Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar?

Carlos Pinho
Procurador-adjunto

SUMÁRIO: I. Introdução; II. O estado atual da Lei n.º 32/2008; III. As decisões do TJUE com maior impacto na Lei n.º 32/2008; 1. Em geral; 2. A violação do princípio da proporcionalidade; 3. A (não) obrigação de conservação dos dados em território da União Europeia; 4. Síntese; IV. Conservação (Retenção) Vs. Preservação de dados; V. O problema da obrigação de conservação e transterritorialidade dos dados; VI. Impacto da entrada em vigor do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016 (RGDP); VII. Conclusão: a reforma que se impõe.

I. Introdução

O propósito deste texto reside na resposta à questão de saber se a Lei n.º 32/2008, de 17 de Julho (doravante, Lei n.º 32/2008), tem ainda um papel a desempenhar no ordenamento jurídico nacional e, em caso afirmativo, se se mostra necessária a sua reforma e em que sentidos deve a mesma apontar.

Após descrever brevemente o atual regime derivado da Lei n.º 32/2008 e algumas questões quanto à sua inserção sistemática no ordenamento jurídico, proceder-se-á à análise dos argumentos com maior impacto nesta Lei derivados das decisões da Grande Secção do Tribunal de Justiça da União Europeia (doravante, TJUE), indicar-se-ão os argumentos para a sua superação, referindo-se as

especificidades relativas à conservação de dados, no seu confronto e complemento com o regime de preservação de dados e abordar-se-á o problema da obrigação de conservação e da transterritorialidade dos dados gerados no âmbito de comunicações eletrónicas.

Anotar-se-á o impacto derivado da entrada em vigor do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, retificado em 23 de Maio de 2018 – o regulamento geral de proteção de dados (doravante, RGPD).

Concluir-se-á com síntese de propostas de reforma da Lei n.º 32 /2008.

II. O Estado Atual da Lei N.º 32/2008

A Lei n.º 32/2008 resultou do processo de transposição para a ordem jurídica interna da Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

O escopo essencial da Diretiva n.º 2006/24/CE era o de "*harmonizar as disposições dos Estados-membros relativas às obrigações dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de crimes graves*".

No processo de transposição, o legislador nacional optou por criar um quadro normativo para além do escopo essencial da Diretiva n.º 2006/24/CE, que se cingia à consagração de um quadro de obrigações para os fornecedores de serviços de comunicações eletrónicas, concebendo um regime processual específico nesta matéria, nomeadamente quanto ao acesso aos dados armazenados para a finalidade

exclusiva de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, designadamente as normas conjugadas do n.º 1 e 2 do artigo 3.º e o artigo 9.º da Lei n.º 32/2008.

O regime normativo constante da Lei n.º 32/2008 foi, desde a data da sua entrada em vigor, fonte de problemas interpretativos, designadamente na sua relação com as normas do Código de Processo Penal, particularmente as atinentes ao regime das escutas, problemas estes agravados ainda pela entrada em vigor da Lei n.º 109/2009, de 15 de Setembro (doravante, Lei do Cibercrime), pela qual foi transposta para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação (entretanto substituída pela Diretiva n.º 2013/40/EU do Parlamento Europeu e do Conselho, de 12 de Agosto de 2013), e adaptado o direito interno à Convenção sobre o Cibercrime do Conselho da Europa (Convenção de Budapeste).

Talvez o mais evidente exemplo da desconformidade normativa com as regras do Código de Processo Penal seja a definição muito restritiva de crime grave constante da alínea g) do n.º 1 do artigo 2.º, todos da Lei n.º 32/2008[1], quando comparado com o catálogo previsto no n.º 1 do artigo 187.º do Código de Processo Penal.

A definição restritiva de crime grave tem uma óbvia consequência prática: na aplicação da Lei n.º 32/2008 não é possível a obtenção de dados de tráfego e de localização relativamente a parte dos crimes constantes do catálogo do n.º 1 do artigo 187.º do Código de Processo Penal[2], preceito este que define as condições

[1] «Crime grave», crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

[2] A generalidade dos crimes punidos com pena de prisão de máximo superior a três anos, não enquadráveis nas categorias de criminalidade violenta ou altamente organizada, bem como os crimes de contrabando, de injúria, de ameaça, de coacção, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone, de ameaça com prática de crime ou de abuso e simulação de sinais de perigo.

de admissibilidade de escutas telefónicas, ou seja, no ordenamento jurídico português existem crimes na investigação dos quais é admissível a obtenção de prova consubstanciada em dados de conteúdo gerados no contexto de comunicações (v.g., de voz ou texto), mas não de dados de tráfego ou de localização – seguramente menos intrusivos na esfera da vida privada dos visados.

Esta consequência é extensível, *mutatis mutandis*, ao catálogo de crimes previstos em especial no artigo 11.º da Lei do Cibercrime[3].

O problema é que, aplicando-se exclusivamente o regime da Lei n.º 32/2008 à obtenção dos dados gerados no âmbito de comunicações eletrónicas, estaria criado um vazio legal consubstanciado na impossibilidade de obtenção de tais dados numa multiplicidade de crimes, particularmente aqueles cometidos por meio de comunicações eletrónicas, com graves consequências para a obtenção da prova essencial no processo criminal.

Este problema foi, em certa medida, resolvido em termos práticos, considerando-se existirem na verdade dois regimes fundamento (e, por consequência, duas bases de dados armazenados distintas, como efetivamente ocorre) para a obrigação/conveniência dos fornecedores de serviços de comunicações quanto à conservação de dados: um geral, que pelo prazo de seis meses habilita os operadores a conservar os dados para efeitos de faturação (resultante da aplicação da norma resultante da conjugação das normas contidas na alínea d) do n.º 1 do artigo 1.º, do n.º 1 e n.º 2 do artigo 9.º e do n.º 1 do artigo 10.º, todos da Lei n.º 23/96, de 26 de Julho, pese embora o problema intercalar resultante entrada em vigor da Lei n.º 5/2004, em 11 de Fevereiro de 2004, cuja norma revogatória do n.º 2 do seu artigo 127.º se manteve até

[3] Crimes previstos na Lei do Cibercrime (crimes informáticos *strictu sensu*), crimes cometidos por meio de um sistema informático e crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

que veio a ser revogada, por força da entrada em vigor da Lei n.º 51/2011, de 13 de Setembro), pelo qual podiam tais dados ser obtidos aplicando as regras próprias do processo penal e da Lei do Cibercrime, a partir da sua entrada em vigor; e um regime especial, pelo prazo de um ano, aquele previsto na Lei n.º 32/2008.

Esta solução prática é, no entanto, precária.

Com efeito, a Lei não determina que concretos dados devem ser armazenados pelo prazo de seis meses pelas operadoras, apenas refere que lhes é lícito conservar os que sejam necessários ao exercício do direito do consumidor à faturação detalhada[4] e correspondente exercício do direito de cobrança do operador.

Ora, os concretos dados que permitem a execução desses direitos dependem do interesse e posicionamento de mercado de cada operador, pelo que nem todos os dados necessários à prova em processo penal devem ser, nesta vertente interpretativa, conservados.

Com efeito, atualmente, para as operadoras alguns tipos de dados têm um valor comercial residual e não se mostram necessários àquelas finalidades, tais como os dados de tráfego fixo/móvel para contratos de uso ilimitado de taxa fixa e serviços pré-pagos, a identificação de origem (ou seja, número de telefone) para chamadas entradas, os endereços IPV4 (e respetivos portos), os dados de ID de célula (localização) e os dados de transmissão de correio eletrónico – refira-se que a única razão pela qual estes dados são conservados tem que ver com as obrigações de retenção decorrentes da Lei n.º 32/2008.

Acresce ainda o facto de o armazenamento de dados para efeito de faturação, nos termos descritos, não ser realizado para fins de deteção, investigação e repressão criminal, pelo que o seu tratamento pelas operadoras não está abrangido pelas especiais garantias que devem ser aplicáveis para esta finalidade específica[5].

[4] Cfr. n.º 5 do artigo 39.º, em conjugação com o artigo 94.º, ambos da Lei n.º 51/2011, de 13 de Setembro.

[5] Como aliás resulta evidente do disposto no n.º 4 do artigo 1.º da Lei n.º 41/2004, de 18 de Agosto (Lei de proteção de dados pessoais e privacidade nas telecomunicações), segundo a qual *"as exceções à aplicação da presente lei*

A solução destas questões pode ser alcançada com a reforma da Lei n.º 32/2008, no sentido de esta estabelecer o regime legal único para a conservação de determinados dados gerados ou tratados no âmbito dos serviços de comunicações, designadamente eletrónicas, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de deteção e de repressão de crimes, adequando-se o catálogo criminal, o regime de garantias e o regime de acesso aos mesmos[6].

III. As Decisões do TJUE com Maior Impacto na Lei N.º 32/2008

1. Em geral

No decurso do processo de transposição, a partir de 2010, foram proferidas algumas decisões pelos Tribunais de Estados-membros declarando a invalidade de normas relativas à legislação interna de transposição da Diretiva n.º 2006/24/CE[7].

Entretanto, o TJUE veio a declarar a invalidade da Diretiva n.º 2006/24/CE, por força do Acórdão do Tribunal de Justiça (Grande Secção) de 8 de Abril de 2014, Processos apensos C-293/12 e C-594/12[8] (doravante, Digital Rights Ireland), tendo a propósito da

que se mostrem estritamente necessárias para a proteção de atividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infrações penais são definidas em legislação especial".

[6] Designadamente aqui se incluindo a figura da Autoridade Judiciária competente, a fim de contemplar a obtenção dos dados que não sejam de tráfego/localização pelo Ministério Público, enquanto titular da fase de inquérito do processo criminal.

[7] À data do Acórdão Digital Rights, a decisão n.º 1258, de 8 de Outubro de 2009, do Tribunal Constitucional da Roménia, o Acórdão 1 BvR 256/08, de 2 de Março de 2010, do Tribunal Constitucional da Alemanha (Bundesverfassungsgericht), o Acórdão do Supremo Tribunal de Chipre de 1 de Fevereiro de 2011 e o Acórdão do Tribunal Constitucional da República Checa de 22 de Março de 2011 (apenas algumas normas). Para informação mais atualizada, ver *National Data Retention Laws since the CJEU's Tele-2/Watson Judgment*, de Setembro de 2017, disponível em www.privacyinternational.org e *Note from the General Secretariat of the Council of the European Union*, de 7 de Março de 2017, disponível em http://data.consilium.europa.eu/doc/document/ST-6726-2017-REV-1/en/pdf (com último acesso, tal como a todos os endereços electrónicos citados, em 23.06.2018)

[8] Disponível para consulta, simples e comparada, em https://eur-lex.europa.eu/legal-content/EN/

Diretiva n.º 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas: e-privacy), alterada pela Diretiva n.º 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, reforçado os argumentos aduzidos naquele aresto no Acórdão do Tribunal de Justiça (Grande Secção) de 21 de Dezembro de 2016, Processos apensos C-203/15 e C-698/15[9] (doravante, Tele2 Sverige AB).

O TJUE considerou que, ao adotar a Diretiva n.º 2006/24/CE, o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.º (direito ao respeito pela vida privada e familiar), 8.º (direito de proteção de dados pessoais) e 52.º, n.º 1 (aplicação do Princípio da proporcionalidade na restrição ao exercício de direitos e liberdades), todos da Carta de Direitos Fundamentais da União Europeia[10] (acrescentando o segundo aresto ainda o artigo 11.º da Carta, que tutela o direito à liberdade de expressão e de informação).

Concluiu o TJUE, no aresto do caso Digital Rights Ireland, que é inválida a Diretiva n.º 2006/24/CE, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que alterou a Diretiva n.º 2002/58/CE.

Como ambas as decisões resultaram da apreciação de questões prejudiciais colocadas pelos respetivos Tribunais dos Estados-membros, nos termos do artigo 267.º do Tratado de Funcionamento da União Europeia (doravante, TFUE), apenas estes se encontram vinculados pelas decisões, pelo que não pode

[9] Disponível para consulta, simples e comparada, em https://eur-lex.europa.eu/legal-content/EN/

[10] Disponível designadamente em http://www.europarl.europa.eu/charter/pdf/text_pt.pdf.

considerar-se que a Diretiva n.º 2006/24/CE se encontra afastada da ordem jurídica interna.

Para que tal sucedesse, seria exigido que a decisão do Tribunal tivesse resultado de um recurso de anulação, nos termos do artigo 263.º do TFUE, o qual teria força obrigatória geral, mas o facto é que a jurisprudência do TJUE foi fixada, em face do quadro legal vigente, pelo que, com os mesmos fundamentos, não é expectável uma decisão diversa.

Pese embora algumas das objeções aduzidas pela Tribunal não tenham impacto na Lei n.º 32/2008, em face das normas constantes deste diploma e resultantes do processo de transposição da Diretiva n.º 2006/24/CE que as afastam, existem duas que não estão cabalmente resolvidas na Lei nacional.

2. A violação do princípio da proporcionalidade

A primeira diz respeito à violação do Princípio da Proporcionalidade[11], no segmento da necessidade (ingerência nos direitos fundamentais para lá do estritamente necessário), e que tem que ver com o âmbito subjetivo da conservação dos dados.

O TJUE, nos parágrafos 56 e 59 do aresto Digital Rights Ireland, refere que a Diretiva 2006/24/CE *"visa todos os meios de comunicação eletrónica cuja utilização está muito divulgada e é de crescente importância na vida quotidiana de todos. Além disso, em conformidade com o seu artigo 3.º, a referida diretiva abrange todos os assinantes e utilizadores registados. Comporta, portanto, uma ingerência nos direitos fundamentais de quase toda a população europeia.* (…)

[11] Na acepção do n.º 1 do artigo 52.º da Carta dos Direitos Fundamentais da União Europeia: *"Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros".*

A referida diretiva não exige nenhuma relação entre os dados cuja conservação está prevista e uma ameaça para a segurança pública e, designadamente, não se limita a uma conservação nem de dados relativos a um período de tempo e/ou a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar implicadas, de uma maneira ou de outra, numa infração grave, nem de dados relativos a pessoas, cuja conservação, por outros motivos, pudesse contribuir para a prevenção, a deteção ou a repressão de infrações graves".

No aresto Digital Rights Ireland, quanto à questão de saber se a ingerência que a Diretiva 2006/24/CE comporta se limita ao estritamente necessário, no juízo de proporcionalidade efetuado pelo TJUE, são indicados três pontos essenciais de fundamentação[12].

O primeiro diz respeito ao facto de a Diretiva 2006/24/CE ser aplicável à conservação de dados mesmo relativamente a pessoas em relação às quais inexistam indícios de que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com infrações graves (designadamente, não se limita a uma conservação nem de dados relativos a um período de tempo e/ou a uma zona geográfica determinada e/ou a um círculo de pessoas determinadas que possam estar implicadas, de uma maneira ou de outra, numa infração grave) nem prever qualquer exceção, sendo aplicável mesmo a pessoas cujas comunicações estão sujeitas ao segredo profissional.

Este ponto é exacerbado no aresto Tele2 Sverige AG, no parágrafo 111: "No que se refere à delimitação de uma medida deste tipo quanto ao público e às situações potencialmente abrangidas, *a regulamentação nacional deve basear-se em elementos objetivos que permitam visar um público cujos dados sejam suscetíveis de revelar uma relação*, pelo menos indireta, *com atos de criminalidade grave*, de contribuir

[12] A descrição subsequente corresponde a súmula dos parágrafos 56 a 65 do aresto Digital Rights Ireland, salvo quando indicada fonte diversa.

de uma maneira ou outra para a luta contra a criminalidade grave ou de prevenir um risco grave para a segurança pública. Tal *delimitação pode ser assegurada através de um critério geográfico* quando as autoridades nacionais competentes considerem, com base em elementos objetivos, que existe um risco elevado de preparação ou de execução desses atos, numa ou em mais zonas geográficas".

O segundo ponto da fundamentação diz respeito ao facto de a Diretiva 2006/24/CE não estabelecer critérios objetivos que permitam delimitar o acesso das autoridades nacionais competentes aos dados e a sua utilização posterior, designadamente ao não dispor expressamente que este acesso e a utilização posterior dos dados em causa devam ser estritamente restringidos para fins de prevenção e de deteção de infrações graves, bem como não se prever que o acesso aos dados conservados pelas autoridades nacionais competentes não esteja sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente.

O terceiro ponto da fundamentação refere-se ao facto de a Diretiva 2006/24/CE não concretizar o período de duração da conservação dos dados, nem especificar que a determinação do período de conservação se deva basear em critérios objetivos a fim de garantir que se limita ao estritamente necessário.

3. A (não) obrigação de conservação dos dados em território da União Europeia

A segunda objeção refere-se à omissão de imposição da conservação dos dados em território da União Europeia.

O TJUE, no parágrafo 68 do aresto Digital Rights Ireland, refere que a Diretiva 2006/24/CE*"não impõe que os dados em causa sejam conservados no território da União, pelo que não se pode considerar que esteja plenamente garantida a fiscalização, por uma entidade independente, expressamente exigida pelo artigo 8.º, n.º 3, da Carta,*

do respeito das exigências de proteção e de segurança, tal como referidas nos dois números anteriores. Ora, semelhante fiscalização, efetuada com base no direito da União, constitui um elemento essencial do respeito da proteção das pessoas relativamente ao tratamento dos dados pessoais".

Este argumento tem acrescida importância em face do problema da fiscalização e auditoria no acesso e tratamento dos dados conservados, a fim de garantir a segurança destes dados e impedir a sua utilização desconforme às finalidades definidas pelo direito da União Europeia.

No parágrafo 122 do Acórdão Tele2 Sverige AB, este argumento é densificado, ali se referindo que "*no que se refere às regras relativas à segurança e à proteção dos dados conservados pelos prestadores de serviços de comunicações eletrónicas, há que constatar que o artigo 15.º, n.º 1, da Diretiva 2002/58 não permite que os Estados-Membros estabeleçam exceções ao seu artigo 4.º, n.º 1*[13], *nem ao seu artigo 4.º, n.º 1-A*[14]. *Estas últimas disposições exigem que esses prestadores de serviços adotem medidas de ordem técnica e de organização adequadas para garantir uma proteção eficaz dos dados conservados contra os riscos de abuso e contra qualquer acesso ilícito a esses dados. Tendo em conta a quantidade de dados conservados, o caráter sensível desses dados bem como o risco de acesso ilícito aos mesmos, os*

[13] Artigo 4.º/1 da Diretiva 2002/58/CE: "O prestador de um serviço de comunicações eletrónicas publicamente disponível adoptará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede. Tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas asseguram um nível de segurança adequado aos riscos existentes".

[14] Artigo 4.º/1-A da Diretiva 2002/58/CE, aditado pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de Novembro de 2009: "sem prejuízo do disposto na Diretiva 95/46/CE, as medidas referidas no n.º 1 compreendem, no mínimo: a garantia de que aos dados pessoais apenas possa ter acesso pessoal autorizado, para fins autorizados a nível legal; a proteção dos dados pessoais armazenados ou transmitidos contra a destruição acidental ou ilegal, a perda ou alteração acidental e o armazenamento, tratamento, acesso ou divulgação não autorizados ou ilegais, e a garantia da aplicação de uma política de segurança relativa ao tratamento dos dados pessoais. As autoridades nacionais competentes devem ter competência para auditar as medidas tomadas por prestadores de serviços de comunicações eletrónicas acessíveis ao público e para emitir recomendações sobre melhores práticas relativas ao nível de segurança que estas medidas devem alcançar".

prestadores de serviços de comunicações eletrónicas devem, para assegurar a plena integridade e a confidencialidade dos referidos dados, garantir um nível particularmente elevado de proteção e de segurança através de medidas técnicas e de organização adequadas. Em especial, a regulamentação nacional deve prever a conservação no território da União bem como a destruição definitiva dos dados no termo do respetivo período de conservação".

4. Síntese

No que diz respeito ao argumento da violação do princípio da proporcionalidade, como se aprofundará no capítulo subsequente, sustentamos que é incontornável, sob pena de se criar um vazio de punição gravíssimo, a opção pela conservação de dados, consagradas que sejam as necessárias salvaguardas quanto à definição de classes de dados, respetiva encriptação e regime estrito de acesso, impedindo qualquer operação de cruzamento dos mesmos na base de dados.

Com efeito, este é precisamente o risco aduzido pelo TJUE que sustenta a sua argumentação neste ponto, como aliás se mostra evidente pelo parágrafo 27 do Acórdão Digital Rights Ireland, segundo o qual *"estes dados, considerados no seu todo, são suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados".*

O argumento da não previsão da conservação dos dados em território da União Europeia relaciona-se com este fundamento, pois que o TJUE considera que tal omissão dificulta o controlo e fiscalização das bases de dados, que contêm dados pessoais dos cidadãos europeus, ou seja, trata-se da questão da transterritorialidade, que se abordará em maior detalhe em IV.

IV. Conservação (Retenção) Vs. Preservação de Dados

O argumento de maior impacto nas decisões do TJUE é o âmbito subjetivo da obrigação de conservação de dados de todos os dados gerados no âmbito das comunicações, designadamente eletrónicas, pois que abrange os dados relativos a todos os cidadãos europeus.

O TJUE optou pela lógica da preservação (ainda que preventiva, no caso de dados gerados no âmbito de comunicações) de dados, a fim de delimitar o âmbito subjetivo alargado inerente à conservação de dados.

No entanto, existem claras diferenças entre preservação e conservação de dados, que justificam a sua complementaridade e não a exclusão mútua[15].

A preservação de dados, também chamada de preservação acelerada de dados armazenados (*quick freeze*), ocorre nas situações em que é exigido legalmente a uma pessoa ou entidade (por exemplo, um ISP) que preserve determinados dados informáticos, impedindo a sua perda ou modificação, por um período de tempo específico. No ordenamento jurídico interno, a preservação de dados encontra-se prevista e regulada no artigo 12.º da Lei do Cibercrime.

Já no que diz respeito à conservação de dados, esta exige que os operadores retenham os dados gerados ou processados como resultado da atividade de todos os utilizadores dos serviços de comunicações ou de serviços de rede, para que possam ser legalmente disponibilizados às autoridades competentes e usados para fins de prevenção, deteção e repressão criminal, sendo esta a matriz da Lei n.º 32/2008.

[15] Neste sentido, cfr. Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries, European Commission Directorate General for Home Affairs, disponível em https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/police-cooperation/data-retention/docs/drd_task_2_report_final_en.pdf.

O valor da conservação obrigatória de dados de comunicações é a garantia de que todos os dados potencialmente valiosos para a investigação criminal estarão disponíveis por um determinado período de tempo.

Este valor não é despiciendo, porquanto se mostra essencial para garantir a eficácia da recolha de prova em processo penal.

Esta mesma conclusão, se bem que limitada a um juízo de eficácia acrescido, foi retirada pelo próprio Tribunal Constitucional Alemão, no Acórdão[16] em que declarou a inconstitucionalidade das normas de transposição da Diretiva n.º 2006/24/CE, ao afirmar, no seu parágrafo 208, que "*o legislador também pode julgar necessário um armazenamento de seis meses dos dados de tráfego de telecomunicações. Não é evidente a existência de meios menos drásticos que permitam obter resultados com relevância equivalente. Uma possibilidade atual seria o chamado procedimento de "congelamento rápido", mediante o qual a preservação de dados é realizada apenas em casos particulares em que exista uma concreta suspeita prévia. Tal procedimento apenas pode obter a preservação de dados prévios ao pedido caso estes existam, pelo que não é tão eficaz como a conservação contínua, a qual garante a disponibilidade da totalidade dos dados relativos aos últimos seis meses*".

Com efeito, com a cada vez mais rápida evolução tecnológica, assiste-se à transferência da criminalidade tradicional para a criminalidade cometida por meio informático, mesmo que não se trate de criminalidade estritamente informática.

Sem a possibilidade de obter dados historicamente determinados (não existe processo criminal antes de ocorrer o facto típico), ainda que por um período limitado, no caso de existir apenas um

[16] BVerfG 1 BvR 256/08 - Urteil vom 2. März 2010 – versão traduzida em inglês em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html;jsessionid=1E448A82DA6A4A5C3FB65524723990C0.2_cid361.

regime de preservação de dados (que vale apenas para os *dados que venham a ser gerados*), não será de todo possível obter a prova que é única e essencial para, pelo menos, poder ter a expectativa de identificar o ou os agentes do crime.

Verifique-se, por exemplo, uma hipotética situação de aliciamento sexual de um menor por intermédio de comunicações mantidas numa rede social: se os dados relativos à ou às comunicações do agente do crime forem apagados findas que sejam tais comunicações, não será possível, por qualquer outro meio, obter prova da origem de tais comunicações e, por conseguinte, identificar o agente do crime.

Restringir a investigação, neste caso, à obtenção de prova por recurso à preservação de dados, só funcionaria se tal ordem ocorresse antes do facto – estranhamente, e como acima se deixou claro, parece ser esta a orientação do TJUE, ao prever medidas de preservação *preventiva*, mesmo que geograficamente condicionada, ou seja, emitindo ordens de preservação que *permitam visar um público cujos dados sejam suscetíveis de revelar uma relação*, pelo menos indireta, *com atos de criminalidade grave*[17], ou seja, que as autoridades competentes discriminem de forma intolerável grupos de cidadãos, com base em critérios que até podem ser meramente geográficos (local onde se encontrem), sem qualquer facto típico cometido.

Este entendimento do TJUE, para além de conceber uma regra inaplicável, viola o Princípio da Igualdade e a proibição de discriminação[18].

Neste caso, ou em todos os casos similares, em termos de avaliação da aplicação do critério da necessidade para a restrição

[17] Acórdão Tele2 Sverige AG, parágrafo 111.

[18] Desde logo, previsto no artigo 14.º da Convenção Europeia dos Direitos do Homem: "*o gozo dos direitos e liberdades reconhecidos na presente Convenção deve ser assegurado sem quaisquer distinções, tais como as fundadas no sexo, raça, cor, língua, religião, opiniões políticas ou outras, a origem nacional ou social, a pertença a uma minoria nacional, a riqueza, o nascimento ou qualquer outra situação*".

ao direito à privacidade na circunstância de existir norma fundamento para a conservação de dados, é inequívoco que, a não ser que o legislador pretenda um *vazio de punição* – ou seja, consagre crimes que, em face dos seus requisitos típicos ou concreto modo de execução, não podem ser investigados – tem necessariamente de consagrar um regime de conservação de dados.

Sobre esta específica matéria, o Tribunal Europeu dos Direitos do Homem (doravante, TEDH) já se pronunciou, no Acórdão K.U. Vs. Finland[19] (Application n.º 2872/02), de 2 de Dezembro de 2008.

No referido caso, foi pedida a condenação do Estado Finlandês por incumprimento da sua obrigação positiva de proteger o direito ao respeito pela vida privada e familiar do requerente, de acordo com o artigo 8.º da Convenção Europeia dos Direitos do Homem (doravante, CEDH).

Em síntese, o caso referia-se à colocação de um anúncio num *website* de encontros em nome do requerente, menor de 12 anos, usando o nome, data de nascimento, descrição das características físicas, um *link* para página do menor com fotografias deste e o número de telefone, indicando que este procurava relacionamento íntimo.

No decurso do processo, o ISP recusou prestar às autoridades finlandesas os dados de identificação do utilizador do IP dinâmico que colocou o anúncio.

Numa decisão do Tribunal de Helsínquia, foi negada a obtenção de dados pela investigação, com fundamento na inexistência de norma fundamento na lei finlandesa, designadamente por se tratar de caso de difamação, decisão esta mantida em sede de recurso,

[19] Cfr. https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22notice%22],%22itemid%22:[%22001-89964%22]}

pelo que o caso foi arquivado por insuficiência de prova para a identificação do agente.

Na fundamentação da sua decisão, o TEDH referiu, no parágrafo 46, que "(…) *a previsão de um crime tem efeito dissuasor limitado se não existir meio de identificar o agente e chamá-lo à justiça*". Mais referiu, na sua análise ao âmbito de proteção dos direitos em causa, no seu parágrafo 49, que "(…) *pese embora a liberdade de expressão e a confidencialidade das telecomunicações sejam considerações relevantes (primárias) e os utilizadores de telecomunicações e de serviços de internet devam ter garantias de que a sua própria privacidade e liberdade de expressão será respeitada, tais garantias não são absolutas e devem por vezes ceder em face de outros imperativos legítimos, tais como a prevenção de crimes e a proteção dos direitos e liberdades dos outros* [tarefa esta de concordância prática que cabe ao legislador assegurar]".

O TEDH, em decisão tomada por unanimidade, considerou ter existido a violação do Direito ao respeito pela vida privada e familiar do requerente, previsto no artigo 8.º da CEDH[20], e condenou o Estado Finlandês a indemnizar o requerente.

A imperiosa necessidade de um regime de conservação de dados é igualmente fonte de preocupação a nível europeu.

De acordo com o relatório "*Evidence for necessity of data retention in the EU*", da Direcção-Geral das Migrações e Assuntos Internos, de Março de 2013[21], na análise ao impacto da decisão do Tribunal Constitucional da Alemanha, no Acórdão acima referido, "*se certos dados de tráfego não fossem armazenados, detetar e investigar certos crimes seria praticamente impossível. A experiência*

[20] Artigo 8.º da CEDH: "*1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros*".

[21] Cfr. Biblioteca em https://ec.europa.eu/home-affairs/index_en.

da Alemanha desde o acórdão do Tribunal Constitucional de anular as medidas de retenção de dados em março de 2010 pode ilustrar as consequências da ausência de retenção obrigatória de dados. De acordo com a polícia federal alemã (Bundeskriminalamt) e a polícia estadual (Landeskriminalämter), em 44,5% dos casos envolvendo pedidos de dados de tráfego de históricos, não havia outros meios para conduzir a investigação. Relataram que 30% dos casos criminais entraram em colapso desde o julgamento do Tribunal Constitucional".

Igualmente, no Relatório da Comissão ao Conselho e ao Parlamento Europeu de Avaliação sobre a Diretiva relativa à conservação de dados (2006/24/CE)[22] sustenta-se que "*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*".

Como se acaba de expor, é estritamente necessária, para a finalidade exclusiva de investigação, deteção e repressão criminal no âmbito do processo penal, a conservação de dados a fim de permitir a obtenção de dados historicamente determinados.

Admitir apenas a preservação de dados cria um vazio de punição, pela manifesta impossibilidade de obtenção de prova do facto típico e sua autoria num cada vez maior número de casos, desprotegendo as vítimas e tornando letra morta crimes que o legislador entendeu consagrar no ordenamento jurídico.

[22] Disponível para consulta, em versão traduzida para a língua portuguesa, em http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2011)0225_/com_com(2011)0225_pt.pdf-

Trata-se não apenas de uma medida adequada, mas em muitos casos, é mesmo a única que permite obter prova do facto, como se demonstrou.

Importa é que se prevejam as necessárias alterações ao regime de conservação de dados, a fim de impossibilitar qualquer forma de "*profiling*" ou cruzamento de dados pessoais, salvo os dados concretos e determinados que sejam legitimamente obtidos e possam ser cruzados não na base de dados, mas já dentro do processo penal formal, com todas as garantias de defesa inerentes.

E, como de resto já se encontra previsto na atual Lei n.º 32/2008, a definição dum prazo certo e determinado para a conservação dos dados, findo o qual os mesmos são destruídos, a não ser em casos de pedido anterior ao termo de prazo da preservação de certos e determinados dados.

V. O Problema da Obrigação de Conservação e Transterritorialidade dos Dados

O segundo grande argumento aduzido pelo TJUE refere-se, essencialmente, à inexistência de previsão obrigando à conservação dos dados dentro do território da União Europeia.

Este argumento tem grandes implicações, desde logo em termos de regras de concorrência, pois que, se, a nível nacional e com os operadores estabelecidos em cada país, a consagração de uma tal norma fosse viável (como acontece, na prática, em Portugal), esta criaria limitações em termos de localização dos seus centros de dados e da gestão dos mesmos às quais os operadores externos, num mercado globalizado, não estariam adstritos.

Atualmente, ao nível da União Europeia, está em curso um processo legiferante que abordará esta problemática no quadro da cooperação judiciária.

Trata-se da proposta de Regulamento para a Decisão Europeia de Preservação e Produção de Prova Digital em matéria criminal e da proposta de Diretiva para a harmonização das regras de nomeação de legais representantes para a finalidade de recolha de prova em procedimentos criminais (pacote *e-evidence*)[23].

Alguns dos princípios em que se baseia a proposta devem ser tidos em conta na hipótese de revisão da Lei n.º 32/2008.

Quanto à proposta de Regulamento, são as seguintes:

a) Afasta-se do princípio da territorialidade estrita quanto ao local de armazenamento dos dados – confere obrigações ao prestador de serviço, onde quer que este armazene os dados;
b) Cria um mecanismo de rápida obtenção de dados, a efetuar diretamente ao legal representante do operador detentor dos mesmos;
c) Redefine os conceitos de tipos (classes) de dados, com a maior importância na distinção entre dados de subscrição e dados de acesso (categorias dos tradicionais dados de base).

Quanto à proposta de Diretiva, que se destina à harmonização das regras de nomeação de legais representantes para a finalidade de recolha de prova em procedimentos criminais, estabelece os seguintes princípios:

a) Torna obrigatório aos prestadores de serviços a designação de um legal representante na União Europeia, para receber e dar cumprimento às decisões das autoridades nacionais competentes em processos criminais destinadas à recolha de prova digital.
b) Define um âmbito alargado de aplicação, que inclui os prestadores de serviços sediados num Estado-membro e que oferecem serviços apenas no território daquele Estado-membro,

[23] Para uma visão global da proposta de regulamento e proposta de diretiva, consultar https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

os prestadores de serviços sediados num Estado-membro e que oferecem serviços em vários Estados-membros e os prestadores de serviços sediados fora da União e que oferecem serviços num ou em vários Estados-membros, tenham ou não um estabelecimento num ou mais desses Estados-membros.

VI. Impacto da Entrada em Vigor do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016 (RGDP)[24]

A entrada em vigor do RGPD[25] coloca particulares e prementes questões que importa resolver, por via legislativa, designadamente na Lei n.º 32/2008.

A Lei n.º 32/2008 é o único diploma legal no nosso ordenamento jurídico que expressamente consagra um regime de conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes.

Tratam-se, inequivocamente, de dados pessoais, de cujo tratamento se encontram incumbidas entidades privadas, os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações, ou seja, os dados conservados no âmbito da Lei n.º 32/2008 encontram-se abrangidos pela proteção conferida pelo RGPD.

[24] Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32016R0679.

[25] De acordo com a norma contida no artigo 288.º do TFUE, "O regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros". Na norma contida no artigo 99.º do RGPD, dispõe-se que "O presente regulamento é aplicável a partir de 25 de Maio de 2018".

De acordo com o considerando 19 do RGPD, "*a proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico*[26]. *Nos casos em que o tratamento de dados pessoais por organismos privados fica abrangido pelo presente regulamento, este deverá prever a possibilidade de os Estados-Membros restringirem legalmente, em determinadas condições, certas obrigações e direitos, quando tal restrição constitua medida necessária e proporcionada, numa sociedade democrática, para salvaguardar interesses específicos importantes, incluindo a segurança pública e a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública*".

Ou seja, é possível restringir certos direitos previstos para os titulares dos dados no RGDP desde que tal restrição seja proporcional, adequada e necessária à salvaguarda de interesses específicos, designadamente a deteção ou repressão de infrações penais.

Este predicado encontra concretização no artigo 23.º do RGDP[27] e obriga a que, nos diplomas legais de cada

[26] Trata-se da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho.

[27] Artigo 23.º (Limitações): 1 - O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, (…) desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:
d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;
2 - Em especial, as medidas legislativas referidas no n.º 1 incluem, quando for relevante, disposições explícitas relativas, pelo menos:
a) Às finalidades do tratamento ou às diferentes categorias de tratamento; b) Às categorias de dados pessoais; c) Ao alcance das limitações impostas; d) Às garantias para evitar o abuso ou o acesso ou transferência ilícitos; e) À especificação do responsável pelo tratamento ou às categorias de responsáveis pelo tratamento; f) Aos prazos de conservação e às garantias aplicáveis, tendo em conta a natureza, o âmbito e os objetivos do tratamento ou das categorias de tratamento; g) Aos riscos específicos para os direitos e liberdades dos titulares dos

Estado-Membro, sejam efetuadas as necessárias alterações legislativas que permitam, de acordo com os critérios ali definidos, operar qualquer uma das restrições ao exercício dos direitos dos titulares dos dados.

No caso vertente da Lei n.º 32/2008, são essencialmente dois os direitos cujo exercício se mostra proporcional, adequado e necessário restringir, sob pena de frustração da acção do sistema formal de justiça em processo criminal quanto à obtenção de prova: o direito de oposição ao tratamento e o direito de acesso do titular dos dados.

No n.º 1 do artigo 21.º do RGPD define-se o direito de oposição considerando-se que "*o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito*".

Quanto a esta restrição, a mesma encontra já eco no n.º 4 do artigo 3.º da Lei n.º 32/2008 ao consagrar que "*o titular dos dados não pode opor-se à respetiva conservação e transmissão*".

Outrossim já não ocorre quanto à previsão da limitação ao direito de acesso do titular dos dados.

O n.º 1 do artigo 15.º do RGPD, e particularmente a alínea c) do referido preceito, prescreve que "*o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:* (…) *Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais*".

dados; e h) Ao direito dos titulares dos dados a serem informados da limitação, a menos que tal possa prejudicar o objetivo da limitação.

Ora, inexiste na Lei n.º 32/2008 qualquer previsão normativa consagrando uma limitação a este direito, que tem uma consequência prática evidente: sempre que, no decurso de um processo penal, seja solicitada pela autoridade judiciária competente o acesso a um qualquer dado conservado no âmbito deste regime (o que se aplica, igualmente, aos dados conservados para efeitos de faturação), o responsável pelo tratamento dos dados do fornecedor de serviço de comunicações tem a obrigação, nos termos previstos no RGPD, de comunicar ao titular dos dados que alguns específicos dados pessoais foram divulgados, bem como a que entidade o foram.

As consequências desta omissão relativamente à obtenção de prova em processo penal são manifestas, desde logo por permitirem a eventuais suspeitos da comissão de um crime saber que se encontram sob investigação.

Mesmo admitindo-se que, em alguns casos, o regime de segredo de justiça (quando exista fundamento para tal, dado que a atual regra é a publicidade do processo penal) possa atenuar o efeito da não previsão legal da limitação ao direito de acesso do titular dos dados, importa proceder à necessária alteração da Lei n.º 32/2008.

Tal alteração deverá igualmente contemplar a consagração do direito à informação prévia do titular dos dados relativamente ao regime de conservação de dados e suas finalidades, bem como às restrições de direitos que lhe sejam aplicáveis, em cumprimento aliás do disposto no artigo 13.º do RGPD.

Finalmente, e na sequência da estrita limitação ao tratamento dos dados conservados no âmbito da Lei n.º 32/2008, designadamente por parte do fornecedor de serviços de comunicações, deve atentar-se no critério definido no n.º 1 do artigo 22.º do RGPD, segundo o qual "*o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar*".

VII. Conclusão: A Reforma que se Impõe

Tendo em conta o quadro traçado, entendemos que se impõe a reforma da Lei n.º 32/2008, mantendo o critério da conservação de dados, a qual deverá ser norteada pela lógica de criação do *repositório único* de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações pelas entidades prestadoras desse serviço, com *um só prazo de conservação*, para fim exclusivo de investigação, deteção e repressão criminal no âmbito do processo penal.

Com urgência, deverá densificar as normas relativas à transparência e proteção dos direitos do cidadão, bem como adequar as limitações desses direitos ao RGPD mantendo os prestadores de serviços a obrigação de designarem os responsáveis pelo tratamento de dados, condicionando tal tratamento a operações de acesso para transmissão encriptada de dados concretos e específicos legitimamente provindas da autoridade judiciária competente.

Deverá igualmente adensar e especificar as obrigações dos prestadores de serviços de comunicações, designadamente eletrónicas, proibindo por qualquer forma a existência de operações, designadamente automáticas, de cruzamento de dados, ou quaisquer outras aptas ao "*profiling*" dos titulares dos dados.

Concomitantemente, quer para adequar o sistema à futura regulamentação europeia, mas igualmente com o fito de impedir, desde logo pelo seu armazenamento separado, quaisquer cruzamentos dos dados armazenados, prever a distinção (a ocorrer quando tecnicamente possível), entre dados de subscrição, dados de acesso[28], dados de tráfego e dados de localização.

[28] Que seriam, em síntese, os dados relativos ao início e à cessação de uma sessão de acesso do utilizador a um serviço com o único propósito de identificar o usuário do serviço – o critério do "*one shot*", ou seja, o dado específico de acesso ao serviço – não qualquer correspondente dado comunicacional, que se enquadra já na classe dos dados de tráfego.

Criando-se um repositório único, importa ainda modificar a regulação do regime de acesso aos dados, designadamente contemplando as formas de acesso por parte da autoridade judiciária e, por virtude de tal circunstância, adequar o catálogo de crimes[29] que permitem o acesso a uma ou várias das classes de dados conservados, para o efeito específico e único de investigação, deteção e repressão criminal no âmbito do processo penal.

No essencial, se bem que com adequação a um ordenamento jurídico diverso, estes princípios foram já seguidos na alteração da Lei Belga relativa às comunicações eletrónicas, de 29 de Maio de 2016[30].

Nestes termos, entendemos que não se justifica a "*aposentação*" da Lei n.º 32/2008, mas sim que se impõe, com urgência, a sua reforma, dando-lhe um sentido útil.

[29] Que deverá, com especificidades para dados de cada uma das classes, abranger os tipos legais previstos no catálogo do n.º 1 do artigo 187.º do Código de Processo Penal e nas alíneas a) e b) do n.º 1 do artigo 11.º da Lei do Cibercrime.

[30] Disponível para consulta em http://www.dekamer.be/FLWB/PDF/54/1567/54K1567001.pdf.