estes dezanove Estados-Membros - relativas a todos os crimes comunicados e não apenas aos crimes graves - pode afirmar-se que se registaram, em média, ligeiramente mais de dois pedidos anuais por cada agente de polícia, ou seja, cerca de 11 pedidos por cada 100 crimes registados[107].

Com base nos dados estatísticos e nos exemplos fornecidos, que associam a utilização dos dados históricos conservados das comunicações ao número de condenações, absolvições, processos arquivados e crimes evitados, podem extrair-se diversas conclusões quanto ao papel e ao valor dos dados conservados para efeitos de investigação criminal.

Estabelecer pistas de investigação

Em primeiro lugar, os dados conservados permitem construir pistas de investigação que possam conduzir a uma infracção. Os dados são utilizados para compreender as actividades e as ligações entre suspeitos, ou para corroborar outros meios de prova. Os dados de localização, em particular, têm sido utilizados, tanto pelas autoridades responsáveis pela aplicação da lei como pelos arguidos, para excluir suspeitos da prática de um crime ou confirmar álibis. Essas provas podem, pois, fazer com que certas pessoas deixem de ser alvo de investigações criminais, eliminando assim a necessidade de investigações mais intrusivas ou conduzindo à sua absolvição em tribunal. A Bélgica referiu a condenação, em 2008, dos autores do rapto de um funcionário de um tribunal criminal de Antuérpia, Neste processo, os dados de localização permitiram associar as actividades levadas a cabo pelos malfeitores em três localidades distintas, o que se revelou determinante para convencer o júri da sua cumplicidade. Num outro processo, relativo a um homicídio cometido em 2007 a que estava associado um gang de motociclistas, os dados de localização dos telemóveis dos autores do crime provaram que estes se encontravam na zona em que o homicídio teve lugar, o que deu origem a uma confissão parcial[108]. Segundo a Bélgica, a Irlanda e o Reino Unido, certos crimes envolvendo comunicações através da Internet *só* podem ser investigados através da conservação de dados: por exemplo, é frequente que as ameaças de violência expressas em fóruns de discussão em linha, muitas vezes, não deixem qualquer rasto, excepto os dados de tráfego no ciberespaço. Uma situação idêntica sucede no caso dos crimes executados por via telefónica. A Hungria e a Polónia referiram um caso de burla de idosos no final de 2009/início de 2010, efectuada através de chamadas telefónicas, cujos autores fingiam ser familiares que precisavam de um empréstimo e que só puderam ser identificados graças aos dados telefónicos que foram conservados.

Dar início a investigações criminais

---

107 Em 2007, existiam na UE-27 1,7 milhões de agentes de polícia, dos quais 1,2 milhões nos dezanove Estados-Membros que forneceram estatísticas sobre os pedidos de dados conservados; em 2007, foram registadas nas várias forças policiais da UE 29,2 milhões de crimes, dos quais 24 milhões nos dezanove Estados-Membros que forneceram dados estatísticos. (Fonte: Eurostat 2009).

108 National Policing Improvement Agency (Reino Unido), *The Journal of Homicide and Major Incident Investigation*, Volume 5, n.º 1, Primavera de 2009, pp. 39-51.

Em segundo lugar, já houve casos em que, na falta de provas forenses ou testemunhais, a única forma de poder iniciar uma investigação criminal foi a partir da consulta dos dados conservados. A Alemanha referiu o caso do homicídio de um polícia, em que o autor do crime fugiu na viatura da vítima, tendo-a posteriormente abandonado. Foi possível apurar que o autor do crime tinha telefonado para tentar obter um meio de transporte alternativo. Não existiam provas forenses ou testemunhais quanto à identidade do assassino e as autoridades tiveram de recorrer aos dados de tráfego para poder avançar com a investigação. Nos casos de abuso sexual de crianças através da Internet, a conservação de dados tem sido indispensável para o êxito das investigações. Juntamente com outras técnicas de investigação, a conservação de dados permite identificar os consumidores de conteúdos de abuso sexual de crianças[109], ajudando a identificar e a proteger as crianças vítimas desses abusos. A República Checa indicou que, sem o acesso aos dados da Internet conservados teria sido impossível dar início às investigações no âmbito da Operação Vilma sobre uma rede de utilizadores e divulgadores de pornografia infantil. A nível da União Europeia, a eficácia da Operação Rescue (sob os auspícios da Europol) para proteger as crianças contra os abusos sexuais foi dificultada porque a falta de legislação de transposição em matéria de conservação de dados impediu alguns Estados-Membros de investigarem os membros de vasta rede pedófila internacional utilizando endereços IP cuja antiguidade podia atingir mais de um ano.

Na investigação do cibercrime, os endereços IP constituem, muitas vezes, a primeira pista. As autoridades responsáveis pela aplicação da lei podem, através da recolha dos dados de tráfego, identificar o assinante do endereço IP antes de decidirem se avançam ou não com uma investigação criminal. Podem também permitir à polícia prevenir as potenciais vítimas de ciberataques: quando a polícia consegue confiscar um servidor de comando e controlo utilizado pelos operadores de *Botnet*, só consegue ver os endereços IP ligados a esse servidor; todavia, através do acesso aos dados conservados, a polícia pode identificar e prevenir as potenciais vítimas detentoras desses endereços IP.

Os dados conservados fazem parte integrante da investigação criminal

Em terceiro lugar, embora as autoridades responsáveis pela aplicação da lei e os tribunais da maior parte dos Estados-Membros não mantenham estatísticas sobre que tipo de provas foram determinantes para assegurar uma condenação ou absolvição, os dados conservados fazem parte integrante da investigação e da repressão do crime na UE. Alguns Estados-Membros referiram que nem sempre podiam isolar o contributo dos dados conservados para o êxito da investigação ou da repressão criminal porque os tribunais tinham em conta todas as provas que lhes eram apresentadas, raramente considerando elementos de prova isolados como sendo conclusivos[110]. Os Países Baixos comunicaram que, entre Janeiro e Julho de 2010, os dados de tráfego históricos foram um factor determinante em 24 sentenças judiciais. A Finlândia indicou que em 56% dos 3 405 pedidos formulados, os dados conservados foram considerados «importantes» ou «essenciais» para a detecção e/ou repressão em processos penais. O Reino Unido forneceu dados a fim de quantificar o impacto de conservação de dados nos processos-crime. Informou ainda que, para três das suas autoridades responsáveis

---

109 O projecto de «medição e a análise da actividade P2P (*peer-to-peer*) contra conteúdos pedófilos», financiado no âmbito do programa Para uma Internet mais segura, forneceu informações precisas sobre a pedofilia no sistema de comunicação *peer-to-peer* eDonkey, permitindo a identificação de 178 000 utilizadores que solicitaram conteúdos pedófilos (num total de 89 milhões de utilizadores controlados).

110 Bélgica, República Checa e Lituânia.

pela aplicação da lei, os dados conservados foram necessários na maioria, se não mesmo em todas, as investigações que deram origem a processos-crime ou a condenações.

5.5. Evolução tecnológica e utilização de cartões SIM pré-pagos

A aplicação da lei tem de acompanhar o ritmo dos novos desenvolvimentos tecnológicos que são utilizados para praticar crimes ou encorajar a criminalidade. A conservação de dados é um dos instrumentos necessários para que a investigação criminal possa fazer face, de uma forma gerível e eficaz em termos de custos, aos desafios da criminalidade contemporânea, em toda a sua diversidade, volume e rapidez. Diversas formas de comunicação cada vez mais comuns encontram-se fora do âmbito de aplicação da Directiva. As redes privadas virtuais, por exemplo, das universidades ou das grandes empresas, permitem a vários utilizadores acederem à Internet através de um ponto de acesso único, com o mesmo endereço IP. Estão actualmente a ser introduzidas novas tecnologias que permitem a atribuição de endereços individuais aos utilizadores destas redes privadas virtuais.

A percentagem de utilizadores de telefones móveis que utilizam serviços pré-pagos varia dentro do território da UE. Alguns Estados-Membros declararam que o anonimato proporcionado pelos cartões SIM pré-pagos, em especial quando são adquiridos noutro Estado-Membro, pode ser aproveitado por pessoas envolvidas em actividades criminosas para evitar a sua identificação em investigações criminais[111]. Seis Estados-Membros (Dinamarca, Espanha, Itália, Grécia, Eslováquia e Bulgária) adoptaram medidas que exigem o registo dos cartões SIM pré-pagos. Estes e outros Estados-Membros (Polónia, Chipre e Lituânia) mostraram-se favoráveis a uma acção a nível da UE para impor o registo obrigatório da identidade dos utilizadores de serviços pré-pagos. Não foi, todavia, fornecida qualquer prova quanto à eficácia dessas medidas nacionais. Forem referidas algumas das suas potenciais limitações, nomeadamente em caso de roubo de identidade ou quando o cartão SIM é adquirido por um terceiro ou o utilizador esteja em *roaming* com um cartão adquirido num país terceiro. De um modo geral, a Comissão não está convencida de que, nesta fase, seja necessária qualquer acção neste domínio a nível da UE.

6. IMPACTO DA CONSERVAÇÃO DOS DADOS NOS OPERADORES E NOS CONSUMIDORES

6.1. Operadores e consumidores

Numa declaração conjunta apresentada à Comissão, cinco das principais associações sectoriais consideraram que o impacto económico da Directiva foi «considerável» ou «enorme» para os pequenos operadores, na medida em que deixava uma «ampla margem de manobra»[112]. Oito operadores transmitiram estimativas, muito variáveis, quanto ao custo em termos de capital e de despesas operacionais para dar cumprimento à Directiva. Estas alegações podem ser confirmadas pelas indicações quanto aos níveis de reembolso dos custos dos operadores que foram transmitidos por quatro Estados-Membros (ver Quadro 6).

Um estudo realizado antes da transposição da Directiva na maior parte dos Estados-Membros estimou o custo da criação de um sistema de conservação de dados por um fornecedor de

---

111 Conclusões do Conselho sobre a luta contra a utilização criminosa e a utilização anónima das comunicações electrónicas.

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

serviços da Internet com meio milhão de clientes em, aproximadamente, 375 240 EUR no primeiro ano, e em 9 870 EUR de custos mensais de funcionamento daí para a frente[113]. Os custos da criação de um sistema de extracção de dados foram estimados em 131 190 EUR e os custos de funcionamento em 28 960 EUR por mês. O Tribunal Constitucional da Alemanha considerou, contudo, no seu acórdão de 2 de Março de 2010, que a imposição de uma obrigação de conservação de dados não era «excessivamente onerosa para os fornecedores de serviços da Internet afectados [nem] desproporcionada quanto aos encargos financeiros a suportar pelas empresas em consequência desse dever de conservação de dados[114].» Os custos unitários da conservação dos dados são inversamente proporcionais à dimensão do operador e ao nível de normalização adoptada pelo Estado-Membro para a interacção com os operadores[115].

Nas suas respostas ao questionário da Comissão, a maioria dos operadores não foi capaz de quantificar o impacto da Directiva sobre a concorrência, os preços a retalho para os consumidores ou os investimentos em novas infra-estruturas e serviços.

Não existe qualquer elemento que indique que a Directiva tenha tido efeitos consideráveis ou quantificáveis sobre os preços dos serviços de comunicações electrónicas para o consumidor. Os representantes dos consumidores não enviaram quaisquer contributos para a consulta pública efectuada em 2009. Uma sondagem efectuada na Alemanha em nome de uma organização da sociedade civil indicou que os consumidores pretendiam mudar os seus comportamentos em matéria de comunicações, evitando utilizar os serviços de comunicações electrónicas em determinadas circunstâncias, mas não existem elementos que corroborem que uma alteração comportamental desse tipo tenha tido lugar em qualquer Estado-Membro ou na União Europeia em geral[116].

A Comissão tenciona avaliar o impacto para o sector e os consumidores de uma futura alteração da Directiva, incluindo, eventualmente, através da realização de um inquérito Eurobarómetro especificamente destinado a avaliar a sensibilidade da opinião pública quanto a estas questões.

6.2. Reembolso dos custos

A Directiva não regulamenta o reembolso dos custos suportados pelos operadores em virtude das suas obrigações de conservação de dados. Estes custos podem ser encarados como:

(a) *despesas de funcionamento*, ou seja, **custos de funcionamento** ou custos recorrentes, relacionados com o funcionamento da empresa, de um dispositivo, componente, peça de equipamento ou das instalações; e

(b) *despesas de capital*, ou seja, as despesas que geram benefícios futuros, ou os custos de desenvolvimento ou de fornecimento de partes não consumíveis para

---

113 Wilfried Gansterer & Michael Ilger, Data retention – The EU Directive 2006/24/EC from a Technological Perspective, Wien: Verlag Medien und Recht, 2008

114 Bundesverfassungsgericht, 1 BvR 256/08 de 2 de Março de 2010, ponto 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx

116 A sondagem foi realizada pela Forsa e encomendada pela AK Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

o produto ou sistema, que podem incluir os custos de pessoal ou relacionados com as instalações e despesas como rendas ou serviços de base.

Todos os Estados-Membros procedem a um reembolso quando os dados são solicitados no âmbito de um processo-crime. Dois Estados-Membros informaram que reembolsavam tanto as despesas de funcionamento como as despesas de capital. Seis Estados-Membros reembolsam apenas as despesas de funcionamento. Nenhum outro sistema de reembolso foi notificado à Comissão. O quadro seguinte fornece mais pormenores.

Quadro 6: Estados-Membros que reembolsam os custos suportados			
Estado-Membro	**Despesas de funcionamento**	**Despesas de capital**	**Custos anuais reembolsados (milhões de EUR)**
Bélgica	Sim	Não	22 (2008)
Bulgária	Não	Não	-
República Checa	Ainda não transpôs a Directiva[117]		
Dinamarca	Sim	Não	-
Alemanha	Ainda não transpôs a Directiva		
Estónia	Sim	Não	-
Irlanda	Não	Não	-
Grécia	Não	Não	-
Espanha	Não	Não	-
França	Sim	Não	-
Itália	-	-	-
Chipre	Não	Não	-
Letónia	Não	Não	-
Lituânia	Sim, se for solicitado e justificado	Não	-
Luxemburgo	Não	Não	-
Hungria	Não	Não	-
Malta	Não	Não	-
Países Baixos	Sim	Não	-
Áustria	Ainda não transpôs a Directiva.		
Polónia	Não	Não	-
Portugal	Não	Não	-
Roménia	Ainda não transpôs a Directiva.		
Eslovénia	Não	Não	-
Eslováquia	Não	Não	-
Finlândia	Sim	Sim	1
Suécia	Ainda não transpôs a Directiva.		
Reino Unido	Sim	Sim	55 (reembolsados globalmente os custos suportados durante três anos)

Pode concluir-se que a Directiva não atingiu plenamente o objectivo de criar condições de concorrência equitativas para todos os operadores da UE. A Comissão irá, por conseguinte, estudar atentamente as alternativas para minimizar os obstáculos ao funcionamento do mercado interno, garantindo que os operadores serão reembolsados de forma mais homogénea

[117] Antes da anulação da lei de transposição, a República Checa procedia ao reembolso das despesas de funcionamento e das despesas de capital, tendo declarado 6,8 milhões de euros de custos de reembolso em 2009.

dos custos que forem obrigados a suportar para cumprir a obrigação de conservação de dados, em especial os pequenos e médios operadores.

7. IMPLICAÇÕES DA CONSERVAÇÃO DE DADOS PARA OS DIREITOS FUNDAMENTAIS

7.1. Direitos fundamentais de respeito pela vida privada e de protecção dos dados pessoais

A conservação de dados constitui uma limitação dos direitos ao respeito pela vida privada e à protecção dos dados de carácter pessoal, que constituem direitos fundamentais da União Europeia[118]. Tal limitação deve, nos termos do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais, «ser prevista por lei e respeitar o conteúdo essencial desses direitos, de acordo com o princípio da proporcionalidade», ser necessária e corresponder efectivamente a objectivos de interesse geral reconhecidos pela União Europeia, ou à necessidade de protecção dos direitos e liberdades de terceiros. Na prática, tal significa que quaisquer limitações devem[119]:

(a) ser formuladas de modo preciso e previsível;

(b) ser necessárias para realizar um objectivo de interesse geral ou para proteger os direitos e liberdades de outrem;

(c) ser proporcionadas tendo em conta o objectivo pretendido; e

(d) respeitar o conteúdo essencial dos direitos fundamentais em causa.

O artigo 8.º, n.º 2, da Convenção Europeia dos Direitos do Homem também reconhece que a ingerência de uma autoridade pública no exercício do direito de uma pessoa à sua vida privada só se justifica se for necessária para a segurança nacional, para a segurança pública, ou para prevenir infracções penais[120]. O artigo 15.º, n.º 1, da Directiva relativa à privacidade e às comunicações electrónicas e os considerandos da Directiva relativa à conservação de dados reiteram estes princípios, em que assenta a abordagem da UE em matéria de conservação de dados.

A jurisprudência posterior do Tribunal de Justiça Europeu e do Tribunal Europeu dos Direitos do Homem permitiu definir as condições a que deve obedecer qualquer limitação do direito à vida privada. Esses acórdãos são pertinentes para determinar se a Directiva deve ser alterada, em especial no que respeita às condições de acesso e de utilização dos dados conservados.

---

118 Os artigos 7.° e 8.° da Carta dos Direitos Fundamentais da União Europeia (JO C 83 de 30.3.2010, p. 389), garantem a todas as pessoas o direito à «protecção dos dados de carácter pessoal que lhes digam respeito». O artigo 16.° do Tratado sobre o Funcionamento da União Europeia (JO C 83 de 30.3.2010, p. 1) consagra igualmente o direito de todas as pessoas à «protecção dos dados de carácter pessoal que lhes digam respeito».

119 Ver a «lista de controlo» dos direitos fundamentais para todas as propostas legislativas da Comissão que figura na Comunicação da Comissão COM (2010) 573/4, «Estratégia para a aplicação efectiva da Carta dos Direitos Fundamentais pela União Europeia».

120 Ver artigo 8.° da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdades Fundamentais (STE n.° 5), Conselho da Europa, 4.11.1950.

Qualquer limitação do direito à vida privada deve ser formulada de modo preciso e garantir a previsibilidade

No processo Österreichischer Rundfunk, o Tribunal de Justiça Europeu considerou que qualquer interferência da lei com o direito à vida privada deve ser «redigida com precisão suficiente para permitir que o cidadão possa adaptar o seu comportamento em conformidade... [de modo a] a respeitar a exigência de previsibilidade.»

Qualquer limitação do direito à vida privada deve ser necessária e acompanhada de salvaguardas essenciais

No processo Copland contra Reino Unido, relativo ao controlo pelo Estado das chamadas telefónicas, do correio electrónico e da utilização da Internet por parte de um cidadão, o Tribunal Europeu dos Direitos do Homem considerou que essa restrição do direito à vida privada só podia ser considerada necessária se tivesse por base legislação nacional aplicável[121]. No processo S. e Marper contra Reino Unido, relativo à conservação dos perfis ADN ou de impressões digitais de qualquer pessoa absolvida da prática de um crime ou cujo processo tenha sido arquivado antes de qualquer condenação, o Tribunal de Justiça concluiu que uma tal restrição do direito à vida privada só poderia ser justificada se respondesse a uma necessidade social premente, fosse proporcional relativamente ao objectivo perseguido e as justificações apresentadas pela autoridade pública fossem pertinentes e suficientes[122]. Os princípios fundamentais da protecção de dados exigem que a sua conservação seja proporcionada em relação aos objectivos da recolha dos dados e que o período dessa conservação seja limitado»[123]. Para as escutas telefónicas, as medidas de vigilância secreta e os serviços de informações secretas «[seria] essencial… dispor de regras claras e pormenorizadas sobre o âmbito e a aplicação dessas medidas, bem como garantias mínimas no que se refere, nomeadamente, à duração, ao armazenamento, à utilização, ao acesso de terceiros, aos procedimentos para preservar a integridade e a confidencialidade dos dados, assim como para a sua destruição, proporcionando assim garantias suficientes contra o risco de abusos e de arbitrariedade.»

Qualquer limitação do direito à vida privada deve ser proporcional ao interesse geral

Do mesmo modo, o Tribunal de Justiça Europeu, no acórdão proferido no processo Schecke & Eifert, relativo à publicação na Internet da identidade de todos os beneficiários de subvenções agrícolas[124], considerou que, aparentemente, o legislador da UE não teria tomado as medidas adequadas para garantir um equilíbrio entre o respeito pelo conteúdo essencial do direito à vida privada e o interesse geral (transparência), tal como reconhecidos pela UE. Mais concretamente, o Tribunal considerou que o legislador não teria tido em consideração outros métodos que pudessem ser mais conformes com os objectivos e que fossem ao mesmo tempo menos lesivos do direito dos beneficiários das subvenções ao respeito da sua vida privada e à protecção dos seus dados pessoais. Consequentemente, o Tribunal considerou que o legislador

---

121 *Copland contra Reino Unido*, acórdão do Tribunal Europeu dos Direitos do Homem, Estrasburgo 3.4.2007, p. 9.

122 *Marper contra Reino Unido*, acórdão do Tribunal Europeu dos Direitos do Homem, Estrasburgo, 4.12.2008, p. 31.

123 *Marper*, p. 30.

124 Processo C-92/09 Volker e Markus Schecke GbR / Land Hessen e C-93/09 Eifert / Land Hessen e Bundesanstalt für Landwirtschaft und Ernährung, de 9.11.1010.

havia excedido os limites da proporcionalidade, na medida em que as limitações em matéria de protecção dos dados pessoais «devem ocorrer na medida estrita do necessário.»

7.2. Críticas ao princípio da conservação de dados

Várias organizações da sociedade civil interpelaram a Comissão alegando que a conservação de dados constitui, em princípio, uma restrição injustificada e desnecessária do direito à vida privada. Estas organizações consideram que a conservação de dados individuais relativos às telecomunicações, em matéria de tráfego, localização e assinaturas, «de uma forma abrangente e indiscriminada» e não consensual, constitui uma restrição ilegal dos direitos fundamentais. Na Irlanda, na sequência de um processo apresentado em tribunal por uma associação de direitos civis, a questão da legalidade da Directiva deverá ser sujeita à apreciação do Tribunal de Justiça Europeu[125]. Também a Autoridade Europeia para a Protecção de Dados já manifestou dúvidas quanto à necessidade da medida.

7.3. Apelos a um reforço das regras de segurança e protecção dos dados

No seu relatório sobre a segunda acção comum de controlo da aplicação da legislação, o Grupo de Trabalho do «Artigo 29.°» alegava que os riscos de violação da confidencialidade das comunicações e da liberdade de expressão eram inerentes ao armazenamento de qualquer tipo de dados de tráfego. O Grupo de Trabalho criticou alguns aspectos da aplicação da Directiva a nível nacional, nomeadamente o registo dos dados, os seus períodos de conservação, o tipo de dados conservados e as medidas de segurança adoptadas. O Grupo de Trabalho identificou alguns casos em que foi conservado o *conteúdo* das comunicações na Internet, não abrangido pelo âmbito de aplicação da Directiva, incluindo endereços IP de destino, endereços URL dos sítios Web, o cabeçalho das mensagens electrónicas ou a lista dos destinatários em «cc». O Grupo decidiu, por conseguinte, solicitar que fosse clarificado que a enumeração das categorias é exaustiva, não podendo ser impostas aos operadores outras obrigações de conservação de dados.

A Autoridade Europeia para a Protecção de Dados afirmou que a Directiva «não conseguiu harmonizar as legislações nacionais» e que a utilização dos dados conservados não se limitava estritamente à luta contra a criminalidade grave[126]. A Autoridade Europeia declarou ainda que um instrumento da UE que impõe regras em matéria de obrigatoriedade de conservação de dados deveria, caso se demonstre a sua necessidade, contemplar igualmente regras em matéria de acesso e utilização das autoridades responsáveis pela aplicação da lei. A Autoridade Europeia para a Protecção de dados instou a UE a adoptar um enquadramento legislativo global, que não só imponha aos operadores a obrigação de conservarem os dados, mas também regule a forma como os Estados-Membros utilizam os dados para efeitos da aplicação da lei, de modo a criar «segurança jurídica para os cidadãos».

As diferentes autoridades responsáveis pela protecção de dados defenderam, em geral, que a conservação dos dados implica, em si mesma, um risco de eventuais violações da vida privada, que não é abordado pela Directiva a nível da UE, sendo antes exigido aos

---

125 Em 5 de Maio de 2010, o «High Court» irlandês concedeu à *Digital Rights Ireland Limited* autorização para recorrer ao Tribunal de Justiça Europeu, ao abrigo do artigo 267.º do Tratado sobre o Funcionamento da União Europeia.

126 Discurso de Peter Hustinx proferido na Conferência «Taking on the Data Retention Directive», em 3 de Dezembro de 2010.

Estados-Membros que assegurem o respeito das normas de protecção dos dados a nível nacional. Embora não existam exemplos concretos de violações graves da vida privada, o risco de ocorrerem violações da segurança dos dados continuará a existir, podendo até aumentar com os novos desenvolvimentos tecnológicos e as tendências actuais verificada nas novas formas de comunicação, independentemente de os dados serem armazenados para fins comerciais ou de segurança, no interior ou fora da UE, a menos que sejam adoptadas novas medidas de protecção.

8. CONCLUSÕES E RECOMENDAÇÕES

O presente relatório identificou uma série de vantagens e de aspectos em que se pode melhorar o actual regime de conservação de dados da UE. A União Europeia adoptou a Directiva numa altura de grande alarme face à iminência de ataques terroristas. A avaliação de impacto que a Comissão pretende realizar proporciona uma boa oportunidade para avaliar a conservação dos dados na UE em função dos princípios da necessidade e da proporcionalidade, tendo em conta o interesse da segurança interna, o bom funcionamento do mercado interno e a defesa do respeito pela vida privada e do direito à protecção dos dados pessoais. A proposta da Comissão relativa à revisão do quadro legislativo da UE em matéria de conservação de dados deve assentar nas conclusões e recomendações seguintes.

8.1. A UE deve apoiar e regulamentar a conservação de dados enquanto medida de segurança

A maioria dos Estados-Membros considera que as normas da UE em matéria de conservação de dados continuam a ser um instrumento necessário para a aplicação da lei, a protecção das vítimas e os sistemas de justiça criminal. Embora as provas fornecidas pelos Estados-Membros, sob a forma de dados estatísticos e de exemplos, sejam limitadas quanto a alguns aspectos, atestam o papel fundamental que a conservação de dados desempenha no âmbito da investigação criminal. Estes dados fornecem pistas e elementos de prova valiosos para a prevenção e a repressão da criminalidade, assim como para a eficácia da justiça criminal. A sua utilização possibilitou condenações por infracções penais, que, sem a conservação dos dados, nunca poderiam ter sido alcançadas. Possibilitou igualmente a absolvição de muitos inocentes. A harmonização das normas neste domínio deve garantir que a conservação de dados constitui um instrumento eficaz para combater a criminalidade, que as empresas dispõem de segurança jurídica quanto ao bom funcionamento do mercado interno e que são aplicados de forma coerente em toda a União Europeia elevados níveis de respeito pela vida privada e de protecção dos dados pessoais .

8.2. A transposição da Directiva não tem sido homogénea

Já se encontra em vigor legislação de transposição da Directiva em 22 Estados-Membros. A grande margem de manobra deixada aos Estados-Membros para adoptarem medidas de conservação de dados ao abrigo do artigo 15.º, n.º 1, da Directiva relativa à privacidade e às comunicações electrónicas torna muito problemática a avaliação da Directiva relativa à conservação de dados. Existem diferenças consideráveis entre as legislações de transposição no que respeita à limitação das finalidades, ao acesso aos dados, aos períodos de conservação, à protecção e segurança dos dados e às estatísticas. Três Estados-Membros encontram-se em situação de incumprimento da Directiva, pois a sua legislação de transposição foi revogada pelos respectivos tribunais constitucionais. Dois outros Estados-Membros ainda não efectuaram a transposição. A Comissão continuará a colaborar com todos os

Estados-Membros para garantir a aplicação efectiva da Directiva. Continuará também a desempenhar o seu papel de controlo da aplicação da legislação da UE, em última análise mediante processos por infracção, se tal se revelar necessário.

8.3. A Directiva não permitiu harmonizar totalmente a abordagem em matéria de conservação de dados, não tendo criado condições de concorrência equitativas para todos os operadores

A Directiva permitiu assegurar que a maioria dos Estados-Membros procede actualmente à conservação de dados. A Directiva não garante, por si só, que os dados conservados são armazenados, extraídos e utilizados no pleno respeito do direito à vida privada e à protecção dos dados pessoais. A responsabilidade por assegurar o respeito desses direitos incumbe aos Estados-Membros. A Directiva tinha apenas por objectivo uma harmonização parcial dos métodos de conservação dos dados. Por conseguinte, não é surpreendente que não exista uma abordagem comum, quer em termos das disposições específicas da Directiva, como a limitação das finalidades ou os períodos de retenção, quer em termos de outros aspectos fora do seu âmbito de aplicação, como o reembolso dos custos suportados pelos operadores. Contudo, para além do nível de variação expressamente previsto na Directiva, as divergências nacionais na aplicação da conservação de dados suscitaram dificuldades consideráveis aos operadores.

8.4. Os operadores devem ser reembolsados de forma homogénea pelos custos que tiverem de suportar

Continua a haver falta de segurança jurídica para as empresas. A obrigação de conservação e de extracção de dados representa um custo significativo para os operadores, em especial para os pequenos operadores. Os operadores são afectados e reembolsados de forma diferente consoante os Estados-Membros, embora não existam indícios de que o sector das telecomunicações, em geral, tenha sido afectado negativamente em resultado da Directiva. A Comissão irá analisar as possibilidades de assegurar um reembolso homogéneo das despesas suportadas pelos operadores.

8.5. Garantir a proporcionalidade ao longo de todo o processo de armazenamento, extracção e utilização dos dados

A Comissão assegurará que qualquer proposta futura em matéria de conservação de dados satisfaça o princípio da proporcionalidade e seja adequada para consecução do objectivo da luta contra a criminalidade grave e o terrorismo, não excedendo o estritamente necessário para o alcançar. Tal proposta deverá reconhecer que as excepções e derrogações em matéria de protecção dos dados de carácter pessoal só podem ser aplicadas na medida em que forem necessárias. A Comissão avaliará atentamente as consequências, para a eficácia dos sistemas de justiça penal e para a aplicação da lei, assim como para a vida privada, e para os custos da administração pública e dos operadores, da adopção de regulamentação mais exigente em matéria de armazenamento, acesso e utilização dos dados de tráfego. Essa avaliação de impacto deve ter em conta, especialmente, os seguintes aspectos:

- a coerência entre a limitação das finalidades da conservação dos dados e os tipos de crimes em relação aos quais os dados conservados podem ser acedidos e utilizados;

- uma maior harmonização e, se possível, a redução dos períodos obrigatórios de conservação dos dados;

- a supervisão independente dos pedidos de acesso e do regime geral de acesso e de conservação dos dados aplicável em todos os Estados-Membros;

- a limitação das autoridades que podem aceder aos dados;

- a redução das categorias de dados a conservar;

- orientações sobre as medidas de segurança técnicas e organizativas para acesso aos dados, incluindo os procedimentos da sua transmissão;

- orientações quanto à utilização dos dados, incluindo a prevenção da prospecção de dados; e

- o desenvolvimento de procedimentos viáveis para a medição e a elaboração de relatórios, de modo a permitir efectuar comparações quanto à aplicação e avaliação do futuro instrumento.

A Comissão irá ainda analisar a questão de saber se - e de que modo - uma abordagem da UE em matéria de preservação de dados pode complementar a conservação de dados.

No que respeita à «lista de controlo» dos direitos fundamentais e à abordagem adoptada quanto à gestão da informação em matéria de liberdade, segurança e justiça[127], a Comissão analisará cada um destes domínios segundo os princípios da proporcionalidade e da exigência de previsibilidade. A Comissão assegurará igualmente a coerência com a revisão em curso do quadro em matéria de protecção de dados da UE[128].

8.6. Próximas etapas

Tendo em conta a presente avaliação, a Comissão vai apresentar uma proposta de revisão do actual quadro jurídico da UE em matéria de conservação de dados. A Comissão apresentará varias alternativas, em consulta com as entidades responsáveis pela aplicação da lei, o poder judicial, os representantes das empresas, as associações de consumidores, as autoridades responsáveis pela protecção dos dados e as organizações da sociedade civil. A Comissão irá ainda analisar a percepção do público em matéria de conservação de dados e o seu impacto nos comportamentos. Essas conclusões servirão para alimentar uma avaliação do impacto das opções estratégicas identificadas, que constituirá a base da proposta da Comissão.

---

127 Ver *supra* a referência à Comunicação sobre a aplicação da Carta dos Direitos Fundamentais: «Apresentação geral da gestão da informação no domínio da liberdade, segurança e justiça», COM(2010)385, de 20.7.2010.

128 COM (2010) 609 de 4.11.2010.

Anexo: Estatísticas suplementares sobre a conservação dos dados de tráfego

Notas relativas ao Anexo:

1. A antiguidade dos dados significa o período de tempo decorrido entre a data a partir da qual os dados foram conservados e a data em que as autoridades competentes solicitaram a sua transmissão,

2. Os dados relativos à Internet são os dados relativos ao acesso à Internet, correio electrónico e comunicações telefónicas através da Internet.

3. Os dados estatísticos relativos à República Checa, à Letónia e à Polónia são apresentados sob reserva (ver ponto 5.1).

Dados estatísticos transmitidos pelos Estados-Membros para o ano de 2008

Quadro 7: Pedidos de dados de tráfego conservados, por antiguidade - 2008									
Antiguidade dos dados solicitados (meses)/Estado-Membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	n.d.								
Bulgária	n.d.								
República Checa	102691	18440	10110	319	0	0	0	0	131560
Dinamarca	2669	672	185	37	23	2	7	4	3599
Alemanha	9363	2336	985	0	0	0	0	0	12684
Estónia	2773	733	157	827	0	0	0	0	4490
Irlanda	8981	2016	936	1855	90	85	78	54	14095
Grécia	Não foi fornecida discriminação por antiguidade dos dados								584
Espanha	22629	15868	10298	4783	0	0	0	0	53578
França	Não foi fornecida discriminação por antiguidade dos dados								503437
Itália	n.d.								
Chipre	30	4	0	0	0	0	0	0	34
Letónia	10539	2739	1368	1211	597	438	0	0	16892
Lituânia	55735	23817	5251	512	0	0	0	0	85315
Luxemburgo	n.d.								
Hungria	n.d.								
Malta	810	59	0	0	0	0	0	0	869
Países Baixos	Não foi fornecida discriminação por antiguidade dos dados								85000
Áustria	Não foi fornecida discriminação por antiguidade dos dados								3093
Polónia	n.d.								
Portugal	n.d.								
Roménia	n.d.								
Eslovénia	Não foi fornecida discriminação por antiguidade dos dados								2821
Eslováquia	n.d.								
Finlândia	9134	1144	448	214	268				4008
Suécia	n.d.								
Reino Unido	315350	88339	34665	19398	6385	2973	1536	1576	470222
Total	**533504**	**156167**	**64403**	**29156**	**7095***	**3230***	**1353***	**1366***	**1392281**

* Com excepção da Finlândia

Quadro 8: Pedidos de dados de tráfego conservados, por tipo de dados - 2008 (entre parênteses figura o número de casos em que os pedidos não foram satisfeitos – quando indicado)				
Tipo de dados / Estado-Membro	**Rede fixa**	**Rede móvel**	**Internet**	**Total**
Bélgica	n.d.			
Bulgária	n.d.			
República Checa	4983 (131)	125040 (2276)	1537 (83)	131560 (2490)
Dinamarca	192 (0)	3273 (5)	134 (0)	3599 (5)
Alemanha	Não foi fornecida discriminação por tipo de dados			12684 (931)
Estónia	4114 (1519)	376 (7)	n.d.	4490 (1526)
Irlanda	5317 (16)	5873 (48)	2905 (33)	14095 (97)
Grécia	Não foi fornecida discriminação por tipo de dados			584
Espanha	4448 (0)	40013 (0)	9117 (0)	53578 (0)
França	Não foi fornecida discriminação por tipo de dados			503437
Itália	n.d.			
Chipre	3 (0)	31 (5)	0 (0)	34 (5)
Letónia	1602 (90)	14238 (530)	1052 (76)	16892 (696)
Lituânia	765 (72)	84550 (5657)	n.d.	85315 (5729)
Luxemburgo	n.d.			
Hungria	n.d.			
Malta	29 (0)	748 (120)	92 (13)	869 (133)
Países Baixos	Não foi fornecida discriminação por tipo de dados			85000
Áustria	Não foi fornecida discriminação por tipo de dados			3093
Polónia	n.d.			
Portugal	n.d.			
Roménia	n.d.			
Eslovénia	Não foi fornecida discriminação por tipo de dados			2821
Eslováquia	n.d.			
Finlândia	Não foi fornecida discriminação por tipo de dados			4008
Suécia	n.d.			
Reino Unido	90747 (0)	329421 (0)	50054 (0)	470222 (0)
Total				**1392281**

Quadro 9: Pedidos de dados conservados relativos à *rede telefónica fixa* que foram satisfeitos, por antiguidade - 2008									
Antiguidade dos dados solicitados (meses)/Estado-Membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	n.d.								
Bulgária	n.d.								
República Checa	3669	916	143	124	0	0	0	0	4852
Dinamarca	133	28	31	0	0	0	0	0	192
Alemanha	n.d.								
Estónia	1876	161	74	484	0	0	0	0	2595
Irlanda	4118	712	197	182	32	21	23	16	5301
Grécia	n.d.								
Espanha	1948	1431	741	328	0	0	0	0	4448
França	n.d.								
Itália	n.d.								
Chipre	3	0	0	0	0	0	0	0	3
Letónia	698	213	167	193	104	137	0	0	1512
Lituânia	251	442	0	0	0	0	0	0	693
Luxemburgo	n.d.								
Hungria	n.d.								
Malta	28	1	0	0	0	0	0	0	29
Países Baixos	n.d.								
Áustria	n.d.								
Polónia	n.d.								
Portugal	n.d.								
Roménia	n.d.								
Eslovénia	n.d.								
Eslováquia	n.d.								
Finlândia	n.d.								
Suécia	n.d.								
Reino Unido	54805	27052	5340	753	1135	437	1050	175	90747
Total	**67529**	**30956**	**6693**	**2064**	**1271**	**595**	**1073**	**191**	**110372**

Quadro 10: Pedidos de dados conservados relativos à *rede telefónica móvel* que foram satisfeitos, por antiguidade - 2008									
Antiguidade dos dados solicitados (meses)/Estado-Membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	n.d.								
Bulgária	n.d.								
República Checa	98232	17013	7518	1	0	0	0	0	122764
Dinamarca	2433	628	143	33	20	1	7	3	3268
Alemanha	n.d.								
Estónia	248	58	35	28	0	0	0	0	369
Irlanda	4326	820	230	240	57	63	52	37	5825
Grécia	n.d.								
Espanha	17403	12114	7444	3052	0	0	0	0	40013
França	n.d.								
Itália	n.d.								
Chipre	23	3	0	0	0	0	0	0	26
Letónia	8928	2298	1085	746	394	257	0	0	13708
Lituânia	55484	23375	14	20	0	0	0	0	78893
Luxemburgo	n.d.								
Hungria	n.d.								
Malta	575	53	0	0	0	0	0	0	628
Países Baixos	n.d.								
Áustria	n.d.								
Polónia	n.d.								
Portugal	n.d.								
Roménia	n.d.								
Eslovénia	n.d.								
Eslováquia	n.d.								
Finlândia	n.d.								
Suécia	n.d.								
Reino Unido	229375	52241	26228	16040	3333	521	339	1344	329421
Total	**417027**	**108603**	**42697**	**20160**	**3804**	**842**	**398**	**1384**	**594915**

Quadro 11: Pedidos de dados conservados relativos ao *tráfego de internet* que foram satisfeitos, por antiguidade - 2008									
Antiguidade dos dados solicitados (meses)/Estado-Membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	n.d.								
Bulgária	n.d.								
República Checa	737	412	137	168	0	0	0	0	1454
Dinamarca	102	14	11	2	3	1	0	1	134
Alemanha	n.d.								
Estónia	n.d.								
Irlanda	492	460	498	1422	0	0	0	0	2872
Grécia	n.d.								
Espanha	3278	2323	2113	1403	0	0	0	0	9117
França	n.d.								
Itália	n.d.								
Chipre	0	0	0	0	0	0	0	0	0
Letónia	424	150	75	219	74	34	0	0	976
Lituânia	n.d.								
Luxemburgo	n.d.								
Hungria	n.d.								
Malta	76	3	0	0	0	0	0	0	79
Países Baixos	n.d.								
Áustria	n.d.								
Polónia	n.d.								
Portugal	n.d.								
Roménia	n.d.								
Eslovénia	n.d.								
Eslováquia	n.d.								
Finlândia	n.d.								
Suécia	n.d.								
Reino Unido	31170	9046	3097	2605	1917	2015	147	57	50054
Total	**36279**	**12408**	**5931**	**5819**	**1994**	**2050**	**147**	**58**	**64686**

Dados estatísticos transmitidos pelos Estados-Membros para o ano de 2009

Quadro 12: Pedidos de dados conservados, por antiguidade - 2009									
Antiguidade dos dados solicitados (meses)/Estado-Membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	n.d.								
Bulgária	n.d.								
República Checa	210975	56623	11620	1053	0	0	0	0	280271
Dinamarca	2980	685	179	104	54	38	12	14	4066
Alemanha	n.d.								
Estónia	4299	1836	1210	1065	0	0	0	0	8410
Irlanda	8117	1652	805	297	168	134	69	41	11283
Grécia	n.d.								
Espanha	29775	19346	13999	6970	0	0	0	0	70090
França	Não foi fornecida discriminação por antiguidade dos dados								514813
Itália	n.d.								
Chipre	31	8	1	0	0	0	0	0	40
Letónia	20758	2414	1088	796	565	475	0	0	26096
Lituânia	30247	35456	5886	884	0	0	0	0	72473
Luxemburgo	n.d.								
Hungria	n.d.								
Malta	3336	362	151	174	0	0	0	0	4023
Países Baixos	n.d.								
Áustria	n.d.								
Portugal	n.d.								
Roménia	n.d.								
Polónia	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Eslovénia	Não foi fornecida discriminação por antiguidade dos dados								1918
Eslováquia	Não foi fornecida discriminação por antiguidade dos dados								5214
Finlândia	2000	1310	532	152	76	0	0	0	4070
Suécia	n.d.								
Reino Unido	n.d.								
Total	**954845**	**297998**	**110996**	**64021**	**27961**	**24571**	**14065**	**34683**	**2051085**

Quadro 13: Pedidos de dados conservados, por tipo de dados - 2009 (entre parênteses figura o número de casos em que os pedidos não foram satisfeitos – quando indicado)				
Tipo de dados / Estado-Membro	**Rede fixa**	**Rede móvel**	**Internet**	**Total**
Bélgica	n.d.			
Bulgária	n.d.			
República Checa	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Dinamarca	133 (0)	3771 (10)	162 (1)	4066 (11)
Alemanha	n.d.			
Estónia	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Irlanda	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Grécia	n.d.			
Espanha	5055 (0)	56133 (0)	8902 (0)	70090 (0)
França	Não foi fornecida discriminação por tipo de dados			514813
Itália	n.d.			
Chipre	0 (0)	23 (3)	14 (0)	40 (3)
Letónia	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Lituânia	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Luxemburgo	n.d.			
Hungria	n.d.			
Malta	156 (10)	3693 (882)	174 (10)	4023 (902)
Países Baixos	n.d.			
Áustria	n.d.			
Polónia	Não foi fornecida discriminação por tipo de dados			1048318
Portugal	n.d.			
Roménia	n.d.			
Eslovénia	Não foi fornecida discriminação por tipo de dados			1918 (48)
Eslováquia	Não foi fornecida discriminação por tipo de dados			5214 (157)
Finlândia	Não foi fornecida discriminação por tipo de dados			4070
Suécia	n.d.			
Reino Unido	n.d.			
Total				**2051082 (1069885)**

Quadro 14: Pedidos de dados conservados relativos à *rede telefónica fixa* que foram satisfeitos, por antiguidade - 2009									
Antiguidade dos dados solicitados (meses)/Estado-Membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	n.d.								
Bulgária	n.d.								
República Checa	9919	2907	47	36	0	0	0	0	12909
Dinamarca	105	19	7	2	0	0	0	0	133
Alemanha	n.d.								
Estónia	2254	866	599	424	0	0	0	0	4143
Irlanda	3934	337	69	70	50	39	16	11	4526
Grécia	n.d.								
Espanha	2371	1492	844	348	0	0	0	0	5055
França	n.d.								
Itália	n.d.								
Chipre	0	0	0	0	0	0	0	0	0
Letónia	744	253	157	143	68	89	0	0	1454
Lituânia	469	773	73	6	0	0	0	0	1321
Luxemburgo	n.d.								
Hungria	n.d.								
Malta	83	25	18	20	0	0	0	0	146
Países Baixos	n.d.								
Áustria	n.d.								
Polónia	n.d.								
Portugal	n.d.								
Roménia	n.d.								
Eslovénia	n.d.								
Eslováquia	n.d.								
Finlândia	n.d.								
Suécia	n.d.								
Reino Unido	n.d.								
Total	**19879**	**6672**	**1814**	**1049**	**118**	**128**	**16**	**11**	**29687**

Quadro 15: Pedidos de dados conservados relativos à *rede telefónica móvel* que foram satisfeitos, por antiguidade - 2009									
Antiguidade dos dados solicitados (meses)/Estado-Membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	n.d.								
Bulgária	n.d.								
República Checa	197620	48841	472	0	0	0	0	0	246933
Dinamarca	2777	639	162	98	47	19	12	7	3761
Alemanha	n.d.								
Estónia	318	397	96	70	0	0	0	0	881
Irlanda	3669	835	220	210	115	92	50	28	5219
Grécia	n.d.								
Espanha	24065	15648	11147	5273	0	0	0	0	56133
França	n.d.								
Itália	n.d.								
Chipre	17	16	0	0	0	0	0	0	23
Letónia	18832	1912	778	515	394	263	0	0	22694
Lituânia	25713	19595	28	0	0	0	0	0	45336
Luxemburgo	n.d.								
Hungria	n.d.								
Malta	2332	246	111	122	0	0	0	0	2811
Países Baixos	n.d.								
Áustria	n.d.								
Polónia	n.d.								
Portugal	n.d.								
Roménia	n.d.								
Eslovénia	n.d.								
Eslováquia	n.d.								
Finlândia	n.d.								
Suécia	n.d.								
Reino Unido	n.d.								
Total	**275343**	**88119**	**13014**	**6288**	**556**	**374**	**62**	**35**	**383791**

Quadro 16: Pedidos de dados conservados relativos ao *tráfego de internet* que foram satisfeitos, por antiguidade - 2009									
Antiguidade dos dados solicitados (meses)/Estado-Membro	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Bélgica	n.d.								
Bulgária	n.d.								
República Checa	3369	4811	861	942	0	0	0	0	9983
Dinamarca	98	27	10	4	4	7	0	1	151
Alemanha	n.d.								
Estónia	315	145	56	102	0	0	0	0	618
Irlanda	489	455	502	0	0	0	0	0	1446
Grécia	n.d.								
Espanha	3339	2206	2008	1349	0	0	0	0	8902
França	n.d.								
Itália	n.d.								
Chipre	12	2	0	0	0	0	0	0	14
Letónia	852	198	74	90	88	86	0	0	1388
Lituânia	4060	15087	1	88	0	0	0	0	19236
Luxemburgo	n.d.								
Hungria	n.d.								
Malta	150	14	0	0	0	0	0	0	164
Países Baixos	n.d.								
Áustria	n.d.								
Polónia	n.d.								
Portugal	n.d.								
Roménia	n.d.								
Eslovénia	n.d.								
Eslováquia	n.d.								
Finlândia	n.d.								
Suécia	n.d.								
Reino Unido	n.d.								
Total	**12684**	**22945**	**3512**	**2575**	**92**	**93**	**0**	**1**	**41902**