UNIVERSIDADE CATÓLICA PORTUGUESA

A Proteção de Dados Pessoais no TJ

Entre o Direito à Privacidade e a Retenção de Dados de Comunicações Eletrónicas

Miguel António Faria Mendes de Castro

Dissertação de Mestrado em Direito

Faculdade de Direito | Escola do Porto

2020

UNIVERSIDADE CATÓLICA PORTUGUESA

A Proteção de Dados Pessoais no TJ

Entre o Direito à Privacidade e a Retenção de Dados de Comunicações Eletrónicas

Miguel António Faria Mendes de Castro

Sob orientação da Professora Doutora Sofia Oliveira Pais

Dissertação de Mestrado em Direito

Faculdade de Direito | Escola do Porto

2020

When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else.

David Brin

Agradecimentos

Dedicando este espaço a todos os que me apoiaram ao longo da elaboração desta investigação, sei que as palavras de agradecimento, indubitavelmente devidas, serão sempre pequenas demais para expressar a verdadeira gratidão que sinto, mas seria impensável não tentar:

O meu primeiro agradecimento dirige-se à Professora Doutora Sofia Oliveira Pais, por me ter inspirado para a elaboração desta dissertação e por me orientar ao longo deste projeto com dedicação, disponibilidade e simpatia, partilhando generosamente a sua sabedoria e oferecendo sempre motivação.

A todos os Professores com quem me cruzei ao longo deste mestrado, dirijo o meu reconhecimento pela inspiração proporcionada ao partilharem o seu valioso conhecimento com paixão, confiança e generosidade.

Agradeço, de forma especial, à minha família, por sempre me ter apoiado e encorajado ao longo de toda a jornada – académica e pessoal – e aos meus amigos, que me relembraram, sempre que precisei, que estava no caminho certo e que os obstáculos são sempre ultrapassáveis.

Resumo

Os direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais, num mundo cada vez mais rendido à comunicação eletrónica, têm sido tema de conversa quotidiana e de intenso debate jurídico, quer a nível interno quer a nível europeu. A comunicação eletrónica tornou-se um meio prioritário, utilizado diariamente, muitas vezes sem a consciência de que os dados pessoais daí resultantes podem ser alvo de retenção.

No contexto da UE, a proteção dos dados pessoais está devidamente consagrada, enquanto direito fundamental, mas vê-se ameaçada perante o sistema de vigilância que a União criou e regulou, essencialmente com fins de prevenção e repressão criminais. Levanta-se, assim, a questão de até que ponto poderemos estar perante uma violação do direito da UE.

A complexidade e atualidade deste problema levou-nos a investigar, com base na jurisprudência do TJ, de que forma a União tem vindo a harmonizar estas duas realidades em constante confronto – a proteção dos direitos fundamentais dos cidadãos e a necessidade dos Estados de reter os seus dados de comunicação. Pretendemos, com esta investigação, clarificar os complicados contornos das vertentes em contraposição e explorar o debate em torno do caminho jurisprudencial que temos observado.

Palavras-chave: Carta dos Direitos Fundamentais da UE; Dados de Comunicação Eletrónica; Dados Pessoais; Direito à Privacidade; Jurisprudência do TJ; Proteção de Dados; Retenção de Dados.

Abstract

The fundamental rights to respect for privacy and protection of personal data, in an increasingly surrendered to electronic communication world, is a topic that has been the subject of daily dialogue and intense legal debate, both at internal and European level. Electronic communication has become a preferred medium, used daily, often without the awareness that the resulting personal data may be retained.

In the context of the EU, the protection of personal data is properly enshrined as a fundamental right, but it is threatened by the surveillance system that the Union has set up and regulated, mainly for the purposes of criminal prevention and prosecution. Therefore, the question arises as to the extent to which we may be facing a violation of EU law.

The complexity and presentness of this problem led us to investigate, based on the jurisprudence of the ECJ, how the EU has been harmonizing these two realities in constant confrontation – the protection of citizens' fundamental rights and the need for States to retain their communication data. With this investigation, we intend to clarify the complicated traits of the opposing aspects and explore the debate around the jurisprudential path that we have been observing.

Keywords: Charter of Fundamental Rights of the European Union; Data Protection; Data Retention; ECJ Case Law; Electronic Communications Data; Personal Data; Right to Privacy.

Índice

Siglas e Abreviaturas

CDFUE: Carta dos Direitos Fundamentais da União Europeia

CE: Comissão Europeia

Cfr.: Conferir

***Cit.*:** Citado(a)

E-M: Estado-Membro / Estados-Membros

***Et al.*:** E outros

***Ibid.*:** Na mesma fonte

***Id.*:** Na mesma fonte, no lugar citado

***Loc cit.*:** No lugar citado

***Op cit.*:** Obra citada

P.: Página

Pp.: Páginas

TFUE: Tratado sobre o Funcionamento da União Europeia

TJ: Tribunal de Justiça

UE: União Europeia

V.: Ver

Introdução

Os direitos fundamentais à proteção da vida privada e dos dados pessoais, num mundo cada vez mais rendido à comunicação eletrónica, têm sido tema de diálogo quotidiano e de intenso debate jurídico. A comunicação eletrónica tornou-se um meio prioritário, sendo utilizado diariamente, muitas vezes sem a consciência de que os dados pessoais daí resultantes podem ser alvo de retenção.

No contexto da UE, a proteção da vida privada e dos dados pessoais está devidamente consagrada enquanto direito fundamental, nos artigos 7.º e 8.º da CDFUE, respetivamente, mas vê-se ameaçada perante o sistema de vigilância que a União criou e regulou, essencialmente com fins de prevenção e repressão criminais, e que é levado a cabo pelos E-M. Levanta-se, assim, a questão de até que ponto poderemos estar perante uma violação da Carta por parte dos Estados.

A complexidade e atualidade desta problemática levou-nos a investigar, com base na jurisprudência do TJ, de que forma a União tem vindo a harmonizar estas duas realidades em constante confronto – a proteção dos direitos fundamentais dos cidadãos e a necessidade dos Estados de reter os seus dados de comunicação, com especial foco na verificação do *princípio da proporcionalidade* e nos conceitos de *crime grave* e de *ingerência grave* nos direitos fundamentais.

Para apresentar esta investigação, começaremos por contextualizar a matéria, expondo o caminho percorrido pela UE até ao presente, no que toca à conciliação entre a proteção e a retenção de dados pessoais, assim como o seu enquadramento jurídico, partindo depois para uma análise jurisprudencial de casos que chegaram ao TJ e que demonstram as dúvidas que se fazem sentir, neste aspeto, nos E-M.

Em síntese, pretendemos clarificar os complicados contornos das vertentes em contraposição e explorar o debate em torno do caminho jurisprudencial que temos observado, através da explanação do quadro jurídico, da jurisprudência e da doutrina relevantes.

1. O Tratamento de Dados Pessoais de Comunicações Eletrónicas na UE

A crescente utilização de meios de comunicação eletrónica trouxe consigo a crescente preocupação com a retenção dos dados pessoais aí gerados. Esta controversa retenção surge como um meio de os E-M da União garantirem uma efetiva prevenção, investigação e repressão de infrações penais, mas a que custo?

A um esforço penal que passa pela retenção dos dados pessoais gerados num novo contexto tecnológico está subjacente uma nova ameaça à privacidade dos seus utilizadores. Será a retenção de dados pessoais de comunicações eletrónicas um preço justo a pagar por uma investigação, repressão e prevenção penais mais efetivas?

Ao longo desta investigação desenvolveremos esta questão, explorando as formas como o direito da UE traça a linha entre a violação dos direitos fundamentais dos cidadãos relativos à sua privacidade e medidas que, embora constituam uma ingerência nos seus direitos fundamentais, são devidamente justificadas.

Antes de aprofundarmos mais esta questão, é importante entender em que contexto se desenvolveu a previsão legal do tratamento de dados pessoais dos cidadãos da União. Começaremos por contextualizar teoricamente este regime e, seguidamente, analisaremos os instrumentos jurídicos em causa.

1.1. Breve Contextualização

O principal alerta para a necessidade de um reforço da vigilância coletiva foi o pânico gerado pela ocorrência de ataques terroristas[1]. Depois do alarme social do ataque de 11 de setembro de 2001 às Torres Gémeas, nos Estados Unidos, o direito à proteção dos dados pessoais tornou-se vulnerável "a um grau inimaginável"[2]. No contexto europeu, pouco tempo depois, ocorreram os atentados de Madrid e de Londres, em 2004 e 2005, respetivamente, direcionando a atenção, que antes estava virada para a proteção da privacidade, para a necessidade de prevenir e punir os crimes.

Mais concretamente, e sem nos alargarmos, para já, na exposição dos instrumentos legais, num primeiro momento o tratamento de dados era regulado pelas Diretivas 95/46 e 2002/58,

[1] OUAKI, Myriam (2015). "Declaração de invalidade de uma diretiva pelo TJ: O caso da conservação de dados", in *Estudos Comemorativos dos 20 anos da Abreu Advogados* (coord.: Luís Gonçalves da Silva e Ricardo Costa), Coimbra, Almedina, pp. 615 e 616.

[2] VEDASCHI, Arianna e LUBELLO, Valerio (2015). "Data Retention and its Implications for the Fundamental Right to Privacy", in *Tilburg Law Review*, vol. 20, n.º 1, p. 15 (tradução nossa).

que previam a possibilidade de os Estados adotarem medidas restritivas da proteção de dados, com vista à realização de certos interesses fundamentais, entre os quais a prevenção e deteção criminais.

A adoção de medidas deste tipo veio exigir da União uma harmonização entre as legislações dos vários E-M, o que resultou na adoção de um novo instrumento legal – a Diretiva 2006/24[3]. Este instrumento foca-se exatamente na retenção de dados – que passa a ser exigida aos Estados[4] – e já não na sua proteção[5]. Para compreender esta novidade, é importante notar que esta Diretiva surge num ambiente de grande pressão política face à urgência da luta contra o terrorismo[6], e se era claro que o conteúdo das comunicações eletrónicas teria de permanecer privado, em respeito aos direitos fundamentais dos cidadãos, o mesmo já não era tão óbvio no que toca aos dados de tráfego e de localização[7].

Assim, nasce na União uma obrigação de retenção[8] de dados de comunicações eletrónicas pelos fornecedores de redes, criando-se um sistema de vigilância que procede a uma verdadeira retenção em massa[9] de todos os dados pessoais de tráfego e de localização de todos os utilizadores, sem necessidade de uma prévia ordem de um órgão jurisdicional. Estes dados poderão ser conservados por períodos de seis meses a dois anos desde a data de comunicação, ficando o período exato à escolha do E-M.

O novo rumo do direito da União parecia estar plenamente definido, até que em abril de 2014 o TJ atravessa o caminho declarando que a Diretiva 2006/24 foi "longe demais"[10], através

[3] OUAKI, Myriam, *op cit*., p. 616.

[4] WHITE, Matthew (2016). "Data retention and national law: whatever the CJEU rules, data retention may still survive!", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2016/03/data-retention-and-national-law.html, consultado a 18 de dezembro de 2019.

[5] VEDASCHI, Arianna e LUBELLO, Valerio, *op cit*., p. 18.

[6] NESTEROVA, Irena (2017). "Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards", in *European Society of International Law Conference Paper Series*, vol. 8, n.º 5, p. 4.

[7] Nos termos do artigo 2.º da Diretiva 2002/58 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, *dados de tráfego* são "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas" e *dados de localização* são "quaisquer dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas publicamente disponível".

[8] Note-se que falamos de *retenção* de dados e não de *preservação* de dados, que ocorre quando um órgão jurisdicional requere a um fornecedor de serviço de comunicação que preserve os dados relativos a determinado cidadão suspeito de atividade criminosa no âmbito de uma investigação. Cfr. GUILD, Elspeth e CARRERA, Sergio (2014). "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", in *CEPS Paper in Liberty and Security in Europe*, n.º 65, maio, p. 2.

[9] Para uma análise mais detalhada do fenómeno da retenção em massa de dados pessoais na UE, v. BIGO, Didier, *et al.* (2013). "Mass Surveillance of Personal Data by EU Member States and its compatibility with EU Law", in *CEPS Paper in Liberty and Security in Europe*, n.º 62, novembro.

[10] WHITE, Matthew (2016), *cit.* (tradução nossa).

de uma decisão prejudicial. Abre-se, assim, a "caixa de Pandora" de questões acerca do alcance do sistema de vigilância da União e da sua compatibilidade com a proteção dos direitos fundamentais, protagonizando o TJ o papel de orientador dos Estados nesta difícil conciliação.

1.2. Quadro Jurídico

A entrada em vigor do Tratado de Lisboa, em dezembro de 2009, foi especialmente importante para a proteção de dados essencialmente por dois motivos: esta proteção passou a estar prevista pelo **TFUE**[11] – o número 1 do artigo 16.º do Tratado afirma que "[todas] as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" – e a **CDFUE** tornou-se obrigatória e parte do ordenamento jurídico da União de tal forma que apesar de "formalmente não fazer parte dos Tratados, tem o mesmo valor daqueles"[12].

A Carta reveste especial importância no que toca à proteção de dados pessoais pois prevê no seu artigo 7.º o *respeito pela vida privada e familiar* e no seu artigo 8.º a *proteção de dados pessoais*. Analisando sumariamente estes dois artigos, no que toca ao primeiro, é referido que "[todas] as pessoas têm direito ao respeito […] pelas suas comunicações". Como observa Cristina Máximo dos Santos, os direitos que este artigo garante são os mesmos a que se refere o artigo 8.º da Convenção Europeia dos Direitos do Homem, mas a expressão "correspondência" foi substituída por "comunicações", o que já demonstra a atenção à evolução tecnológica[13]. Quanto ao segundo, o seu número 2 menciona que os dados pessoais "devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei".

No que toca ao campo de aplicação da Carta, o número 1 do artigo 51.º prevê que as suas disposições terão como destinatários os E-M "apenas quando apliquem o direito da União" e o artigo 52.º limita o âmbito dos direitos previstos, prevendo a possibilidade da sua restrição, desde que respeite o seu conteúdo essencial e esteja prevista por lei. As restrições terão de observar o princípio da proporcionalidade e, dessa forma, "só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União", como refere o número 1. Concretizando com base na jurisprudência do TJ, terá de ser

[11] TEIXEIRA, Maria Leonor da Silva (2013). "A União Europeia e a Proteção de Dados Pessoais – «Uma visão futurista»", in *Revista do Ministério Público*, n.º 135, p. 78.

[12] PAIS, Sofia Oliveira (2012). *Estudos de Direito da União Europeia*, Coimbra, Almedina, p. 121.

[13] SANTOS, Cristina Máximo dos (2004). "As novas tecnologias da informação e o sigilo das telecomunicações" in *Revista do Ministério Público*, n.º 99, p. 90.

feita uma ponderação entre meios e fins que indique que as medidas em causa são razoáveis e, além de aptas a concretizar o objetivo em causa, não ultrapassam essa concretização[14].

A primeira Diretiva a regular o tratamento de dados pessoais foi a **Diretiva 95/46 (Diretiva dos Dados Pessoais)**[15] que, mais especificamente, regulava a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[16], devendo-se entender por *tratamento de dados pessoais* "qualquer operação ou conjunto de operações" que tenha por objeto "qualquer informação relativa a uma pessoa singular identificada ou identificável"[17].

A aplicação desta Diretiva não se verificava face ao tratamento de dados que tivesse como objeto "a segurança pública, a defesa, a segurança do Estado […] e as atividades do Estado no domínio do direito penal"[18] e estavam previstos objetivos que justificariam medidas dos Estados restritivas do alcance deste instrumento, entre os quais a segurança estadual, a defesa, segurança pública e a prevenção, investigação, deteção e repressão de infrações penais[19].

O artigo 4.º previa situações em que os E-M deveriam aplicar as disposições nacionais resultantes da transposição desta Diretiva. Neste âmbito, a CE notou que havia diferenças significativas entre as várias disposições nacionais adotadas, sacrificando o objetivo visado[20]. Assim, a Diretiva acabou por não conseguir evitar a "fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares" devido à falta de consistência na sua execução e aplicação[21], tendo a União optado por criar um Regulamento em sua substituição – o **Regulamento 2016/679 (Regulamento Geral sobre a Proteção de Dados)**[22]**.**

[14] SILVEIRA, Alessandra (2013). "Artigo 52.º - Âmbito e Interpretação dos Direitos e dos Princípios" in *Carta dos direitos fundamentais da UE: comentada* (coord.: Alessandra Silveira e Mariana Canotilho), Coimbra, Almedina, p. 605.

[15] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[16] Cfr. artigo 1.º da Diretiva *cit.*

[17] *Ibid.,* artigo 2.º

[18] *Ibid.,* artigo 3.º, número 2, primeiro travessão.

[19] *Ibid.,* artigo 13.º

[20] WONG, Rebecca (2012). "The Data Protection Directive 95/46/EC: Idealisms and Realisms", in *International Review of Law Computers & Technology*, vol. 26, n.º 2, p. 238.

[21] Considerando 9 do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[22] Regulamento (UE) 2016/679, *cit*.

Uma novidade deste instrumento é a adição de novos elementos identificadores da pessoa singular – além do número de identificação são ainda referidos, a título de exemplo, dados de localização e identificadores por via eletrónica[23]. Esta novidade evidencia o caráter extremamente mutável do conceito de *dados pessoais*, dada a rápida e incessante evolução tecnológica, e a exigência de "aperfeiçoamentos cirúrgicos pontuais", nas palavras de Menezes Cordeiro[24].

No que toca ao âmbito de aplicação, está excluído o tratamento "para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais"[25] e, territorialmente, a aplicação restringe-se ao tratamento de dados pessoais de titulares que estejam no território da União, nos termos do n.º 2 do artigo 3.º [26].

É importante notar que o considerando 4 refere que o "direito à proteção de dados pessoais não é absoluto", devendo ser "equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade".

No âmbito mais específico do sector das comunicações eletrónicas, o tratamento de dados pessoais é regulado pela **Diretiva 2002/58 (Diretiva E-privacy)**[27]. A regulação oferecida por este instrumento visa "impedir o acesso não autorizado às comunicações"[28], tendo os E-M de garantir "a confidencialidade das comunicações e respetivos dados de tráfego"[29].

Quanto ao âmbito de aplicação, mais uma vez, o tratamento feito no âmbito de "atividades relacionadas com a segurança pública, a defesa, a segurança do Estado (…) e as atividades do Estado em matéria de direito penal" vê-se excluído[30].

---

[23] Cfr. artigo 4.º, n.º 1 do Regulamento *cit.*

[24] CORDEIRO, A. Barreto Menezes (2018). *Dados Pessoais: Conceito, extensão e limites*, Centro de Investigação de Direito Privado, Universidade de Lisboa, disponível em https://blook.pt/publications/publication/e38a9928dbce/, consultado a 11 de fevereiro de 2020, p. 2.

[25] Cfr. artigo 2.º, alínea d) do Regulamento *cit.*

[26] A versão portuguesa do Regulamento refere que este se aplica "ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento […]" no entanto a expressão "residentes" resulta de um erro de tradução, como se observa pela leitura das outras versões do Regulamento. Na versão inglesa podemos ler que o Regulamento se aplica ao tratamento "of personal data of data subjects who are in the Union […]", não fazendo qualquer referência à residência. Assim, a tradução correta seria "O presente regulamento aplica-se ao tratamento de dados pessoais de titulares que estão no território da União […]".

[27] Esta Diretiva, *cit.*, foi já alvo de alterações em duas ocasiões – em 2006, através da Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março; e em 2009, através da Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro. Esta última alterou a *Diretiva E-Privacy* enquanto parte do quadro regulamentar das redes e serviços de comunicações eletrónicas, cuja aplicação "está sujeita a revisão periódica pela Comissão, com vista, em especial, a determinar a eventual necessidade de alteração à luz da evolução tecnológica e do mercado" (cfr. considerando 1).

[28] Cfr. considerando 21 da Diretiva 2002/58, *cit*.

[29] *Ibid.,* artigo 5.º

[30] *Ibid.,* artigo 3.º, número 1.

O artigo 15.º, que apresenta um conteúdo semelhante ao artigo 13.º da *Diretiva dos Dados Pessoais*, prevê no seu n.º 1 objetivos que possibilitam a adoção de medidas nacionais que se traduzem numa restrição da confidencialidade das comunicações – entre eles, a prevenção, investigação, deteção e repressão de infrações penais. A possibilidade de adoção de uma medida deste tipo é apresentada "em termos um tanto vagos"[31]: esta terá de ser "necessária, adequada e proporcionadas numa sociedade democrática". Terá também de ser conforme com os princípios gerais do direito europeu, pelo que esta disposição deverá ser lida à luz dos artigos 7.º e 8.º da CDFUE, uma vez que possibilita ingerências nos direitos fundamentais aí consagrados – respeito pela vida privada e proteção dos dados pessoais, respetivamente.

Esta Diretiva poderá vir a ser revogada brevemente, tendo a CE já apresentado, em janeiro de 2017, uma **Proposta de Regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas**[32]. Esta proposta mantém "o essencial do artigo 15.º da Diretiva Privacidade e Comunicações Eletrónicas"[33] dando aos E-M a liberdade de regular a matéria, desde que o façam de acordo com o direito da UE. Além disso, o artigo 11.º permite aos Estados uma restrição do princípio da confidencialidade desde que, como refere no número 1, "tal restrição respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária, adequada e proporcionada". Como refere Matthew White, esta restrição poderá ser através da retenção dos dados de comunicação e seu fornecimento a autoridades[34].

Ainda no âmbito dos serviços de comunicação eletrónica, é importante recuar no tempo e mencionar a "controversa"[35] **Diretiva 2006/24 (Diretiva da Conservação de Dados)**[36], à qual a doutrina se refere como como um dos passos "mais contundentes"[37] por parte do legislador europeu.

[31] LÓPEZ-LAPUENTE, Leticia (2008). "La conservación de los datos por los operadores de servicios de comunicaciones electrónicas", in *Actualidad Jurídica - Uría Menéndez*, n.º 19, janeiro-abril, p. 73.

[32] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58 (COM/2017/010 final - 2017/03 (COD)).

[33] Cfr. parágrafo 1.3.

[34] WHITE, Matthew (2017). "A Threat to Human Rights? The new e-Privacy Regulation and some thoughts on Tele2 and Watson", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2017/01/a-threat-to-human-rights-new-e-privacy.html, consultado a 03 de dezembro de 2019.

[35] VEDASCHI, Arianna e LUBELLO, Valerio, *op cit*., p. 14 (tradução nossa).

[36] Diretiva 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, e que altera a Diretiva 2002/58/CE.

[37] LÓPEZ-LAPUENTE, Leticia, *op cit*., p. 72 (tradução nossa).

Como relembram os seus considerandos 10 e 11, o Conselho reafirmou, na sua condenação aos ataques terroristas de 2005 em Londres, a necessidade de aprovar "medidas comuns relativas à conservação de dados de telecomunicações" dada a sua importância para a investigação, deteção e repressão de infrações penais. Esta conservação não abrangia o conteúdo da comunicação[38] portanto foi vista como respeitadora dos direitos fundamentais ao respeito pela vida privada e à proteção de dados pessoais, consagrados na CDFUE[39]. Sendo esta Diretiva anterior à entrada em vigor do Tratado de Lisboa, que concedeu força vinculativa à Carta no direito da UE, esta é a única referência que lhe é feita[40].

Sendo a principal motivação deste instrumento a harmonização das legislações dos E-M para garantir a disponibilidade dos dados para efeitos penais[41], pode-se argumentar que as garantias de proteção dos direitos fundamentais dos cidadãos passaram para segundo plano, o que suscitou "as mais veementes críticas por parte dos [seus] defensores"[42]. A polémica continuou na fase de transposição nos diversos Estados[43], dificultada pelo seu "caráter invasivo da privacidade"[44] e por "suspeitas de desconformidade […] no plano constitucional" na legislação nacional daí resultante[45].

Apesar de todo o debate político que este instrumento suscitou desde o seu nascimento, foi com a entrada em vigor do Tratado de Lisboa (2009), e a força vinculativa da CDFUE daí resultante, que esta Diretiva se viu realmente ameaçada, acabando por ser invalidada, como será explorado na análise jurisprudencial.

[38] Cfr. considerando 13 da Diretiva *cit*.
[39] *Ibid.,* considerando 22.
[40] OUAKI, Myriam, *op cit*., pp. 617-619.
[41] Cfr. artigo 1.º, n.º 1 da Diretiva *cit*.
[42] OUAKI, Myriam, *op cit.*, p. 642.
[43] GUILD, Elspeth e CARRERA, Sergio, *op cit*., p. 4; e JONES, Chris (2014). "National legal challenges to the Data Retention Directive", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2014/04/national-legal-challenges-to-data.html, consultado a 12 de dezembro de 2019.
[44] NEVES, Rita Castanheira (2011). *As ingerências nas comunicações eletrónicas em processo penal: natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*, Coimbra, Coimbra Editora, p. 74.
[45] RAMALHO, David Silva e COIMBRA, José Duarte (2016). "A declaração de invalidade da Diretiva 2006/24/CE - presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", in *O Direito*, ano IV, nº 147, p. 998.

2. Análise Jurisprudencial

Feita esta contextualização, podemos avançar para uma análise mais profunda do tema central desta investigação – a contraposição entre a necessidade de garantir a proteção dos direitos fundamentais relativos à privacidade e a necessidade de reter dados pessoais de comunicações eletrónicas para efeitos penais, tendo por palco o TJ.

Para tal análise, selecionamos cinco casos – *Digital Rights Ireland e o*., *Tele2 Sverige e Watson e o*., *Ministerio Fiscal*, *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs e o*. e *Ordre des barreaux francophones e germanophone e o.* No que toca aos três primeiros, analisaremos as questões prejudiciais submetidas e a decisão prejudicial do TJ. Quanto aos dois últimos casos, ao tempo da investigação o TJ ainda não facultou a sua decisão por isso a exposição irá reservar-se às questões submetidas e opinião do advogado-geral.

Podemos desde já referir que a exposição que se segue permitirá observar que é deveras uma conciliação complexa, claramente sem uma resposta fixa, e que o juiz europeu está a percorrer um caminho a cada esclarecimento e orientação que oferece, mas os passos percorridos nem sempre se mostram pacíficos entre a doutrina.

Dos acórdãos selecionados, percebe-se que os esforços do TJ ao longo deste caminho para harmonizar estas duas necessidades levantam o véu sobre, essencialmente, três questões de relevo – qual o alcance do princípio da proporcionalidade enquanto balizador da possibilidade de retenção de dados pessoais, o que se deve entender por *ingerência grave* nos direitos fundamentais relativos à privacidade, e a quem cabe e qual o preenchimento do conceito de *crime grave*.

2.1. *Digital Rights Ireland e o.*[46]

Resumo dos Factos

A *Digital Rights Ireland* pede ao *High Court* que declare a nulidade da Diretiva 2006/24, que obriga os fornecedores de serviços de comunicações a conservarem dados de tráfego e de localização para efeitos penais.

[46] Acórdão de 8 de abril de 2014, *Digital Rights Ireland e o.* (C-293/12 e C-594/12, EU:C:2014:238).

A *High Court* suspendeu a instância e questionou o TJ acerca da proporcionalidade e adequação entre a exigência de conservação desta Diretiva e a restrição dos direitos que daí resulta – direito ao respeito pela vida privada (artigo 7.º da Carta) e direito à proteção dos dados pessoais (artigo 8.º da Carta).

Decisão do TJ

O TJ afirma que a conservação generalizada de dados e acesso aos mesmos pelas autoridades constitui uma ingerência "de grande amplitude e [que] deve ser considerada particularmente grave" [47].

Uma vez que estamos perante direitos fundamentais previstos pela Carta, o juiz europeu teve de "passar ao crivo"[48] os requisitos ditados pelo artigo 52.º, n.º 1, entre os quais o que suscita mais dúvidas, no caso, é o respeito pelo princípio da proporcionalidade, que dita que "os atos das instituições da União sejam adequados à realização dos objetivos legítimos prosseguidos pela regulamentação em causa e não excedam os limites do que é adequado e necessário à realização desses objetivos"[49].

Esta Diretiva abrange "todos os meios de comunicação eletrónica e todos os dados relativos ao tráfego", não contendo uma limitação face ao seu objetivo material de luta contra a criminalidade grave, e afeta "todas as pessoas que utilizam serviços de comunicações eletrónicas" não se limitando a quem está "numa situação suscetível de dar lugar a ações penais"[50]. Além disso, o número de pessoas com autorização de acesso aos dados conservados e a duração temporal de conservação dos dados não se apresentam balizados por critérios objetivos que garantam o limite do estritamente necessário[51].

Após a enumeração de vários pontos criticáveis, o TJ conclui que a Diretiva 2006/24 é inválida[52] por desrespeitar o princípio da proporcionalidade nas ingerências que faz nos direitos ao respeito pela vida privada e à proteção dos dados pessoais.

[47] Cfr. parágrafo 37 do acórdão *cit.*
[48] OUAKI, Myriam, *op cit*., p. 620.
[49] Cfr. parágrafos 45 e 46 do acórdão *cit.*
[50] *Ibid.,* parágrafos 57 e 58.
[51] *Ibid.,* parágrafos 62 e 64.
[52] É de salientar que não estamos perante uma anulação de um ato legislativo decorrente de um recurso de anulação (artigo 263.º do TFUE) mas sim uma declaração de invalidade afirmada no âmbito de um reenvio prejudicial. O Parlamento e o Conselho ficaram responsáveis por acatar a decisão tomada, optando, no caso, por anular a Diretiva. V. RAMALHO, David Silva e COIMBRA, José Duarte, *op cit.,* pp. 1018 a 1030.

Análise

Um ponto curioso em relação a esta Diretiva é que a sua base legal tinha sido alvo de debate quando, no caso *Irlanda vs. Parlamento e Conselho*[53], a Irlanda pediu ao TJ que anulasse a mesma por não ter sido adotada com fundamento numa base jurídica adequada: a base é o funcionamento do mercado interno e a Irlanda argumenta que seria a cooperação policial e judiciária em matéria penal. O TJ discorda e afirma que a base legal era a correta, tendo em conta o seu conteúdo material[54]. É importante verificar que esta decisão data de 10 de fevereiro de 2009, ou seja, é anterior à entrada em vigor do Tratado de Lisboa e, consequentemente, a Carta ainda não constituía direito primário da União, o que torna mais compreensível a decisão.

Desta vez, a Diretiva foi invalidada somente com recurso a artigos da Carta, afirmando-se, em termos práticos, o papel constitucional do TJ[55] e a utilidade de se conceder à União "o seu próprio instrumento jurídico em matéria de direitos fundamentais"[56].

Várias questões surgiram após este acórdão, essencialmente no que toca ao delineamento da fronteira entre as competências dos E-M e da UE[57]. As dúvidas foram adensadas pelo facto de a CE não ter tomado iniciativa de criar uma nova Diretiva em sua substituição, deixando a matéria de conservação de dados ao poder dos Estados, sujeita à previsão do artigo 15.º da Diretiva 2002/58[58].

Agências de segurança e serviços de inteligência receberam mal esta novidade, temendo a proibição absoluta da retenção de dados, mas houve quem alertasse, mais otimisticamente, que o cerne da questão é a necessidade de prever condições apertadas para justificar essa retenção, algo que a Diretiva em causa não previa[59].

Perante isto, haverá margem para a retenção de dados em massa? Steve Peers opina que não será possível, pois quer uma possível Diretiva substituta quer a legislação dos Estados neste

[53] Acórdão de 10 de fevereiro de 2009, Irlanda/Parlamento e Conselho (C-301/06, EU:C:2009:68).
[54] Parágrafos 84 e 85 do acórdão *cit*.
[55] VEDASCHI, Arianna e LUBELLO, Valerio, *op cit*., p. 17.
[56] OUAKI, Myriam, *op cit.*, p. 629.
[57] LYNSKEY, Orla (2013). "Plenty to retain? Opinion of the Advocate General in Joined Cases C-293/12 and 594/12, Digital Rights Ireland ltd and Seitlinger and others", in *The European Law Blog – News and Comments on EU Law*, disponível em https://europeanlawblog.eu/2013/12/17/plenty-to-retain-opinion-of-the-advocate-general-in-joined-cases-c-29312-and-59412-digital-rights-ireland-ltd-and-seitlinger-and-others/, consultado a 04 de janeiro de 2020.
[58] VERBRUGGEN, Frank, *et al.* (2018). "Reconsidering the Blanket-Data-Retention-Taboo, For Human Rights' Sake?", in *The European Law Blog – News and Comments on EU Law*, disponível em http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/, consultado a 04 de janeiro de 2020.
[59] *Id.*

domínio terão de efetuar uma especificação de comunicações particularmente ligadas a *crimes graves*, já que uma vigilância indiscriminada será sempre uma ingerência injustificável no âmbito da Carta[60]. Concordamos com esta ideia, mas a verdade é que esta dúvida continua a ecoar nos E-M (como poderemos observar na restante exposição jurisprudencial).

A definição europeia de *crime grave*, ou a sua falta, é também uma das maiores questões. A este propósito, Arianna Vedaschi e Valerio Lubello relembram que, na prática, os Estados preencheram este conceito de formas muito diversas, tendo alguns adotado listas de crimes considerados graves ao passo que outros utilizam como critério a moldura penal[61]. Esta discrepância é algo preocupante pois a gravidade do crime é um limite aos grupos de utilizadores e aos meios de comunicação passíveis de retenção, assim como ao período temporal da sua conservação.

O que observamos, no que toca à doutrina, é a defesa de uma harmonização no preenchimento deste conceito. Neste sentido, Elspeth Guild e Sergio Carrera defendem que terá de haver uma definição comum aos vários Estados[62], e Steve Peers afirma que uma nova Diretiva substituta teria de conter regras quanto a esta definição[63].

Vanessa Franssen chama a atenção para outro problema neste âmbito: um crime pode começar por ser considerado "normal" e, com o decorrer da investigação, passar a ser considerado grave por haver novas descobertas[64], o que traz dificuldades, nomeadamente, quanto ao limite temporal de conservação dos dados (à partida, mais curto, por se considerar, precipitadamente, que não se tratava de um crime grave). Esta observação revela que a gravidade de um crime é, realmente, um conceito muito relevante nesta matéria, levando à urgência de maiores esclarecimentos pelo direito da UE.

Um outro aspeto deste acórdão que merece a nossa atenção é referido por Orla Lynskey – a decisão do TJ não questiona a efetividade da retenção de dados como ferramenta de

[60] PEERS, Steve (2014). "The Domino Effect: how many EU treaties violate the rights to privacy and data protection?", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2014/11/the-domino-effect-how-many-eu-treaties.html, consultado a 21 de janeiro de 2020, e PEERS, Steve (2014). "The data retention judgment: The CJEU prohibits mass surveillance", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2014/04/the-data-retention-judgment-cjeu.html, consultado a 21 de janeiro de 2020.

[61] VEDASCHI, Arianna e LUBELLO, Valerio, *op cit*., p. 20.

[62] GUILD, Elspeth e CARRERA, Sergio, *op cit*., p. 14

[63] PEERS, Steve (2014). "The Domino Effect: how many EU treaties violate the rights to privacy and data protection?", *cit.*

[64] FRANSSEN, Vanessa (2016). "The future of national data retention obligations – How to apply Digital Rights Ireland at national level?" in *The European Law Blog – News and Comments on EU Law*, disponível em https://europeanlawblog.eu/2016/07/25/the-future-of-national-data-retention-obligations-how-to-apply-digital-rights-ireland-at-national-level, consultado a 11 de janeiro de 2020.

combate ao crime[65], referindo apenas, sucintamente, que "tendo em conta a crescente importância dos meios de comunicação eletrónica, os dados que devem ser conservados em aplicação desta diretiva […] constituem um instrumento útil nas investigações penais"[66]. Concordando com a opinião de Lynskey, consideramos que a falta de maiores considerações sobre este tema, nomeadamente com evidência empírica, revela-se algo desapontante.

Surgem também dúvidas quanto aos efeitos desta decisão em matéria de aplicabilidade das legislações nacionais de transposição[67]. Sendo as legislações adotadas com base nas medidas impostas pela Diretiva, as medidas dessas mesmas legislações terão, também elas, de ser confrontadas com a interpretação oferecida pelo TJ, pois "o conteúdo das disposições nacionais de transposição poderá ser […] contrário ao Direito da União"[68]. Não sendo possível a interpretação conforme, decorre do princípio do primado que as medidas nacionais contrárias às disposições europeias devem ser desaplicadas pelas autoridades do E-M[69]. Nas palavras de Rostane Mehdi, há uma verdadeira obrigação de "excluir as regras internas adotadas em violação da legalidade comunitária"[70].

Depois de todas estas dúvidas suscitadas pelo acórdão, um ponto positivo que podemos observar é a afirmação inequívoca de que o acesso a dados de comunicação pode consubstanciar, por si só, uma ingerência grave na vida privada do cidadão, mesmo não tendo as autoridades acesso ao conteúdo dessas comunicações[71].

2.2. *Tele2 Sverige e Watson e o*.[72]

Resumo dos Factos

A regulamentação nacional da Suécia previa uma obrigação de os prestadores de serviços

[65] LYNSKEY, Orla (2014). "Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and Others: The Good, the Bad and the Ugly", in *The European Law Blog – News and Comments on EU Law*, disponível em https://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/, consultado a 12 de dezembro de 2019.

[66] Cfr. parágrafo 49 do acórdão *cit.*

[67] RAMALHO, David Silva e COIMBRA, José Duarte, *op cit*., p. 998.

[68] *Ibid.,* p. 1031.

[69] OUAKI, Myriam, *op cit*., p. 642.

[70] MEHDI, Rostane (2007). "L'autonomie institutionnelle et procédurale et le droit administratif" in *Droit Administratif Européen* (eds.: Jean-Bernard Auby e Jacqueline Dutheil de la Rochère), Bruxelas, Bruylant, p. 709 (tradução nossa).

[71] GUILD, Elspeth e CARRERA, Sergio, *op cit*., pp. 5 e 6.

[72] Acórdão de 21 de dezembro de 2016, *Tele2 Sverige e Watson e o.* (C-203/15 e C-698/15, EU:C:2016:970).

de comunicações eletrónicas conservarem certos dados pessoais pelo período de seis meses contados a partir do fim da comunicação, podendo ser fornecidos às autoridades nacionais se tal se revelasse necessário "para prevenir, impedir ou constatar uma atividade criminosa"[73].

A entidade prestadora de serviços de comunicação eletrónica Tele2 Sverige, estabelecida na Suécia, notificou a autoridade sueca de supervisão de telecomunicações Post- och telestyrelsen (PTS) de que não iria continuar a reter dados de comunicação, na sequência da decisão do TJ no acórdão *Digital Rights Ireland*. A Direção Geral da Polícia Nacional apresentou queixa à PTS "pelo facto de a Tele2 Sverige ter deixado de lhe comunicar os dados"[74], o que levou a que a PTS ordenasse à Tele2 que, em conformidade com a lei nacional, procedesse à sua retenção.

O órgão jurisdicional de reenvio observa que o artigo 15.º, n.º 1 da Diretiva 2002/58 possibilita, em determinadas circunstâncias, a retenção dos dados de comunicações eletrónicas, mas neste caso temos uma obrigação generalizada de conservação, o que suscita dúvidas. Face a isto, questiona se será compatível com o artigo "uma obrigação geral de conservar dados de tráfego […] sem quaisquer distinções, limitações ou exceções, para efeitos do objetivo de combate à criminalidade"[75].

Decisão do TJ

O TJ refere a importância, expressa pelo número 1 do artigo 52.º da Carta, de uma restrição ao exercício dos direitos e liberdades fundamentais estar "prevista por lei e respeitar o seu conteúdo essencial" e de respeitar o princípio da proporcionalidade, que implica que "as derrogações e as limitações à proteção dos dados pessoais operem na estrita medida do necessário"[76].

Uma vez que a regulamentação nacional em causa "prevê uma conservação generalizada e indiferenciada" que abrange os dados de comunicação de "todos os assinantes e utilizadores registados relativos a todos os meios de comunicação eletrónica", o TJ considera que há uma suscetibilidade de "tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados"[77].

Assim, estamos perante uma ingerência muito ampla e que deve ser considerada

[73] Cfr. parágrafo 22 do acórdão *cit.*
[74] *Ibid.,* parágrafo 45.
[75] *Ibid.,* parágrafos 49 a 51.
[76] *Ibid.,* parágrafo 96.
[77] *Ibid.,* parágrafo 99.

"particularmente grave", pelo que para efeitos de luta contra a criminalidade "só a luta contra a criminalidade grave pode justificar uma medida deste tipo"[78].

Concluindo, esta regulamentação "excede os limites do estritamente necessário e não pode ser considerada justificada"[79], portanto deve ser considerada incompatível com o direito da UE.

Análise

Após as dúvidas levantadas pelo caso *Digital Rights Ireland*, era uma questão de tempo até os juízes dos E-M começarem a submeter pedidos de decisão prejudicial[80]. Se é verdade que com esta decisão o TJ veio esclarecer pontos importantes na saga da retenção de dados, também é verdade que este "está longe de ser o capítulo final"[81].

Como anteriormente referido, algumas interpretações apontavam no sentido de a retenção de dados ser permitida desde que obedecendo a critérios mais restritivos. Com esta decisão, fica mais claro que é essa a interpretação do TJ. Esses critérios passam pela especificação das pessoas abrangidas em função dos crimes que levaram à adoção de medidas nacionais que restrinjam o princípio da confidencialidade, limitadas ao estritamente necessário[82].

No que toca à retenção de dados em massa, há uma verdadeira "rutura com o passado"[83], pois o TJ clarifica, pela primeira vez, que as medidas nacionais que preveem a conservação indiscriminada de dados são excessivas[84]. Neste âmbito, Orla Lynskey acrescenta

[78] *Ibid.,* parágrafos 94 a 102.
[79] *Ibid.,* parágrafo 107.
[80] VERBRUGGEN, Frank, *et al*., *cit.*
[81] FORMICI, Giulia (2019). "ECJ, the floor is yours! The never ending story between Data Retention and Right to Privacy" in *The CiTiP Blog*, disponível em https://www.law.kuleuven.be/citip/blog/ecj-the-floor-is-yours-the-never-ending-story-between-data-retention-and-right-to-privacy/, consultado a 12 de dezembro de 2019 (tradução nossa).
[82] WOODS, Lorna (2016). "Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2016/12/data-retention-and-national-law-ecj.html, consultado a 12 de dezembro de 2019.
[83] LYNSKEY, Orla (2017). "Tele2 Sverige AB and Watson et al - Continuity and Radical Change", in *The European Law Blog – News and Comments on EU Law*, disponível em https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/, consultado a 04 de janeiro de 2020 (tradução nossa).
[84] COUDERT, Fanny (2017). "In the aftermath of Tele2 and Opinion 1/15: when are data retention measures legitimate?", in *The CiTiP Blog*, disponível em https://www.law.kuleuven.be/citip/blog/in-the-aftermath-of-tele2-and-opinion-115-when-are-data-retention-measures-legitimate/, consultado a 4 de janeiro de 2020.

que, no Reino Unido, é de lamentar que esta decisão tenha chegado "demasiado tarde"[85] pois não impediu a entrada em vigor do *Investigatory Powers Act 2016*, que será posteriormente analisado a propósito do acórdão *Ministerio Fiscal*.

Nas suas conclusões, o advogado-geral Saugmandsgaard Øe, tinha oferecido uma interpretação ligeiramente diferente, apontando para a possível justificação de uma retenção indiscriminada de dados. Segundo o advogado-geral, a retenção em massa poderia ser considerada compatível com o direito da União, mas apenas se respeitasse "simultaneamente as exigências estabelecidas no artigo 15.º, n.º 1, da Diretiva 2002/58 e as exigências previstas no artigo 52.º, n.º 1, da Carta"[86].

Voltando ao problema da aplicabilidade das legislações nacionais resultantes da transposição da Diretiva 2006/24, numa carta aberta[87] dirigida à CE, de 25 de junho de 2018, assinada por "sessenta e duas organizações, redes comunitárias e professores académicos, em dezanove Estados", é referido que esta decisão reitera o que foi afirmado no caso *Digital Rights*, desta vez especificamente em relação a legislação nacional, portanto, face à primazia do direito da União, todas as legislações nacionais que prevejam uma retenção em massa de dados pessoais de comunicação deveriam ser consideradas incompatíveis com o direito da UE, no entanto "pelo menos 17" E-M ainda implementam esta retenção.

2.3. *Ministerio Fiscal* [88]

Resumo dos Factos

Em fevereiro de 2015, Hernandez Sierra, cidadão espanhol, é vítima de um assalto violento, em Espanha, no qual lhe é roubado o telemóvel. Na sequência deste assalto, é apresentada queixa à polícia.

Com o objetivo de identificar os suspeitos do crime para fins de inquérito penal, a polícia judiciária pretende obter acesso a dados pessoais na posse dos operadores de telefonia móvel – especificamente, os números de telemóvel ativados com o código IMEI do telemóvel roubado, num período de doze dias após o assalto, e, posteriormente, os dados pessoais

[85] LYNSKEY, Orla (2017), *cit.* (tradução nossa).

[86] Cfr. parágrafo 131 das conclusões do advogado-geral Henrik Saugmandsgaard Øe de 19 de julho de 2016 (C 203/15 e C 698/15, EU:C:2016:572).

[87] Carta disponível em https://www.hermescenter.org/wp-content/uploads/2018/06/STOPdataRetention-Open-Letter.pdf (tradução nossa).

[88] Acórdão de 2 de outubro de 2018 (C-207/16, EU:C:2018:788).

relativos à identidade (nome e, se necessário, endereço postal) de quem estiver registado como titular desses cartões.

Nos termos do Código de Processo Penal Espanhol, é ao juiz que cabe autorizar a interceção e análise de correspondência telegráfica, se tal for pertinente para o processo[89]. A polícia judiciária pede ao juiz de instrução criminal que ordene aos fornecedores de serviços de comunicações eletrónicas que cedam esses dados mas o pedido é indeferido. O juiz entende que esse acesso consubstancia uma ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da CDFUE e, nos termos da lei nacional espanhola – Lei n.º 25/2007[90] – para se considerar justificada, o crime em causa terá de ser grave, que não é o caso.

Segundo o Código Penal Espanhol, a determinação da gravidade de um crime é feita através de um critério normativo formal, em que se considera a pena suscetível de ser aplicada. Assim, serão graves as infrações que a lei pune com pena grave, e penas graves são pena de prisão perpétua ou pena de prisão superior a 5 anos[91]. O crime em causa tem a previsão de pena máxima de 3 anos de prisão, logo não é considerado grave, portanto não haverá justificação para uma intromissão na vida privada dos suspeitos.

Após este indeferimento, entrou em vigor a Lei 13/2015[92], que alterou o Código de Processo Penal Espanhol, introduzindo um novo critério de determinação da gravidade de uma infração – o critério material – que considera a gravidade da ofensa aos bens jurídicos da comunidade em que se traduz o comportamento em causa.

Perante isto, o *Ministerio Fiscal* interpõe recurso do despacho de indeferimento, alegando que a comunicação dos dados em causa deveria ter sido autorizada em razão da natureza do assalto. Neste contexto, o tribunal ordena a prorrogação do prazo de conservação dos dados de comunicação pelos serviços de telefonia e suspende a instância.

O órgão jurisdicional entende que o caso cai no âmbito de aplicação da Diretiva 2002/58 e submete duas questões prejudiciais ao TJ: é questionado se a gravidade do crime, "enquanto critério que justifica a ingerência nos direitos fundamentais", poderá ser determinada apenas com base na pena suscetível de ser aplicada ou se será "necessário identificar na conduta infratora especiais níveis de lesão de bens jurídicos". A título subsidiário, questiona qual o

[89] Cfr. artigo 579º, número 1 do Código de Processo Penal Espanhol.

[90] Lei relativa à conservação de dados relativos a comunicações eletrónicas e a redes públicas de comunicações, de 18 de outubro de 2007 (BOE nº 251, de 19 de outubro de 2007, p. 42517).

[91] Cfr. artigos 13.º, número 1 e artigo 33.º do Código Penal Espanhol.

[92] Lei Orgânica de modificação da Lei de Acusação Criminal para fortalecimento das garantias processuais e regulação das medidas de investigação tecnológica de 5 de outubro de 2015 (BOE n.o 239, de 6 de outubro de 2015, p. 90192).

"limiar mínimo" da pena aplicável, para se considerar a infração grave, e se um limite de três anos seria compatível com o direito da UE[93].

Decisão do TJ

Antes da decisão referente às questões prejudiciais submetidas, o TJ tece considerações acerca da sua competência para as responder. O Governo espanhol alega que o TJ não tem essa competência pois estamos perante matéria excluída do âmbito de aplicação do direito da União, já que, em conformidade com o artigo 1.º, n.º 3, da Diretiva 2002/58, as atividades do Estado em certos domínios, como o penal e da segurança pública, estão excluídas do âmbito de aplicação da Diretiva, e a Carta também não tem aplicação no caso, em conformidade com o seu artigo 51.º, n.º 1, que dita que os E-M são destinatários das suas disposições somente quando aplicam o direito da UE[94].

O TJ entende que, em primeiro lugar, a Diretiva é aplicável ao tratamento de dados pessoais no contexto do fornecimento de serviços de comunicações eletrónicas (artigo 3.º) e, em segundo, as medidas legislativas referidas no artigo 15.º, n.º 1, "estão abrangidas pelo âmbito de aplicação desta diretiva, mesmo que digam respeito a atividades próprias do Estado ou das autoridades estatais"[95]. Além disso, se a medidas em causa impõem retenção de dados pessoais, implicam que os fornecedores de serviços façam um tratamento desses dados e, desta forma, tais medidas "não podem ser equiparadas às atividades próprias dos Estados"[96]. Assim, não há nada a ditar a inaplicabilidade da Diretiva ao caso e o TJ é competente para responder ao pedido de decisão prejudicial.

O Tribunal vai mais longe e esclarece que é irrelevante o facto de o pedido de acesso apenas dizer respeito à identidade dos titulares dos cartões ativados no telemóvel, porque os dados relativos à identidade estão abrangidos pelo conceito de "dados de tráfego" definido no artigo 2.º, segundo parágrafo, alínea b), da Diretiva 2002/58[97].

Voltando às questões prejudiciais, podemos constatar que o órgão de reenvio pressupõe a autonomização a nível de direito da União do conceito de *crime grave*, e pretende saber como o aplicar corretamente. O TJ, em concordância com a opinião do advogado-geral

[93] Cfr. parágrafo 26 do acórdão *cit*.
[94] *Ibid.,* parágrafo 29.
[95] *Ibid.,* parágrafo 34.
[96] *Ibid.,* parágrafo 37.
[97] *Ibid.,* parágrafo 42.

Saugmandsgaard Øe[98], começa por reformular a questão, entendendo que o que deve ser questionado é se uma ingerência não grave nos direitos fundamentais motivada pela luta contra infrações penais só se poderá considerar justificada perante infrações graves. O núcleo do caso é a gravidade da ingerência e não a gravidade do crime[99]. A resposta à questão reformulada é negativa.

O TJ esclarece que o critério de apreciação da justificação da ingerência é o respeito pelo princípio da proporcionalidade e não, necessariamente, o caráter grave da infração penal, e chama a atenção para o facto de o artigo 15.º da Diretiva 2002/58 compreender uma lista exaustiva de objetivos que possam justificar uma derrogação do princípio da confidencialidade das comunicações, como resulta da expressão "pelas razões enunciadas" do segundo período do n.º 1[100]. Quanto ao objetivo aqui prosseguido, só está prevista na Diretiva a "prevenção, investigação, deteção e repressão de infração penal" e não a sua gravidade.

No caso *Tele2*, diferentemente, os dados conservados possibilitam conhecer "a origem de uma comunicação e o seu destino, […] a data, a hora, a duração e o tipo de uma comunicação", portanto fornecem muitas informações sobre a vida privada da pessoa em causa[101]. Estamos perante uma ingerência grave nos direitos fundamentais que, em respeito pelo princípio da proporcionalidade, só seria suscetível de ser justificada perante a luta contra um crime grave.

No caso em análise, o pedido da polícia judiciária é bastante limitado, uma vez que apenas compreende um período temporal de doze dias, um meio de comunicação específico (o telemóvel roubado) e os dados de identidade, além de que as pessoas afetadas têm a característica especial de serem suspeitas de um crime. Assim, não haverá acesso às datas e horas de comunicação, à duração das chamadas ou seus destinatários, nem à sua localização ou frequência, portanto não são especialmente invasivas da vida privada das pessoas, logo não estamos perante uma ingerência grave.

Sintetizando, a justificação para uma ingerência não grave nos direitos fundamentais não exige a verificação de um crime grave.

---

[98] Cfr. parágrafo 73 das conclusões do advogado-geral Henrik Saugmandsgaard Øe de 3 de maio de 2018 (C-207/16, EU:C:2018:300).

[99] ARTEMIOU, Eleni (2018). "The way out of Digital Rights Ireland", in *The CiTiP Blog*, disponível em https://www.law.kuleuven.be/citip/blog/the-way-out-of-digital-rights-ireland/, consultado a 4 de fevereiro de 2020.

[100] Cfr. parágrafo 90 do acórdão *cit.*

[101] Cfr. parágrafos 98 e 99 do acórdão *Tele2*, *cit.*

Análise

No que toca à competência do TJ para responder nesta matéria, que foi esclarecida com este acórdão, é importante fazer uma breve referência ao caso *Liberty c. Secretary of State for the Home Department e o*.[102]. Em traços gerais, *Liberty* – uma organização independente defensora dos direitos humanos – questionou a compatibilidade da *Parte 4* do *Investigatory Powers Act 2016* do Reino Unido com o direito da UE, já que esta lei atribui ao Secretário de Estado o poder de ordenar a retenção de dados pessoais às entidades fornecedoras de serviços de telecomunicações, se considerar essa retenção necessária e proporcional face à salvaguarda da segurança nacional, da deteção e prevenção de crimes e da segurança pública, entre outros objetivos listados na lei. O Supremo Tribunal do Reino Unido entendeu que a disposição é incompatível com o direito da UE na medida em que restringe os direitos fundamentais dos cidadãos sem prever uma limitação ao propósito de luta contra crimes graves nem submeter o acesso aos dados conservados a fiscalização por uma entidade independente, portanto a legislação terá de ser alterada[103].

Esta decisão parece-nos criticável no que toca ao âmbito mais específico dos dados de entidade, previstos na lei. A lei prevê que os dados de comunicação que poderão ser conservados compreendem dados de eventos e dados de entidade. O tribunal entende que os dados de eventos caem no campo de aplicação da Diretiva 2002/58, mas os dados de entidade, em relação aos quais refere como exemplo "o nome de uma pessoa na posse de um determinado telemóvel"[104] já não estarão dentro do seu âmbito de aplicação, portanto recusa submeter um pedido de decisão prejudicial quanto a esta matéria. Como tivemos a oportunidade de expor, o TJ afirmou, em *Ministerio Fiscal*, que a Diretiva se aplica a este tipo de dados (os mesmos que a polícia judiciária pretende obter nesse caso). A decisão parece, então, ter chegado tarde demais, pois o tribunal do Reino Unido assumiu como externa ao direito da União uma matéria em que o TJ afirmou a sua jurisdição.

No que toca às questões prejudiciais respondidas, ao contornar a questão referente ao caráter grave de uma infração, o TJ "foge" ao debate acerca da existência de um conceito

[102] Decisão do Supremo Tribunal do Reino Unido *Liberty c. Secretary of State for the Home Department e o.* [EWHC 975 (Admin)], disponível em http://www.bailii.org/ew/cases/EWHC/Admin/2018/975.html, consultado a 03 de janeiro de 2020.

[103] Para uma análise mais aprofundada a este acórdão, v. WHITE, Matthew (2018). "Data Retention incompatible with EU law: Victory? Victory you say?", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2018/05/data-retention-incompatible-with-eu-law.html, consultado a 20 de outubro de 2019.

[104] Cfr. parágrafo 145 do acórdão *Liberty c. Secretary of State for the Home Department e o., cit.*

europeu autónomo de *crime grave*, o que na opinião de Lorna Woods é uma resposta "tática"[105], mas parece-nos que esta fuga foi um adiamento do inadiável pois, na nossa opinião, futuras questões prejudiciais neste sentido irão exigir um esclarecimento inequívoco do juiz europeu.

Por outro lado, houve uma oportunidade claramente aproveitada nesta decisão – a afirmação clara de que as autoridades nacionais continuam a ter poder para tratar dados de comunicação para efeitos de investigação penal, numa altura em que, como refere Eleni Artemiou, tal começava a parecer impossível dada a crescente preocupação do juiz europeu com a proteção de dados pessoais dos cidadãos[106].

2.4. *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs e o.*

Resumo dos Factos

Neste caso, o *Investigatory Powers Tribunal* do Reino Unido pretende saber se a legislação nacional que prevê a obtenção de dados de comunicação em massa por agências de segurança e serviços de inteligência do Estado, fornecidos por serviços de comunicação eletrónica, é compatível com o direito da UE[107].

Mais concretamente, o órgão jurisdicional questiona o TJ se, com base no artigo 4.º do Tratado da União Europeia (TUE) e no artigo 1.º, n.º 3, da Diretiva 2002/58, uma imposição de fornecimento destes dados às entidades em causa se enquadra no âmbito de aplicação do direito da União e da Diretiva 2002/58[108].

[105] WOODS, Lorna (2018). "Mobile phone theft and EU eprivacy law: the CJEU clarifies police powers*"*, in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2018/10/mobile-phone-theft-and-eu-eprivacy-law.html, consultado a 5 de janeiro de 2020 (tradução nossa).

[106] ARTEMIOU, Eleni, *cit.*

[107] Decisão do *Investigatory Powers Tribunal* de 8 de setembro de 2017, disponível em http://shorturl.at/CHJ45, consultado a 09 de janeiro de 2019.

[108] Pedido de decisão prejudicial de 31 de outubro de 2017 (C-623/17).

Análise

O tribunal refere que o litígio contrapõe a proteção da população nacional pelas entidades de segurança à proteção de privacidade do indivíduo[109]. Tal como afirma Matthew White[110], entendemos ser uma afirmação falaciosa porque a retenção dos dados de comunicação não é feita de forma individualizada, isto é, há uma retenção em massa. A forma como o tribunal expõe o litígio dá a entender que só os indivíduos que representem uma ameaça ao Estado terão os seus dados conservados, o que seria mais fácil de justificar, mas não é a realidade do caso.

O advogado-geral Sánchez Bordona defende que o artigo 15.º, n.º 1, da Diretiva não permite que a transmissão de dados pelos operadores de serviços de comunicação seja excluída do âmbito do direito da União, já que a retenção e posterior transmissão constituem tratamento de dados pessoais de comunicação "pelo que estão evidentemente abrangidas pelo âmbito de aplicação da Diretiva" independentemente de haver razões de segurança nacional a motivar este tratamento[111]. Concluindo, o artigo 1.º, n.º 3 da Diretiva opõe-se à legislação nacional em causa[112].

Este processo continua pendente e será interessante verificar a decisão tomada porque se o TJ continuar a seguir o caminho que tem seguido com a jurisprudência aqui exposta, colocará o cerne da questão no respeito pelo princípio da proporcionalidade e, assim, a previsão de retenção de dados de comunicação terá de conter limites que a circunscrevam ao necessário para atingir o objetivo de proteção da população nacional. Quanto ao que cabe no conceito de "necessário", o rumo que tem vindo a ser traçado não aceita que nele se inclua a retenção de dados em massa, mas os juízes nacionais, por sua vez, entendem que essa retenção é "essencial para a proteção da segurança nacional do Reino Unido, nomeadamente nos domínios do combate ao terrorismo, à espionagem e à proliferação nuclear"[113].

[109] Decisão do *Investigatory Powers Tribunal*, *cit*., parágrafo 6.

[110] WHITE, Matthew (2017). "The Privacy International case in the IPT: respecting the right to privacy?", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2017/09/the-privacy-international-case-in-ipt.html, consultado a 20 de dezembro de 2019.

[111] Cfr. parágrafos 30 e 31 da versão provisória das conclusões do advogado-geral Sánchez Bordona de 15 de janeiro de 2020 (C-623/17, EU:C:2020:5).

[112] *Ibid.,* parágrafo 45.

[113] *Ibid.,* parágrafo 20.

2.5. *Ordre des barreaux francophones e germanophone e o.* [114]

Resumo dos Factos

Este caso foca-se na Lei de 29 de maio de 2016, lei belga relativa à recolha e à conservação de dados no setor das comunicações eletrónicas, que levanta suspeitas de desconformidade com o direito europeu, por prever uma obrigação geral de os operadores procederem a uma conservação generalizada de dados de comunicação para propósitos como luta contra crimes graves, segurança nacional, investigação criminal e identificação de suspeitos de abuso sexual de crianças que usam meios eletrónicos.

O Tribunal Constitucional Belga submeteu ao TJ um pedido de decisão prejudicial questionando se o artigo 15.º, n.º 1, da Diretiva 2002/58 se opõe a uma regulamentação nacional deste tipo.

Este pedido surge do conflito entre duas interpretações distintas do acórdão *Tele2*[115]:

Quem entende que a lei é incompatível com o direito da União argumenta que o acórdão *Tele2* clarificou que a retenção de dados em massa será sempre uma violação do princípio da proporcionalidade. A única forma de reter dados justificadamente é fazê-lo somente em relação a determinados grupos. Além disso, o artigo 15.º da Diretiva 2002/58 prevê restrições ao princípio da confidencialidade como exceções. Se a retenção em massa for permitida, a exceção torna-se a regra.

Por outro lado, o Governo Belga faz uma interpretação diferente, entendendo que a violação do princípio da proporcionalidade da regulamentação em causa, nesse caso, não se devia somente à retenção de dados em massa mas a vários outros fatores combinados. Na sua argumentação, refere que em muitos casos não se pode fazer uma especificação prévia do grupo de pessoas cujos dados serão necessários, e a título de exemplo temos casos de terrorismo em que será necessário analisar com quem é que o responsável comunicou; casos em que alguém é dado como desaparecido e é necessário localizar o telemóvel (pode nem estar em causa uma investigação criminal); casos em que é necessário provar o álibi de uma pessoa e a prova só pode ser feita por dados de comunicação (o que mostra que a retenção de dados pode ser útil inclusivamente para o suspeito de crime); entre outros. Isto para concluir que não se pode predeterminar que dados serão necessários, portanto não terá sentido definir grupos de pessoas

[114] Pedido de decisão prejudicial de 2 de agosto de 2018 (C-520/18).
[115] VERBRUGGEN, Frank, *et al., cit.*

cujos dados podem ser conservados. Esta definição pode até ser discriminatória. Assim, todos os dados devem ser conservados mas apenas alguns poderão ser usados, mediante garantias legais estreitas[116].

Análise

Como observamos, este caso é muito demonstrativo do debate que se tem gerado em torno da conciliação entre a investigação penal e a proteção da privacidade das comunicações, e evidencia especialmente as dúvidas que se fazem sentir quanto à margem de manobra dos Estados para reter indiscriminadamente dados pessoais de comunicação.

Nas suas conclusões, o advogado-geral M. Campos Sánchez-Bordona opina que, em consonância com a linha jurisprudencial que o TJ tem seguido, a retenção dos dados terá de ser limitada, respeitando "o princípio de que só se deve conservar o mínimo […] imprescindível, em função do risco ou da ameaça, e por um período de tempo limitado"[117]. Desta forma, o artigo 15.º, n.º 1 da Diretiva opõe-se a uma legislação nacional que imponha uma obrigação de retenção em massa de dados pessoais de comunicação, independentemente de os objetivos visados através da dita retenção irem além da investigação, deteção e instauração de procedimento criminal contra um crime[118].

Espera-se que, em resposta a este pedido de decisão prejudicial, o TJ venha dar linhas orientadoras mais completas e esclarecedoras e acalmar a discussão gerada.

[116] Acórdão do Tribunal Constitucional Belga de 19 de julho de 2018 *cit. por.* VERBRUGGEN, Frank, *et al., cit.*

[117] Cfr. parágrafo 127 da versão provisória das conclusões do advogado-geral M. Campos Sánchez-Bordona de 15 de janeiro de 2020 (C-520/18, EU:C:2020:7).

[118] *Ibid.,* parágrafo 155.

3. Considerações Finais

3.1. A Verificação do *Princípio da Proporcionalidade* e a Retenção em Massa de Dados de Comunicação

Como observamos, para o TJ o cerne da questão é o respeito pelo princípio da proporcionalidade. Este princípio é usado como princípio geral de direito na sua jurisprudência desde muito cedo, enquanto "critério sobre a adequação de determinada ação da União ou dos Estados", que só deve ser tomada perante a "inexistência de outros meios menos prejudiciais" para os mesmos fins[119]. Como refere João Sérgio Ribeiro, este princípio "serve como um limite inultrapassável que deve ser sempre considerado"[120] perante compressões dos direitos fundamentais, limitando o poder do Estado.

Aplicando ao caso em estudo, as medidas que prevejam a retenção de dados de comunicação respeitarão o princípio da proporcionalidade se forem adequadas ao fim prosseguido e previsto no artigo 15.º da Diretiva 2002/58, e se não ultrapassarem o necessário para atingir esse fim.

No caso da luta contra a criminalidade, estando o período temporal e o grupo de pessoas e de meios de comunicação devidamente limitados em função do objetivo, há ainda a necessidade de se garantir a proporcionalidade entre a retenção dos dados e o crime que a origina, pois se essa retenção levar a que se tirem "conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados"[121] trata-se de uma ingerência grave, que só estará justificada perante um crime grave.

Isto mostra que, quando o objetivo prosseguido pela medida nacional impositora da retenção é a investigação, deteção e repressão de infrações penais, o TJ usa a gravidade do crime como requisito essencial para justificar uma ingerência grave na vida privada dos cidadãos.

Posto isto, apesar de ainda haver dúvidas quanto à proibição da retenção em massa de dados pessoais de comunicação, como se observa pelas questões prejudiciais enviadas nos dois últimos casos expostos ainda sem resposta, parece-nos que há, efetivamente, uma proibição absoluta. Todos os acórdãos colocam ênfase no respeito pelo princípio da proporcionalidade,

[119] GORJÃO-HENRIQUES, Miguel (2010). *Direito da União – História, Direito, Cidadania, Mercado Interno e Concorrência*, Coimbra, Almedina, 6.ª edição, p. 387.

[120] RIBEIRO, João Sérgio (2018). *Direito Fiscal da União Europeia - Tributação Direta*, Coimbra, Almedina, p. 85.

[121] Cfr. parágrafos 98 e 99 do acórdão *Tele2, cit*.

o que implica uma limitação da retenção. Uma retenção indiscriminada mostra-se como o oposto a esta regra.

Finalizando este aspeto, uma delimitação da retenção de dados face à gravidade do crime e da ingerência nos direitos fundamentais do cidadão coloca um maior peso no preenchimento dos conceitos de *ingerência grave* e de *crime grave* no direito da UE. Nos próximos pontos, analisaremos esse mesmo preenchimento.

3.2. O Conceito de *ingerência grave* nos direitos fundamentais à proteção da privacidade e dos dados pessoais

O TJ reconhece que haverá diferentes níveis de intromissão na vida privada das pessoas e desse nível dependerá o nível de justificação exigido, mas não clarifica totalmente o que se deve considerar, em termos de direito da UE, como *ingerência grave* nos direitos consagrados nos artigos 7.º e 8.º da Carta.

Sabemos, desde o caso *Digital Rights Ireland*, que não é necessário o acesso ao conteúdo da comunicação para estarmos perante uma ingerência grave, podendo o mero acesso aos dados de tráfego e de localização consubstanciar tal intromissão[122]. Esta ideia é reafirmada nas conclusões do advogado-geral a propósito do caso Tele2 – "os riscos ligados ao acesso aos dados relativos às comunicações […] podem ser equivalentes, ou inclusivamente superiores, aos que resultam do acesso ao conteúdo destas comunicações" já que estes dados "permitem catalogar quase instantaneamente uma população no seu conjunto, o que o conteúdo das comunicações não permite"[123].

Mesmo considerando que o critério será a quantidade e a precisão de conclusões sobre a vida privada da pessoa que se possa, abstratamente, obter através do acesso aos seus dados, perante casos em que não seja possível fazer essa antevisão de forma clara torna-se difícil perceber se a ingerência é, ou não, grave, e se a retenção poderá ser feita de modo compatível com o direito da União.

Posto isto, entendemos que a garantia de uma correta aplicação do Direito neste âmbito necessita de novos e mais profundos esclarecimentos pelo juiz europeu.

[122] Cfr. parágrafos 27 a 29 do Acórdão *Digital Rights Ireland*, *cit.*

[123] Cfr. parágrafo 259 das conclusões do advogado-geral Saugmandsgaard Øe a propósito do caso *Tele2, cit.*

3.3. *Crime Grave* como conceito europeu autónomo?

O debate em torno da definição de *crime grave* nasce com o acórdão *Digital Rights Ireland* e tudo apontava para que tivesse uma resposta definitiva no acórdão *Ministerio Fiscal* mas, como referido anteriormente, o TJ "escapou" a esta questão.

Recuando à transposição da Diretiva da Conservação de Dados, a falta de uma definição deste conceito nesse instrumento foi mal vista entre a doutrina. Maria Tzanou descreve-a como "problemática" por ter permitido "uma ampliação de seu escopo" e, consequentemente, uma ampliação da possibilidade de retenção de dados de comunicação[124]. Com a mesma opinião, R. van Genderen opina que estamos perante um verdadeiro "problema prático" dado não haver "uma limitação harmonizada das circunstâncias e pretensões de quando, onde e por quem os dados podem ser utilizados"[125].

Antevendo esta dificuldade, o Conselho da UE referiu, na sua Declaração de 10 de fevereiro de 2006, que para esta definição os E-M "devem ter em devida conta os crimes enumerados no artigo 2.º, n.º 2 da Decisão-Quadro relativa ao mandado de detenção europeu […] e os crimes que envolvem telecomunicações"[126] mas tal não foi suficiente pois, como refere Chris Jones[127], a opção de não incluir uma definição acabou por levar a "amplas divergências" entre os E-M. Tal facto é demonstrado pelas considerações tecidas no Relatório de Avaliação sobre a Diretiva relativa à Conservação de Dados, que revela que dez E-M "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 infrações penais previstas na legislação nacional [e a] legislação de quatro Estados-Membros […] faz referência a «crimes graves» ou a «infrações graves» sem avançar uma definição"[128].

---

[124] TZANOU, Maria (2017). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford, Hart Publishing, p. 69 (tradução nossa).

[125] GENDEREN, R. van den Hoven van (2016). *Privacy Limitation Clauses: Trojan Horses under the Disguise of Democracy: On the Reduction of Privacy by National Authorities in Cases of National Security and Justice Matters* (tese de doutoramento em Direito), Amsterdão, Vrije Universiteit Amsterdam, disponível em https://research.vu.nl/en/publications/privacy-limitation-clauses-trojan-horses-under-the-disguise-of-de, consultado a 23 de março de 2020, p. 147 (tradução nossa).

[126] Conselho da União Europeia, 2005/0182(COD), 10 de fevereiro de 2006, disponível em http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205777%202006%20ADD%201, consultado a 23 de março de 2020 (tradução nossa).

[127] JONES, Chris (2014). "Content and implementation of the Data Retention Directive", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2014/04/implementation-of-data-retention.html, consultado a 12 de março de 2020 (tradução nossa).

[128] Comissão Europeia, Relatório de Avaliação sobre a Diretiva relativa à conservação de dados, 18 de abril de 2011, p. 7.

Só o futuro dirá se a UE terá o seu próprio conceito de *crime grave* aplicável aos vários E-M, mas tal autonomização seria uma tarefa difícil, pois analisando o direito penal dos vários Estados, constatamos a disparidade entre os vários sistemas[129]. Como refere Marianne L. Wade, podemos até "falar com alguma clareza sobre o que não determina crime grave", mas o mesmo já não pode ser dito "sobre o que constitui esses crimes"[130].

Ao mesmo tempo que constatamos a dificuldade de adoção de um conceito europeu de *crime grave*, vemos também a necessidade de garantir uma aplicação clara e uniforme do direito europeu. Na verdade, o TFUE, no número 1 do seu artigo 83.º dá ao Parlamento Europeu e ao Conselho o poder de estabelecer regras de definição de infrações no âmbito de "criminalidade particularmente grave" e apresenta uma lista de "Eurocrimes"[131]. A este propósito, Vanessa Franssen questiona se esta lista poderá efetivamente ser considerada "orientação suficiente" para os Estados[132], ao passo que Wade lembra que esta disposição se refere somente "a uma forma mais grave [ou] particularmente culpável de um crime (que pode ou não ser um crime grave em si)"[133]. De facto, a disposição refere-se à criminalidade grave como resultante "da natureza ou das incidências dessas infrações, ou ainda da especial necessidade de as combater, assente em bases comuns". Assim, não são exemplos-padrão de crimes graves, por si só, mas domínios criminais[134] dentro dos quais as infrações podem vir a ser considerados graves, dependendo da forma como foram praticadas no caso concreto, o que demonstra a importância de uma análise casuística.

Na nossa opinião, apesar de não ter assegurado a sua inexistência, vemos como positivo o facto de o juiz europeu não ter autonomizado este conceito no contexto europeu nem ter imposto critérios específicos para determinar a gravidade de um crime.

Como refere o advogado-geral Saugmandsgaard Øe nas suas conclusões em *Ministerio Fiscal*, a gravidade de uma infração é uma noção demasiado variável[135] – varia de Estado para

[129] ARTEMIOU, Eleni, *cit.*

[130] WADE, Marianne L. (2014). *Developing a Criminal Justice Area in the European Union* (Estudo para a Comissão de Liberdades Civis, Justiça e Assuntos Internos do Parlamento Europeu), disponível em https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/493043/IPOL-LIBE_ET%282014%29493043_EN.pdf, consultado a 1 de abril de 2020, p. 12 (tradução nossa).

[131] FRANSSEN, Vanessa (2016), *cit.* (tradução nossa).

[132] *Id*. (tradução nossa).

[133] WADE, Marianne L. *op cit. loc cit.* (tradução nossa).

[134] Os domínios enumerados pelo artigo são "terrorismo, tráfico de seres humanos e exploração sexual de mulheres e crianças, tráfico de droga e de armas, branqueamento de capitais, corrupção, contrafação de meios de pagamento, criminalidade informática e criminalidade organizada".

[135] Cfr. parágrafo 97 das conclusões do advogado-geral Saugmandsgaard Øe a propósito do caso *Ministerio Fiscal, cit.*

Estado, consoante as suas tradições, crenças, valores e prioridades enquanto comunidade; e varia de época para época, com a própria evolução da criminalidade e das políticas penais e constantes mudanças da necessidade de repressão penal. O que é grave num Estado poderá não o ser num outro Estado e o que é considerado grave hoje poderá não o ser no futuro.

Seguir um critério normativo formal para fixar um conceito a nível de direito da UE de infração grave, isto é, fixá-lo com base na pena suscetível de ser aplicada à infração em causa, seria um erro na medida em que a pena depende dos sistemas repressivos dos diferentes Estados e, em termos globais, não reflete o nível de gravidade de uma infração. Desta forma, o TJ não deve estabelecer um *quantum* de pena que defina o limiar mínimo de gravidade pois não iria espelhar a real gravidade do crime.

Se, por outro lado, seguirmos um critério material, guiando-nos pelo específico comportamento em causa e bens jurídicos lesados através dele, constatamos, novamente, o perigo de desadequação, pois os bens jurídicos protegidos são diferentes e têm prioridades diferentes de Estado para Estado e de época para época.

Isto evidencia que se considerarmos uma noção autonomizada de *crime grave* para o direito da UE, este conceito perderá a capacidade de se moldar às variáveis em questão, e corremos o risco de ter um preenchimento do conceito desadequado às especificidades do caso. Posto isto, entendemos ser preferível não o autonomizar e deixar o conceito ser preenchido, com os necessários limites, pelos E-M.

Consideramos que deve ser estabelecida uma analogia entre o preenchimento do conceito de *crime grave* e o preenchimento dos conceitos de *segurança pública*[136] e *ordem pública*. Nestes casos, cabe aos Estados preencher as noções mas estão limitados, nesse preenchimento, pelo direito da UE, pois a jurisprudência estabelece uma interpretação estrita.

No acórdão *P.I contra Oberbürgermeisterin der Stadt Remscheid*, o TJ refere que apesar de os E-M serem "livres de determinar, em conformidade com as suas necessidades nacionais […] as exigências de ordem pública e de segurança pública […] estas exigências devem, contudo, ser entendidas em sentido estrito", não podendo o seu alcance escapar ao "controlo das instituições da União Europeia"[137]. Aplicando este entendimento ao conceito de *crime*

[136] A este propósito, o advogado-geral Saugmandsgaard Øe refere que *segurança pública* é um conceito próximo do de *luta conta criminalidade grave*, portanto é defensável uma analogia entre os dois. Cfr. parágrafo 99 das conclusões a propósito do caso *Ministerio Fiscal*, *cit*.

[137] Acórdão *P.I contra Oberbürgermeisterin der Stadt Remscheid*, de 22 de maio de 2012, (C-348/09, EU:C:2012:300), parágrafos 21 a 23.

A mesma ideia tinha sido transmitida pelo paradigmático acórdão *van Duyn e Home Office*, de 4 de dezembro de 1974, no qual o TJ afirma uma interpretação estrita (nesse caso, de *ordem pública*) "de modo a que o seu âmbito não possa ser unilateralmente determinado por cada Estado-membro sem o controlo das instituições

grave, a interpretação do conceito terá de estar sujeita ao controlo das instituições da UE e será balizada pelo princípio da proporcionalidade.

Tal como a possibilidade de restrição aos direitos fundamentais, a gravidade de um crime deve ser vista como sendo de caráter excecional. Um poder ilimitado dos Estados para preencher o conceito poderia traduzir-se na consideração de uma grande maioria dos crimes como graves, transformando a exceção em regra, tanto no que toca ao conceito de *grave*, como no que toca às ingerências possibilitadas pelo artigo 15.º da Diretiva 2002/58, pois uma restrição grave de direitos seria facilmente justificada como sendo em função da luta contra um crime grave[138].

Densificando esta analogia, é importante verificar os limites e as orientações que se podem aplicar aos E-M no preenchimento da definição:

No acórdão *Regina e Pierre Bouchereau*[139], o TJ esclarece que "o recurso por uma autoridade nacional à noção de ordem pública pressupõe […] a existência […] de uma ameaça *real* e […] *que afete um interesse fundamental da sociedade"*[140]. Este limite deverá ter aplicação análoga no que toca ao recurso à noção de *crime grave*. De facto, se a gravidade de um crime tem caráter excecional, este crime deverá traduzir uma ameaça tal como a descrita para obter essa excecionalidade.

O mesmo acórdão estabelece ainda o requisito da atualidade da ameaça – "a existência de uma condenação penal só pode ser tomada em consideração na medida em que as circunstâncias que deram lugar a essa condenação revelam a existência de um comportamento pessoal que constitua uma ameaça *atual* para a ordem pública."[141] Este critério também deverá ter aplicação no preenchimento do conceito de *crime grave*, pois se o crime em análise revela uma ameaça que já não é presente, não terá sentido atribuir-lhe um caráter excecionalmente justificativo de uma intromissão gravosa na vida privada do cidadão.

comunitárias" embora seja "necessário reconhecer às autoridades nacionais competentes uma margem de apreciação" (C- 41/74, EU:C:1974:133, parágrafo 18).

[138] Cfr. parágrafo 27 das conclusões do advogado-geral Saugmandsgaard Øe a propósito do caso *Ministerio Fiscal, cit*.

[139] Acórdão de 27 de outubro de 1977 (C-30/77, EU:C:1977:172).

[140] Cfr. parágrafo 35 do acórdão *cit*. (itálico nosso).

A mesma ideia está presente no acórdão de 28 de outubro de 1975, *Roland Rutili e Ministro do Interior* (C-36/75, EU:C:1975:137), parágrafo 28.

[141] Cfr. parágrafo 28 do acórdão *Regina e Pierre Bouchereau, cit.* (itálico nosso).

Esta ideia foi também reproduzida no acórdão de 29 de abril de 2004, *Georgios Orfanopoulos e o. e Land Baden-Württemberg* (C-482/01 e C-493/01).

Desta forma, os órgãos jurisdicionais nacionais terão de verificar se, no caso concreto, o crime se traduz numa ameaça que preenche os requisitos necessários – terá de ser real, atual e afetante de um interesse fundamental da sociedade. Só com esta verificação poderá o crime adquirir o carácter excecional de *grave*.

Uma orientação importante aos Estados é dada pelo já referido artigo 83.º do TFUE, que no seu número 1 prevê a intervenção do legislador da União na definição das infrações penais nos "domínios de criminalidade particularmente grave". Como é referido no acórdão *P.I contra Oberbürgermeisterin der Stadt Remscheid*, as infrações dentro deste domínio "constituem uma violação especialmente grave de um interesse fundamental da sociedade, suscetível de representar uma ameaça direta para a tranquilidade e a segurança física da população"[142]. Se uma infração deste tipo for cometida com "características especialmente graves, o que compete ao órgão jurisdicional de reenvio verificar com base numa análise individual do caso concreto"[143] então enquadrar-se-á no conceito de *crime grave*.

Este mesmo entendimento pode ser aplicado, na nossa opinião, ao elenco de crimes do artigo 2.º, n.º 2 da Decisão-Quadro relativa ao mandado de detenção europeu, que como observamos, foi referido pelo Conselho da UE na sua declaração a propósito da transposição da Diretiva da Conservação de Dados como um elenco importante para as definições nacionais de *crime grave*. Parece-nos razoável assumir que as infrações enumeradas na disposição se enquadrarão no conceito em análise desde que – mais uma vez aplicando analogamente o entendimento do TJ – essas infrações tenham sido praticadas com características especialmente graves, no caso concreto.

Concluindo este tópico, a analogia que defendemos permite "fechar a brecha" da falta de uma definição autónoma de *crime grave* a nível europeu, impedindo, graças a uma interpretação estrita, que o seu preenchimento seja feito arbitrariamente pelos E-M e leve a uma ingerência injustificada nos direitos fundamentais dos cidadãos, ao mesmo tempo que possibilita uma adaptação da noção às conceções do Estado e da época.

[142] Cfr. parágrafo 28 do acórdão *P.I contra Oberbürgermeisterin der Stadt Remscheid, cit.*
[143] *Id*.

4. Conclusão

Ao longo desta exposição observamos que a UE tentou responder aos avanços tecnológicos, e criminalidade a estes associada, com um sistema de vigilância que foi longe demais, ultrapassando a barreira exigida pelos direitos fundamentais de respeito pela vida privada e proteção dos dados pessoais. É uma conciliação difícil que ainda não foi completamente solucionada, mas o juiz europeu foi dando preciosas linhas de orientação, sendo que todas tocam o amplo princípio da proporcionalidade.

Com *Digital Rights Ireland*, fica percetível que o TJ tem um papel constitucional e zelará pela proteção dos direitos fundamentais dos cidadãos, mas surgem várias dúvidas: Há uma definição europeia de *crime grave*? Há justificação possível para retenção em massa de dados de comunicação?

Com *Tele2*, fica claro que a retenção de dados só é possível quando justificada através de condições apertadas, com delimitação das pessoas e meios de comunicação abrangidos face ao objetivo visado e sempre com uma limitação ao estritamente necessário. Uma das consequências desta orientação é a largamente discutida proibição da retenção em massa de dados de comunicação, mas a delimitação de um grupo de pessoas cujos dados poderão ser retidos para o objetivo de investigação, deteção e repressão penais é também uma opção questionável, como vimos a propósito do caso *Ordre des barreaux francofones*.

Em *Minsiterio Fiscal*, há uma reafirmação da jurisdição do TJ na matéria do tratamento de dados, mesmo que o caso envolva medidas nacionais relativas a atividades próprias dos Estados, e fica esclarecido que a gravidade de um crime não é um critério obrigatório para a justificação de uma ingerência na privacidade dos utilizadores de comunicações eletrónicas, sendo somente obrigatória para ingerências consideradas, também elas, graves. Reafirma-se, assim, o princípio da proporcionalidade.

O TJ tem já em mãos novos casos por decidir, neste mesmo âmbito, e será importante analisar as suas considerações pois daí resultará uma consolidação do caminho jurisprudencial a que temos assistido, ou uma mudança de paradigma e o nascimento de novos debates.

A manter-se esta linha jurisprudencial, as questões que mais ecoam e que devem ser, a nosso ver, esclarecidas pelo juiz nestas novas oportunidades para tal, prendem-se com o que se deverá considerar como *ingerência grave* e com a possível existência de um conceito europeu de *crime grave*.

Para já, o que sabemos acerca da primeira questão é que terá de ser feita uma antevisão das conclusões sobre a vida privada do cidadão passíveis de ser extraídas pela retenção dos

seus dados pessoais de comunicação, sendo que uma grande quantidade, com grande precisão, aponta, claramente, para uma ingerência grave, mesmo sem acesso ao conteúdo da comunicação. Voltamos a referir que esta antevisão nem sempre é clara, daí a questão permanecer.

Quanto à segunda questão, recapitulando brevemente as considerações que apresentamos, *crime grave* é um conceito demasiado variável para ter um preenchimento europeu definitivo. Defendemos que a única forma de garantir a sua adequação às especificidades dos Estados e das épocas é atribuir a competência do seu preenchimento aos próprios Estados. Por outro lado, para combater intromissões injustificadas nos direitos fundamentais, é necessário balizar este poder nacional, com a imposição de uma interpretação estrita do conceito, tal como a jurisprudência prevê para os conceitos de *ordem pública* e *segurança pública*. Assim, o preenchimento da noção de *crime grave* terá de ter em consideração a excecionalidade da qualificação de uma conduta como *grave*, pelo que os órgãos jurisdicionais nacionais terão de verificar se, no caso concreto, o crime se traduz numa ameaça real, atual e afetante de um interesse fundamental da sociedade. Teremos, assim, simultaneamente, um conceito adequado ao Estado e à época e compatível com o direito da União.

Bibliografia

ARTEMIOU, Eleni (2018). "The way out of Digital Rights Ireland", in *The CiTiP Blog*, disponível em https://www.law.kuleuven.be/citip/blog/the-way-out-of-digital-rights-ireland/

BIGO, Didier, *et al.* (2013). "Mass Surveillance of Personal Data by EU Member States and its compatibility with EU Law", in *CEPS Paper in Liberty and Security in Europe*, n.º 62, novembro.

CORDEIRO, A. Barreto Menezes (2018). *Dados Pessoais: Conceito, extensão e limites*, Centro de Investigação de Direito Privado, Universidade de Lisboa, disponível em https://blook.pt/publications/publication/e38a9928dbce/

COUDERT, Fanny (2017). "In the aftermath of Tele2 and Opinion 1/15: when are data retention measures legitimate?", in *The CiTiP Blog*, disponível em https://www.law.kuleuven.be/citip/blog/in-the-aftermath-of-tele2-and-opinion-115-when-are-data-retention-measures-legitimate/

FORMICI, Giulia (2019). "ECJ, the floor is yours! The never ending story between Data Retention and Right to Privacy" in *The CiTiP Blog*, disponível em https://www.law.kuleuven.be/citip/blog/ecj-the-floor-is-yours-the-never-ending-story-between-data-retention-and-right-to-privacy/

FRANSSEN, Vanessa (2016). "The future of national data retention obligations – How to apply Digital Rights Ireland at national level?" in *The European Law Blog – News and Comments on EU Law*, disponível em https://europeanlawblog.eu/2016/07/25/the-future-of-national-data-retention-obligations-how-to-apply-digital-rights-ireland-at-national-level/

GENDEREN, R. van den Hoven van (2016). *Privacy Limitation Clauses: Trojan Horses under the Disguise of Democracy: On the Reduction of Privacy by National Authorities in Cases of National Security and Justice Matters* (tese de doutoramento em Direito), Amsterdão, Vrije Universiteit Amsterdam, disponível em https://research.vu.nl/en/publications/privacy-limitation-clauses-trojan-horses-under-the-disguise-of-de

GORJÃO-HENRIQUES, Miguel (2010). *Direito da União – História, Direito, Cidadania, Mercado Interno e Concorrência*, Coimbra, Almedina, 6.ª edição.

GUILD, Elspeth e CARRERA, Sergio (2014). "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", in *CEPS Paper in Liberty and Security in Europe*, n.º 65, maio.

JONES, Chris (2014). "Content and implementation of the Data Retention Directive", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2014/04/implementation-of-data-retention.html.

-. (2014). "National legal challenges to the Data Retention Directive", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2014/04/national-legal-challenges-to-data.html

LÓPEZ-LAPUENTE, Leticia (2008). "La conservación de los datos por los operadores de servicios de comunicaciones electrónicas", in *Actualidad Jurídica Uría Menéndez*, n.º 19, janeiro-abril.

LYNSKEY, Orla (2014). "Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and Others: The Good, the Bad and the Ugly", in *The European Law Blog – News and Comments on EU Law*, disponível em https://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/

-. (2013). "Plenty to retain? Opinion of the Advocate General in Joined Cases C-293/12 and 594/12, Digital Rights Ireland ltd and Seitlinger and others", in *The European Law Blog – News and Comments on EU Law*, disponível em https://europeanlawblog.eu/2013/12/17/plenty-to-retain-opinion-of-the-advocate-general-in-joined-cases-c-29312-and-59412-digital-rights-ireland-ltd-and-seitlinger-and-others/

-. (2017). "Tele2 Sverige AB and Watson et al - Continuity and Radical Change", in *The European Law Blog – News and Comments on EU Law*, disponível em https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/

MEHDI, Rostane (2007). "L'autonomie institutionnelle et procédurale et le droit administratif" in *Droit Administratif Européen* (eds.: Jean-Bernard Auby e Jacqueline Dutheil de la Rochère), Bruxelas, Bruylant.

NESTEROVA, Irena (2017). "Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards", in *European Society of International Law Conference Paper Series*, vol. 8, n.º 5.

NEVES, Rita Castanheira (2011). *As ingerências nas comunicações eletrónicas em processo penal: natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*, Coimbra, Coimbra Editora.

OUAKI, Myriam (2015). "Declaração de invalidade de uma diretiva pelo TJ: O caso da conservação de dados", in *Estudos Comemorativos dos 20 anos da Abreu Advogados* (coord.: Luís Gonçalves da Silva e Ricardo Costa), Coimbra, Almedina.

PAIS, Sofia Oliveira (2012). *Estudos de Direito da União Europeia*, Coimbra, Almedina.

PEERS, Steve (2014). "The data retention judgment: The CJEU prohibits mass surveillance", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2014/04/the-data-retention-judgment-cjeu.html

-. (2014). "The Domino Effect: how many EU treaties violate the rights to privacy and data protection?", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2014/11/the-domino-effect-how-many-eu-treaties.html

RAMALHO, David Silva e COIMBRA, José Duarte (2016). "A declaração de invalidade da Diretiva 2006/24/CE - presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", in *O Direito*, ano IV, n.º 147.

RIBEIRO, João Sérgio (2018). *Direito Fiscal da União Europeia - Tributação Direta*, Coimbra, Almedina.

SANTOS, Cristina Máximo dos (2004). "As novas tecnologias da informação e o sigilo das telecomunicações" in *Revista do Ministério Público*, n.º 99.

SILVEIRA, Alessandra (2013). "Artigo 52.º - Âmbito e Interpretação dos Direitos e dos Princípios" in *Carta dos direitos fundamentais da UE: comentada* (coord.: Alessandra Silveira e Mariana Canotilho), Coimbra, Almedina.

TEIXEIRA, Maria Leonor da Silva (2013). "A União Europeia e a Proteção de Dados Pessoais – «Uma visão futurista»", in *Revista do Ministério Público*, n.º 135.

TZANOU, Maria (2017). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, Oxford, Hart Publishing.

VEDASCHI, Arianna e LUBELLO, Valerio (2015). "Data Retention and its Implications for the Fundamental Right to Privacy", in *Tilburg Law Review*, vol. 20, n.º 1.

VERBRUGGEN, Frank, *et al.* (2018). "Reconsidering The Blanket-Data-Retention-Taboo, For Human Rights' Sake?", in *The European Law Blog – News and Comments on EU Law*, disponível em http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/

WADE, Marianne L. (2014). *Developing a Criminal Justice Area in the European Union* (Estudo para a Comissão de Liberdades Civis, Justiça e Assuntos Internos do Parlamento Europeu), disponível em https://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/493043/IPOL-LIBE_ET%282014%29493043_EN.pdf

WHITE, Matthew (2017). "A Threat to Human Rights? The new e-Privacy Regulation and some thoughts on Tele2 and Watson", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2017/01/a-threat-to-human-rights-new-e-privacy.html

-. (2016). "Data retention and national law: whatever the CJEU rules, data retention may still survive!", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2016/03/data-retention-and-national-law.html

-. (2017). "The Privacy International case in the IPT: respecting the right to privacy?", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2017/09/the-privacy-international-case-in-ipt.html

-. (2018). "Data Retention incompatible with EU law: Victory? Victory you say?", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2018/05/data-retention-incompatible-with-eu-law.html

WONG, Rebecca (2012). "The Data Protection Directive 95/46/EC: Idealisms and Realisms", in *International Review of Law Computers & Technology*, vol. 26, n.º 2.

WOODS, Lorna (2016). "Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2016/12/data-retention-and-national-law-ecj.html

-. (2018). "Mobile phone theft and EU eprivacy law: the CJEU clarifies police powers", in *EU Law Analysis - Expert insight into EU law developments*, disponível em http://eulawanalysis.blogspot.com/2018/10/mobile-phone-theft-and-eu-eprivacy-law.html

Jurisprudência Consultada

Acórdãos do TJ:

Acórdão de 4 de dezembro de 1974, *van Duyn e Home Office* (C- 41/74, EU:C:1974:133).

Acórdão de 28 de outubro de 1975, *Roland Rutili e Ministro do Interior* (C-36/75, EU:C:1975:137).

Acórdão de 27 de outubro de 1977, *Regina e Pierre Bouchereau* (C-30/77, EU:C:1977:172).

Acórdão de 29 de abril de 2004, *Georgios Orfanopoulos e o. e Land Baden-Württemberg* (C-482/01 e C-493/01, EU:C:2004:262).

Acórdão de 10 de fevereiro de 2009, *Irlanda/Parlamento e Conselho* (C-301/06, EU:C:2009:68).

Acórdão de 22 de maio de 2012, *P.I contra Oberbürgermeisterin der Stadt Remscheid* (C-348/09, EU:C:2012:300).

Acórdão de 8 de abril de 2014, *Digital Rights Ireland e o.* (C-293/12 e C-594/12, EU:C:2014:238).

Acórdão de 21 de dezembro de 2016, *Tele2 Sverige e Watson e o*. (C-203/15 e C-698/15, EU:C:2016:970).

Acórdão de 2 de outubro de 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788).

Outra Jurisprudência:

Conclusões do advogado-geral Henrik Saugmandsgaard Øe de 19 de julho de 2016, *Tele2 Sverige e Watson e o*. (C-203/15 e C-698/15, EU:C:2016:572).

Decisão do *Investigatory Powers Tribunal* de 8 de setembro de 2017, *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs e o*., disponível em http://shorturl.at/CHJ45

Pedido de decisão prejudicial de 31 de outubro de 2017, *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs e o.* (C-623/17).

Decisão do Supremo Tribunal do Reino Unido *Liberty contra Secretary of State for the Home Department e o.* [EWHC 975 (Admin)] de 27 de abril de 2018, disponível em http://www.bailii.org/ew/cases/EWHC/Admin/2018/975.html

Conclusões do advogado-geral Henrik Saugmandsgaard Øe de 3 de maio de 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:300).

Pedido de decisão prejudicial de 2 de agosto de 2018, *Ordre des barreaux francophones and germanophone e o.* (C-520/18).

Versão provisória das conclusões do advogado-geral Manuel Campos Sánchez Bordona de 15 de janeiro de 2020, *Ordre des barreaux francophones e germanophone e o*. (C-520/18, EU:C:2020:7).

Versão provisória das conclusões do advogado-geral Manuel Campos Sánchez Bordona de 15 de janeiro de 2020, *Privacy International contra Secretary of State for Foreign and Commonwealth Affairs e o.* (C-623/17, EU:C:2020:5).