FORUM
DE PROTEÇÃO DE DADOS

N.º 03 JULHO 2016 SEMESTRAL

EM FOCO

GEO LOCALIZAÇÃO

OPINIÃO DE FERNANDO NEGRÃO

MOTORES DE BUSCA:
O DIREITO A NÃO SER LISTADO

ACESSO A DADOS DE TRÁFEGO

FORUM
DE PROTEÇÃO DE DADOS

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

ANOTAÇÃO

1. O presente acórdão do Tribunal da Relação de Lisboa confirma o despacho judicial inicial que negou a pretensão do Ministério Público de, no âmbito da investigação de um crime de roubo num estabelecimento comercial, aceder aos dados de localização e de tráfego relativos a todos os dispositivos de comunicação que se encontravam numa determinada área (envolvente daquele estabelecimento), num determinado período temporal, conservados pelas operadoras de comunicações eletrónicas.

No essencial, apesar de o Ministério Público ter alegado a imprescindibilidade do acesso a tais dados para identificar os suspeitos do crime e de o tipo de crime ser considerado grave (na categoria de criminalidade violenta), o Tribunal da Relação considerou que o acesso aos dados de todas as pessoas que se encontravam naquela zona e naquele período não preenche o pressuposto de os dados serem relativos a suspeitos, exigido no n.º 3 do artigo 9.º da Lei n.º 32/2008, de 17 de julho, uma vez que não existem quanto a elas indícios da prática de crime, o que constituiria uma violação da privacidade das mesmas.

2. Importa, antes do mais, assinalar que os dados cujo acesso é pretendido são dados pessoais, porque constituem informação relativa a pessoas identificadas ou identificáveis (abrangendo os dados conexos necessários para a identificação do dispositivo de comunicação e do seu utilizador), e que, por revelarem dados da vida privada (localização e pessoas com quem se comunicou), estão sujeitos a um regime jurídico de proteção reforçado – cf. n.º 3 do artigo 35.º da Constituição da República Portuguesa e artigo 7.º da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto – Lei de Proteção de Dados Pessoas (LPDP).

Apesar da proibição geral de conservação e acesso aos dados pessoais relativos a comunicações eletrónicas, constante da Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, o legislador nacional, em transposição da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, tendo em vista a harmonização dos direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais com outros bens jurídicos fundamentais, veio, na Lei n.º 32/2008, de 17 de julho, impor às empresas que prestam serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas o dever de conservação de tais dados pessoais e da sua transmissão para efeitos de investigação de crimes graves. É ao abrigo deste diploma que o Tribunal decide, e não, como bem esclarece no acórdão, ao abrigo dos artigos 187.º a 189.º do Código de

Processo Penal[1]. Com efeito, está em causa o acesso a dados pessoais relativos a comunicações conservados pelas operadoras do setor das comunicações eletrónicas e não o acesso a tais dados em tempo real.

É certo que a Diretiva que a Lei n.º 32/2008 transpõe foi declarada inválida pelo Tribunal de Justiça da União Europeia (TJUE) – no acórdão de 8 de abril de 2014, processos C-293/12 e C-594/12 – e que o legislador nacional ainda não retirou as consequências devidas de tal declaração, em especial quanto ao caráter excessivo da conservação de informação desta natureza, relativa à vida privada, de todos os que utilizem comunicações eletrónicas independentemente de sobre eles existir ou não indício de atividade criminosa[2].

O acórdão do Tribunal da Relação de Lisboa, não se pronunciando sobre a conformidade da lei com a Constituição portuguesa e com a Carta dos Direitos Fundamentais da União Europeia, assenta na aparente legitimidade da conservação de dados pessoais relativos às comunicações eletrónicas pelas operadoras, mas acaba por ter subjacente um juízo paralelo de desproporcionalidade quanto ao acesso aos dados de todos os que se encontrem em determinada área e por um determinado período de tempo quando sobre eles não existe indício de prática de crime.

Na verdade, o Tribunal considera não estar preenchido o pressuposto do n.º 3 do artigo 9.º da Lei n.º 32/2008, por não se encontrarem delimitados os dados a aceder, nem em termos subjetivos (uma ou mais pessoas identificadas), nem em termos objetivos (um concreto dispositivo de comunicação eletrónica), pelo que o deferimento do pedido «transformaria em suspeitos todos aqueles que no momento estivessem ou passassem pelo local». E, transcrevendo a importante afirmação constante do acórdão do Tribunal da Relação de Évora de 18 de outubro de 2011 (Proc. n.º 19/11.6GGEVR-A.E1), defende que o que se pretende aqui é «[…] a autorização para que se abra um caminho que possa vir a tornar-se meio de obtenção de prova; pretende-se que se destape uma caixa de Pandora e que dela ressalte o fio que haverá de conduzir a uma pista de investigação e permita dar corpo a um qualquer grau de suspeita, até agora inexistente. Trata-se, manifestamente, de pretensão que, para

1) Uma observação merece a referência que, neste acórdão, o Tribunal faz à Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), quando afirma que «[…] a Lei n.º 32/2008 se mantém em vigor na parte "arquivística" em relação aos dados contidos no seu artigo 4.º, não sendo invocável para o caso aquela, relativa a comunicação eletrónica, uma vez que se pretendem dados relativos a comunicação telefónica».

Reservando para outra ocasião a análise do entendimento, refletido nesta afirmação, de que a Lei n.º 109/2009 revogou parcialmente a Lei n.º 32/2008, cujo fundamento não se consegue acompanhar – desde logo face à salvaguarda do regime da Lei n.º 32/2008 constante do n.º 2 do artigo 11.º da Lei do Cibercrime, a qual não pode pura e simplesmente ser ignorada –, importa assinalar a aparente confusão que aquela afirmação deixa transparecer a propósito do conceito de comunicação eletrónica e do âmbito de aplicação da Lei n.º 32/2008.

Com efeito, as comunicações telefónicas em redes fixa e móvel, porque se realizam por via digital (e não ou, pelo menos, não totalmente analógica), cabem inegavelmente no conceito de comunicações eletrónicas. Basta a leitura do n.º 1 do artigo 1.º e o n.º 2 do artigo 4.º desta lei para afastar quaisquer dúvidas quanto ao facto de esta regular a conservação e as condições de acesso aos dados de tráfego e de localização relativos às comunicações eletrónicas, o que inclui as comunicações telefónicas. Atente-se, aliás, no ponto 56 do acórdão do Tribunal de Justiça da União Europeia (processos C-293/12 e C-594/12) de 8 de abril de 2014, onde se sublinha que a Diretiva que a Lei n.º 32/2008 veio transpor tem por objeto os «dados relativos ao tráfego respeitante à rede telefónica fixa, à rede telefónica móvel, ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet». Não será, pois, este o critério suscetível de delimitar o âmbito de aplicação da Lei do Cibercrime em relação à Lei n.º 32/2008.

2) Para mais desenvolvimentos, pode ver-se a anotação ao referido acórdão do TJUE, de Clara Guerra e Filipa Calvão, em Forum da Proteção de Dados n.º 1, 2015, pp. 77-80, disponível em https://www.cnpd.pt/bin/revistaforum/forum2015_1/index.html

além de ferir os ditames legais, se apresenta desprovida de razoabilidade, é desproporcionada e inadequada e que a perseguição do crime em investigação não justifica, face à devassa intolerável que o seu deferimento claramente constituiria».

A este propósito, assinala-se que a alegação do Ministério Público de que «os dados obtidos, atenta a forma como solicitados, não violariam a privacidade de qualquer cidadão» revela um limitado entendimento do direito ao respeito pela vida privada, consagrado não apenas nos artigos 24.º, 26.º e 35.º, n.º 3, da Constituição, mas também no artigo 7.º da Carta dos Direitos Fundamentais da União Europeia e no artigo 8.º da Convenção Europeia dos Direitos do Homem, e contraria o regime jurídico decorrente das Diretivas relativas à privacidade nas comunicações eletrónicas (Diretivas 2002/58/CE e 2009/136/CE, que a Lei n.º 41/2004, citada acima, transpôs). A privacidade não se restringe ao conteúdo das comunicações, sendo evidente que muito da vida privada de cada um se revela na informação quanto ao local onde se encontra e na informação relativa às pessoas com quem comunica. E revela-se mesmo quando se esta se limita, como sucedeu no pedido, a uma determinada área espacial e a um período de tempo relativamente curto.

3. Não sendo inovador, por reiterar argumentos e o sentido da decisão vertidos no acórdão do Tribunal da Relação de Évora de 18 de outubro de 2011, já citado, o acórdão aqui em apreço é relevante por duas ordens de razão.

Em primeiro lugar, por retomar uma jurisprudência quanto ao âmbito do conceito de suspeito e ao reconhecimento de limites na investigação criminal decorrentes do respeito pela vida privada das pessoas que não integram aquela categoria, em congruência com a jurisprudência do TJUE, ao contrário do que sucedeu no acórdão do Tribunal da Relação de Évora, de 20 de janeiro de 2015 (Proc. 648/14GCFAR-A.E 1), o qual, numa situação similar, admitiu o acesso aos dados pessoais pretendidos.

Em segundo lugar, pelo facto de, num tempo em que a segurança e a luta contra a criminalidade grave vêm reclamando poderes de investigação alargados e a tecnologia tem cada vez mais o potencial de facilitar a abertura de linhas de investigação quando não existem indícios significativos da autoria de crimes, reafirmar que, num Estado de Direito, os direitos fundamentais não podem ser ignorados ou sacrificados sem mais. As técnicas de data mining (que, grosso modo, corresponde ao processo de deteção e identificação de padrões nos dados conservados) e as múltiplas bases de dados pessoais não podem ser usadas sem que se faça uma cuidada ponderação dos interesses envolvidos e dos direitos fundamentais dos titulares dos dados, considerando todas as implicações da sua utilização, sobretudo na perspetiva da salvaguarda da privacidade e da liberdade humana.

Filipa Calvão

FICHA TÉCNICA

Título
Forum de Proteção de Dados

Proprietário e Editor
Comissão Nacional de Protecção de Dados

Diretor
Filipa Calvão

Sede da redação
Rua de São Bento, 148, 3º 1200-821 Lisboa

Periodicidade
Semestral

Tiragem
500 exs

Design e produção gráfica
Estrelas de Papel Lda.
Lisboa

ISSN 2183-5977

Julho 2016

Impresso em papel reciclado Munken Lynkx 120grs.

Isento de registo na ERC ao abrigo da alínea b) do artigo 12.º do Decreto Regulamentar n.º 8/99, de 9 de junho, alterado por último pelo Decreto Regulamentar n.º 2/2009, de 27 de janeiro.

PRÉMIO ENSAIO

DA COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

Candidaturas até

31OUT. 2016

Aberto a trabalhos académicos e outros de investigação sobre proteção de Dados Pessoais

ÁREAS DAS CIÊNCIAS SOCIAIS E DAS CIÊNCIAS E TECNOLOGIAS

Regulamento disponível em **www.cnpd.pt**

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS