

NEWSLETTER CVA



A CONTROVÉRSIA SOBRE OS METADADOS E O DIREITO DA UE

Na atual era digital, os dados são cada vez mais valiosos e ubíquos. Desde publicações nas redes sociais a transações financeiras, geramos grandes quantidades de dados todos os dias. No entanto, o valor dos dados não reside apenas no seu conteúdo, no sentido tradicional, mas, também, nos seus metadados (ou “dados sobre dados”).[1] Com o aumento da tecnologia digital, os metadados tornaram-se uma rica fonte de provas em investigações criminais, especialmente em casos que envolvem cibercriminalidade, terrorismo e fraude financeira, devido à informação contextual crucial que podem fornecer.

No entanto, a utilização de metadados pode, ao mesmo tempo, levantar questões importantes relacionadas com a privacidade e a proteção dos dados pessoais. Em primeiro lugar, os metadados podem ser utilizados para inferir informações pessoais sobre os indivíduos. Em segundo lugar, os metadados são muitas vezes gerados automaticamente por dispositivos e serviços eletrónicos e as pessoas podem não ter conhecimento da sua recolha ou utilização, colocando em risco os seus dados pessoais e o seu direito à privacidade. Por último, os metadados têm sido gradualmente utilizados pelos governos e

[1] O termo “metadados” designa geralmente os dados que englobam as circunstâncias das comunicações, mas excluem o seu conteúdo (ver, neste sentido, o acórdão n.º 268/2022, do Tribunal Constitucional, n.º 6.1.).

pelas forças de segurança para efeitos de vigilância, alegadamente em detrimento das liberdades civis e dos direitos fundamentais.

I. O impacto do acórdão *Digital Rights Ireland* na conservação de dados

A. *Digital Rights Ireland* e a declaração de invalidade da diretiva relativa à conservação de dados

Em 2006, a conservação obrigatória de dados foi harmonizada a nível da União Europeia ("UE") através da Diretiva 2006/24/CE ("Diretiva relativa à Conservação de Dados"). Esta diretiva destinava-se a ajudar as autoridades nacionais responsáveis pela aplicação da lei na investigação e prevenção de crimes graves. Procurou também resolver a disparidade das medidas nacionais (ver o considerando 6 da Diretiva relativa à Privacidade e às Comunicações Eletrónicas) adotadas com base no n.º 1 do artigo 15.º da Diretiva 2002/58/CE ("Diretiva relativa à Privacidade e às Comunicações Eletrónicas"), que permitia aos Estados-Membros limitar o direito à privacidade das comunicações eletrónicas, desde que visassem salvaguardar a segurança nacional (rectius, a segurança do Estado), a defesa, a segurança pública e a prevenção, investigação, deteção e repressão de infrações penais.

Contudo, em 2014, o Tribunal de Justiça da União Europeia ("TJUE" ou "Tribunal") declarou, no caso *Digital Rights Ireland*, a invalidade da Diretiva relativa à Conservação de Dados. Apesar de reconhecer que a retenção de dados satisfaz genuinamente objetivos de interesse geral no combate à alta criminalidade, o Tribunal considerou que a diretiva não respeitava o princípio da proporcionalidade, uma vez que a interferência nos direitos fundamentais não se limitava ao estritamente necessário. Em particular, o TJUE observou que a Diretiva relativa à Conservação de Dados obrigava as operadoras de telecomunicações a armazenar dados pessoais sensíveis dos utilizadores durante um ano, incluindo informações sobre aspetos da vida privada e familiar, como a localização e os contactos, sem qualquer ligação a atividades criminosas, e sem permitir que os utilizadores se opusessem a essa recolha. Além disso, não existiam exceções para as comunicações abrangidas pelo sigilo profissional e, simultaneamente, não existiam medidas de segurança para proteger os dados pessoais.

A Diretiva relativa à Conservação de Dados foi assim declarada inválida, uma vez que o TJUE considerou que restringia desproporcionadamente os direitos ao respeito pela vida privada e familiar e à proteção dos dados pessoais, consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia ("CDFUE").

Em resultado deste acórdão, a Diretiva relativa à Privacidade e às Comunicações Eletrónicas (re)assumiu o seu papel de base jurídica para a legislação nacional relativa à conservação de dados. Embora o acórdão *Digital Rights Ireland* não tenha afetado a validade dessa diretiva, a conservação e a utilização de metadados com base no seu artigo 15.º, n.º 1, tendo, também,

em conta a sua redação e natureza (designadamente, "(...) sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas (...)", tem necessariamente de estar em conformidade com os requisitos estabelecidos pelo Tribunal nesse acórdão. Isto decorre do facto de os Estados-Membros estarem proibidos de aplicar legislação nacional que transponha uma diretiva inválida, na medida em que essa legislação esteja em contradição com os fundamentos da decisão do Tribunal. De facto, os acórdãos proferidos pelo TJUE têm efeitos "erga omnes", pelo que vinculam o legislador, a administração e o poder judicial de todos os Estados-Membros.

Por isso, é da maior importância que sejam implementadas medidas adequadas para salvaguardar a proteção dos dados pessoais e da privacidade dos cidadãos europeus, em conformidade com este entendimento do TJUE. Aliás, e como adiante se explica, a disposição reposta pelo acórdão *Digital Rights Ireland* já exigia que as medidas restritivas do âmbito dos direitos e obrigações previstos no direito da UE respeitassem o princípio da proporcionalidade.

Neste contexto, na sequência do acórdão do TJUE, vários tribunais nacionais foram chamados a pronunciar-se sobre a legislação nacional adotada para aplicar a Diretiva relativa à Conservação de Dados. Na sequência desses processos, alguns tribunais optaram pelo reenvio prejudicial (C-140/20; C-623/17; C-511/18). Num desses cenários - *Tele2 Sverige* -, o TJUE confirmou que a invalidade da Diretiva relativa à Conservação de Dados afetava, efetivamente, a implementação de disposições nacionais que permitem uma obrigação generalizada e indiferenciada de conservação de metadados.

Declarou ainda que a interpretação da Diretiva relativa à Privacidade e às Comunicações Eletrónicas, nomeadamente o n.º 1 do seu artigo 15.º, deve ter em consideração a importância do direito à privacidade e do direito à proteção dos dados pessoais, tal como garantidos pela CDFUE. Além disso, como a lista de objetivos estabelecida nesse artigo é exaustiva, os Estados-Membros não podem adotar medidas para outros fins que não os mencionados nessa mesma disposição (*Tele2 Sverige*, n.º 90).

Isto limita o direito dos Estados-Membros de introduzir exceções à obrigação de garantir a confidencialidade dos dados pessoais. Consequentemente, nos Estados-Membros, como Portugal, onde a legislação que transpõe a Diretiva relativa à Conservação de Dados continuou a ser aplicada mesmo após a declaração de invalidade dessa diretiva, muitas condenações basearam-se num acesso potencialmente ilegal aos dados.

B. A situação em Portugal na sequência do acórdão *Digital Rights Ireland*

A Diretiva relativa à Conservação de Dados foi transposta para o ordenamento jurídico português pela Lei n.º 32/2008, de 17 de julho (“Lei dos Metadados”). A lei define “metadados” como os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador. Tais dados permitem identificar todos os dados relativos às comunicações eletrónicas, incluindo a localização, a identificação da fonte e do destino da comunicação, a data, a hora, a duração da comunicação, o tipo de comunicação e o equipamento utilizado, com exceção do seu conteúdo ou teor.

Ainda que não tenha sido apresentado qualquer pedido de decisão prejudicial pelos tribunais portugueses, como provavelmente deveria, o acórdão do TJUE no caso *Digital Rights Ireland* não passou despercebido em Portugal. A Comissão Nacional de Proteção de Dados (“CNPD”) emitiu duas recomendações para a não aplicação e revisão da Lei dos Metadados em processos que lhe foram submetidos (Deliberação n.º 641/2017, de 09 de maio de 2017, e deliberação n.º 1008/2017, de 18 de julho de 2017). Além disso, a Provedora de Justiça recomendou ao Governo, em janeiro de 2019, que a Lei dos Metadados fosse tornada conforme com os requisitos da CDFUE e que fosse colmatada a lacuna de supervisão existente em Portugal.

Na ausência de quaisquer manifestações de vontade em alterar a lei, a Provedora de Justiça apresentou um requerimento junto do Tribunal Constitucional (“TC”), no sentido de este apreciar e declarar a desconformidade com a Constituição da República Portuguesa (“CRP”) da retenção generalizada e indiscriminada de dados de tráfego e de localização de assinantes e utilizadores registados para a finalidade específica de investigação, deteção e repressão de crimes, independentemente da sua natureza.

No seu Acórdão n.º 268/2022, o Tribunal Constitucional declarou a desconformidade com a CRP, com força obrigatória geral, das normas constantes da Lei dos Metadados.[2]

[2] No seu acórdão, o Tribunal Constitucional clarificou devidamente a relação (e as diferenças...) entre a análise da conformidade de uma legislação nacional com o direito comunitário e a análise da constitucionalidade dessa mesma legislação com a Constituição nacional: “(...) a incompatibilidade de certa norma nacional com o direito da União Europeia não implica, de forma automática, um juízo de inconstitucionalidade; provoca, ao invés, uma afetação da sua eficácia no plano interno, na medida em que contradiga regras europeias simultaneamente mobilizáveis. E, nos termos como o direito da União Europeia o define, este efeito dá-se independentemente da fonte das normas conflituantes: quer a norma europeia conste de direito originário (como a CDFUE, nos termos do artigo 6.º do TUE) ou derivado (como uma diretiva ou um Regulamento); quer a norma nacional conste de ato regulamentar, de ato legislativo ou mesmo da Constituição. Pelo que a demonstração da contradição das normas em crise com o direito da União Europeia não permite inferir uma conclusão pela respetiva inconstitucionalidade. O juízo de inconstitucionalidade — e, assim, da invalidade da norma nacional — depende da desconformidade das normas fiscalizadas com o seu parâmetro hierarquicamente superior — maxime, a Constituição”.

Em concreto, o TC declarou:

A inconstitucionalidade do artigo 4.º da referida lei, conjugada com o artigo 6.º da mesma lei, relativo à conservação e armazenamento dos dados aí referidos, pelo período de um ano, foi declarada com fundamento, designadamente, na violação do direito à autodeterminação informativa. Segundo o TC, este direito está consagrado no artigo 35.º da CRP, que garante ao seu titular o poder de decidir sobre a utilização e divulgação dos seus dados pessoais, bem como o poder de controlar a informação disponível sobre si. Tal direito é complementado pelo poder de controlo do tratamento dos dados e pelo dever do Estado de proteger esse direito, ambos constitucionalmente consagrados.

O Tribunal Constitucional observou ainda que, para exercer esse controlo, os cidadãos devem ter conhecimento de que os seus dados foram acedidos. O TC sustentou ainda que esse controlo deve ser garantido por uma autoridade administrativa independente, constitucionalmente prevista - o que significa que os dados não podem ser armazenados em jurisdições fora desse controlo (isto é, fora do território da UE).

Não obstante, o armazenamento de dados básicos - endereços de protocolo ("IP") e outros dados básicos como a identidade civil dos titulares de números de telefone e endereços de correio eletrónico e endereços de IP dinâmicos relativos à fonte de uma comunicação -, independentemente do período previsto de um ano, não seria, em si mesmo, inconstitucional se o legislador tivesse cumprido a obrigação de garantir que o armazenamento se efetua no território da União Europeia, o que não aconteceu.

Em contrapartida, o Tribunal Constitucional afirmou que o mesmo não acontece no que respeita à obrigação de conservação dos dados de tráfego, gerados a propósito de uma específica comunicação, com especial relevância para os dados de localização. Neste caso, a compressão do direito fundamental à intimidade da vida privada é mais intensa, o que se repercute na proporcionalidade da restrição. A conservação destes dados é, pois, manifestamente excessiva.

O TC acrescentou, também, que, "se a medida de conservação de dados de tráfego e de localização em si mesma pode ser tida como adequada e necessária para os fins de interesse público que visa salvaguardar, a definição do leque de sujeitos visados só não transgredir os limites da proporcionalidade na medida em que se dirija, de forma direta, às situações em que a agressão aos direitos fundamentais em causa possa ter-se por orientada à perseguição dos objetivos da ação penal. Neste quadro, por se ultrapassarem na medida fiscalizada os limites da proporcionalidade no que concerne ao respetivo âmbito subjetivo, viola-se o n.º 2 do artigo 18.º da Constituição na restrição aos direitos fundamentais à reserva da intimidade da vida privada e à autodeterminação informativa (artigos 26.º, n.º 1, e 35.º, n.º 1, CRP), perdendo relevância a questão de saber se os demais elementos de que dependeria a proporcionalidade da medida (o ajustamento do prazo de conservação ao

estritamente necessário para os fins a alcançar; e a imposição de condições de segurança do respetivo armazenamento) são preenchidos pela regulamentação fiscalizada”.

Decidiu, então, o Tribunal Constitucional que, ao conjugar os artigos 4.º e 6.º da Lei n.º 32/2008, em causa, a obrigação de recolha e conservação dos dados pessoais aí elencados pelo período de um ano, condiciona, no mínimo, os direitos ao respeito pela intimidade e vida privada, ao livre desenvolvimento da personalidade e à autodeterminação informativa.

O TC examinou, igualmente, o artigo 9.º da Lei dos Metadados, relativo à transmissão de dados armazenados às autoridades competentes para a investigação, deteção e repressão de crimes graves. Considerando que não prevê a notificação das pessoas visadas cujos dados tenham sido acedidos pelas autoridades de polícia criminal, na medida em que essa comunicação não seja suscetível de comprometer as investigações ou a vida ou a integridade física de terceiros, existe uma violação do princípio da proporcionalidade por restringir os direitos à privacidade, ao sigilo das comunicações e à proteção judicial efetiva. O direito de alguém ter conhecimento do tratamento dado aos seus dados pessoais é, em si mesmo, inalienável.

Assim, o Tribunal Constitucional decidiu declarar a inconstitucionalidade dos artigos 4º, 6º e 9º da Lei 32/2008.

Em boa verdade, considerando o conteúdo da Lei dos Metadados e tendo em conta o acórdão *Digital Rights Ireland* do TJUE, este desfecho era altamente expectável. Mais do que isso, dado o princípio do primado do direito da UE e a força vinculativa dos acórdãos do Tribunal (acima referidos), todas as disposições nacionais afetadas pelas deficiências identificadas pelo TJUE em disposições semelhantes da diretiva deveriam ter sido imediatamente desaplicadas, sem necessidade de esperar por um acórdão “confirmatório” do Tribunal Constitucional.

II. O que esperar no futuro dos diferentes atores envolvidos?

Desde que a Lei dos Metadados entrou em vigor em 2008, as autoridades portuguesas têm utilizado os metadados como prova legítima no âmbito de processos penais, nomeadamente em casos de fraude na Internet. A despeito do acórdão *Digital Rights Ireland* do TJUE, Portugal manteve a sua lei nacional de transposição da Diretiva relativa à Conservação de Dados até 2022. Assim, durante cerca de nove anos, a lei portuguesa obrigou as operadoras de telecomunicações a reter metadados, incluindo informações sobre o tempo e a duração das comunicações, os números marcados e a localização do dispositivo utilizado. Atendendo a que, sem metadados, se torna muito difícil identificar e monitorizar suspeitos ou os seus dispositivos tecnológicos, é fundamental, por razões de segurança pública, que Portugal adote, o mais rapidamente possível, regras que cumpram o direito comunitário e a CRP e respeitem os direitos fundamentais, sem perder eficácia no

combate a crimes graves (ver Declaração Conjunta de Chefes de Polícia Europeus – Declaração de Lisboa).

Enquanto tal não acontecer, as autoridades não poderão recorrer a metadados em investigações criminais. Porém, de acordo com uma decisão recente do Supremo Tribunal de Justiça (“STJ” ou “Supremo Tribunal de Justiça”), o acórdão do Tribunal Constitucional não afetará as decisões transitadas em julgado. Pese embora esta pareça ser uma interpretação aceitável do n.º 3 do artigo 282.º da CRP, é de lamentar que o STJ não tenha considerado a interação com o direito comunitário.

Efetivamente, a compatibilidade da Lei dos Metadados com os direitos fundamentais era, no mínimo, duvidosa desde o acórdão do TJUE no caso *Digital Rights Ireland*, em 2014. Aparentemente, o Supremo Tribunal de Justiça não se considerou destinatário do acórdão do Tribunal. Ademais, o STJ nem sequer equacionou a obrigação de submeter uma questão prejudicial ao TJUE, para efeitos do terceiro parágrafo do artigo 267.º. Este facto é motivo de grande preocupação, pois compromete a uniformidade e a eficácia da aplicação do direito comunitário em todo o território da UE. Compete aos tribunais nacionais assegurar a aplicação efetiva e uniforme do direito da União no âmbito da sua jurisdição, sendo o TJUE o garante final dessa uniformidade.

No plano da UE, os legisladores também se têm esforçado por adotar nova legislação que estabeleça um equilíbrio adequado entre o direito à privacidade e os interesses legítimos da segurança nacional e do combate à alta criminalidade. Neste contexto, a proposta de regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas (“e-Privacy Regulation”), adotada pela Comissão Europeia em 2017, reconhece a necessidade de a legislação europeia acompanhar o rápido desenvolvimento dos serviços baseados nas TI, a fim de reforçar a confiança e a segurança no mundo digital. A proposta salienta a necessidade de adaptar a legislação em matéria de privacidade eletrónica às novas regras estabelecidas no Regulamento Geral sobre a Proteção de Dados (“RGPD”), incluindo regras para todas as comunicações eletrónicas e, mais especificamente, garantias de privacidade tanto para o conteúdo como para os metadados das comunicações. De certa forma, a proposta de regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas parece fazer parte da resposta da Comissão Europeia à questão no seu conjunto, com o objetivo de resolver a falta de uniformidade e a confusão entre os legisladores nacionais.

Com efeito, desde o acórdão *Digital Rights Ireland*, e na falta de uma resposta imediata do legislador da UE, alguns Estados-Membros introduziram novas disposições para regular a utilização de metadados para fins de investigação criminal. Todavia, as abordagens adotadas variam muito, com alguns Estados-Membros a permitirem a utilização de metadados com poucas restrições, enquanto outros têm regras mais rigorosas. Algumas destas regras foram contestadas com êxito nos tribunais nacionais (ver, por exemplo,

“Polish government working on controversial surveillance bill” e “Intelligence law: what metadata can tell about you”).

Em conclusão, na sequência do caso Digital Rights Ireland, o legislador português deveria ter alterado a lei para responder às preocupações levantadas pelo TJUE. Para além disso, os tribunais nacionais deveriam ter revogado as disposições da lei portuguesa que suscitavam questões semelhantes às identificadas pelo Tribunal, sem esperar pela intervenção do Tribunal Constitucional. Em caso de dúvida, é imperativo submeter o caso a uma decisão prejudicial para que os tribunais nacionais possam cumprir as suas obrigações, e também para garantir que Portugal cumpre o direito da UE na sua plenitude, salvaguardando os direitos fundamentais dos cidadãos da UE.

No que diz respeito às instituições da UE, dada a falta de respostas consistentes a nível nacional e arrastando-se a discussão sobre a proposta de e-Privacy Regulation há vários anos, é urgente a adoção de legislação que regule a conservação e utilização de metadados de forma a respeitar os direitos fundamentais.