O Mercado Único Digital e a interoperabilidade administrativa: a proteção de dados pessoais na articulação entre administrações públicas nacionais e as instituições e órgãos da União Europeia – reflexões prospectivas[1]

JOANA COVELO DE ABREU[2]

Resumo:

Com o Mercado Único Digital, reputou-se adequada a aposta nos serviços públicos digitais, emergindo o paradigma da Administração Pública em linha, potenciada através do método da interoperabilidade administrativa que, a breve trecho, passou a ser perspetivado como princípio geral. Assim, a interoperabilidade pressupõe que as Administrações Públicas nacionais e as instituições da União se encontrem ligadas entre si,

1 Professora da Escola de Direito da Universidade do Minho (jabreu@direito.uminho.pt – Escola de Direito da Universidade do Minho, Campus de Gualtar, 4710-570, Braga) e da Universidade Portucalense (jabreu@upt.pt – Universidade Portucalense Infante D. Henrique, Rua Dr. António Bernardino de Almeida, 541, 4200-072, Porto).

dispondo de bases de dados comuns e de pontes digitais de transição que lhes potenciem as comunicações. Quer as Administrações Públicas nacionais, quer as instituições, tratam de dados pessoais, resultando a sua proteção consolidada em direito derivado da União – o RGPD e o recente Regulamento 2018/1725. Neste contexto, cabe equacionar se estes instrumentos são capazes de, num contexto de interoperabilidade, assegurar o padrão mais elevado do direito fundamental à proteção de dados pessoais e se as articulações entre os tribunais nacionais e o Tribunal de Justiça, em caso de violações, reforçam tal proteção.

Palavras-chave: Mercado Único Digital; Administração Pública em linha; interoperabilidade; RGPD; Regulamento n.º 2018/1725

Abstract:

With the Digital Single Market settlement there was a bet on digital public services. E-Government paramount was optimized by the administrative interoperability method which, with short notice, was seen as a general principle. Therefore, interoperability presupposes national Public Administrations and Union institutions are interconnected, having common databases and transition digital bridges to boost their communications. Both national Public Administrations and European institutions are dealing with personal data whose consolidated protection was achieved through secondary Union law – GDPR and the new Regulation 2018/1725. In this context, it has to be equated if those instruments are able to, in a context of interoperability, secure the highest standard of the fundamental right to personal data protection and if

articulations between national courts and the Court of Justice, in case of violations, reinforce that protection.

Keywords: *Digital Single Market; e-Government; interoperability; GDPR; Regulation No. 2018/1725*

Sumário:

1. O Mercado Único Digital – o interesse público primário inerente ao estado da arte

A *internet* afigura-se como o espaço que definiu uma nova perceção das dimensões económica, política, social, cultural e recreativa já que, no seu seio, aquelas "se confundem e aglomeram, determinando que diferentes paradigmas coabitem"[2]. Emerge, assim, como um fenómeno

2 J. Covelo de Abreu, "O Mercado Único Digital como o novo mundo para a União Europeia: repercussões na estrutura regulatória social e institucional – a redefinição do serviço universal e do Organismo de Reguladores Europeus das Comunicações Eletrónicas (ORECE)", *UNIO – EU Law Journal*, Vol. 4, N.º 2, Julho 2018, p. 60.

de facilitação com repercussões económicas que devem ser atendidas. Outrossim, a generalização das ferramentas digitais permitiu que todos os setores de atividade "se reinventassem e explorassem novas formas de procura e de oferta, novas formas de comercialização, novas plataformas de publicidade e de marketing, etc."[3].

Nesta senda, a União Europeia – ainda durante crise mundial vivenciada – determinou as potencialidades de apostar, no seu espaço e âmbito de atuação, numa estratégia que passasse pelo digital e pela sedimentação das novas tecnologias de informação e comunicação. Assim, na Estratégia Europa 2020, a União começou por definir, entre as "sete iniciativas emblemáticas", o estabelecimento de uma "Agenda digital para a Europa", através da qual visava "acelerar a implantação da Internet de alta velocidade", permitindo que "as famílias e as empresas [pudessem] tirar partido de um mercado único digital", já que este era um dos caminhos promissores para "definir uma estratégia credível de saída da crise"[4]. Desde então, a União Europeia entendeu que as demandas com lastro global se tornavam mais presentes, adiantando que, "[e]nquanto a Europa [tinha] de abordar as suas próprias fragilidades estruturais, o mundo [estava] a evoluir rapidamente" uma vez que as economias se encontravam, já à data, "cada vez mais interligadas"[5].

Neste diapasão, o Mercado Único Digital passou a marcar a agenda política europeia e nacional, determinando que todos os agentes polí-

---

3 J. Covelo de Abreu, "O Mercado Único Digital", UNIO, p. 60.

4 Comissão Europeia, *Comunicação EUROPA 2020, Estratégia para um crescimento inteligente, sustentável e inclusivo*, Bruxelas, 3 de março de 2010, COM(2010) 2020 final, p. 6.

5 Comissão Europeia, *Comunicação EUROPA*, p. 9.

ticos se congratulassem com o seu estabelecimento. Quer os Estados-Membros, quer as instituições europeias começaram a verificar que a oferta digital havia impactado dramaticamente na emergência e perceção privilegiada de uma economia digital, a qual era e continua a ser capaz de acarretar benefícios inegáveis para a sociedade atual porque criadora de um valor digital acrescentado que deve ser considerado no presente e no futuro da União Europeia e na sua estratégia de crescimento e de sustentabilidade económica[6]. Para o efeito, a Comissão Europeia lembrava que se tinha de implementar uma sociedade digital.

A aposta na digitalização personifica-se, então, como o bem comum desta comunidade politicamente organizada que não é avessa ao papel que as plataformas em linha assumiram. Desde cedo que a Comissão Europeia reconheceu que, apesar de "diversas plataformas globalmente competitivas [terem tido] origem na Europa", "globalmente, a UE apenas representa […] cerca de 4% da capitalização total de mercado das maiores plataformas em linha" ainda que contribua para cerca "de 30% das receitas globais nas principais plataformas de distribuição de aplicações"[7]. Já anteriormente tinha apresentado resultados preliminares, explanando que "o mercado mundial das tecnologias de informação e comunicação [ascendia] a dois biliões de EUR mas as empresas europeias só [representavam] um quarto deste total"[8]. Concluiu, assim, pela necessidade

6 Comissão Europeia, *Comunicação ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, A plataformas em linha e o mercado único digital: Oportunidades e desafios para a Europa*, Bruxelas, 25 de maio de 2016, COM(2016) 288 final, p. 1.

7 Comissão Europeia, *Comunicação ao Parlamento Europeu*, p. 3.

8 Comissão Europeia, *Comunicação EUROPA*, p. 14.

de estabelecer um meio propício às inovações nas plataformas em linha já que "[a] criação do enquadramento adequado e do ambiente ideal é essencial para reter, desenvolver e promover a emergência de novas plataformas em linha na Europa"[9].

Para o efeito, a estratégia política de implementação do Mercado Único Digital foi adotada a 6 de maio de 2015, tendo-se determinado que, até janeiro de 2017, a Comissão Europeia era responsável por apresentar iniciativas específicas no sentido de criar o enquadramento jurídico adequado através do procedimento legislativo ordinário, mobilizando quer o Parlamento Europeu, quer o Conselho para o efeito[10]. Tal é possível pois, como a nomenclatura faz antever, o Mercado Único Digital está a ser atualmente desenvolvido sob o "chapéu" do bom funcionamento do Mercado Interno, ao abrigo das competências partilhadas entre a União e os Estados-Membros – artigo 4.º, n.º 2, a) do Tratado sobre o Funcionamento da União Europeia (doravante TFUE). Na realidade, a União Europeia chamou a si a sua consecução na medida em que, durante longos anos, confiou nas diligências dos seus Estados-Membros. No entanto, começou a verificar que tais desenvolvimentos isoladamente realizados começavam a gerar alguns descompassos e dificuldades de articulação entre as tecnologias implementadas nos diversos Estados-Membros, o que demandava a sua intervenção para o estabelecimento de padrões comuns.

Acresce que a Comissão Europeia também entendeu que tal empenho poderia agilizar um maior acesso às informações por parte dos ci-

9 Comissão Europeia, *Comunicação ao Parlamento Europeu*, p. 4.

10 A. Silveira e J. Covelo de Abreu, "Interoperability solutions under Digital Single Market: European e-Justice rethought under e-Government paradigm", *European Journal of Law and Technology*, Vol. 9, Issue, 1, 2018, p. 1.

dadãos e seria capaz de desenvolver um exercício administrativo mais aberto, inclusivo e participado pelos particulares[11]. Afinal, só assim se contribui decisivamente para a adequação das liberdades fundamentais aos novos desígnios digitais, observando a livre concorrência potenciada ao nível da União[12]. Assim, desenhado enquanto interesse público primário a ser prosseguido pela União e pelos seus Estados-Membros, a sua execução prendeu-se com o estabelecimento de um conjunto de objetivos a serem atingidos enquanto interesses públicos secundários: afinal, o Mercado Único Digital "poderá contribuir com 415 mil milhões de euros para a economia europeia, impulsionando assim o emprego, o crescimento, a concorrência, o investimento e a inovação" e alavancar a transformação dos serviços públicos[13].

Cabe, portanto, às Administrações Públicas europeias (nacionais, quando aplicam o direito da União, e às instituições, órgãos e organismos da União Europeia) prosseguir os interesses públicos secundários, concretizadores do desígnio político do Mercado Único Digital. Tais interesses públicos secundários intuem-se a partir dos objetivos estabelecidos, dos quais dois ganham relevância para a nossa exposição: i) a sedimentação de uma interoperabilidade administrativa que permita que as Administrações Públicas nacionais e as instituições e órgãos da União tenham efetiva expressão digital e capacidade de interação, entre si e com os administrados, por essa via, a fim de observar as liberdades fun-

11 COMISSÃO EUROPEIA, *Commission staff working document – A Digital Single Market for Europe – Analysis and Evidence*, Bruxelas, 6 de maio de 2015, SWD(2015) 100 final , p. 3.

12 COMISSÃO EUROPEIA, *Commission staff working document*, p. 3.

13 COMISSÃO EUROPEIA, *Mercado Único Digital*, *in* https://ec.europa.eu/commission/priorities/digital-single-market_pt [acesso: 25.01.2019].

damentais características do Mercado Interno; e ii) o estabelecimento de um elevado padrão de proteção de dados pessoais no contexto da União, para, a par e passo, se exponenciar também a livre circulação de dados pessoais num ambiente controlado e protetivo e o estabelecimento de uma "economia europeia dos dados"[14].[15]

Cabe, assim, precisar que serão chamadas à colação tanto as Administrações Públicas nacionais quanto as instituições e órgãos da União a fim de dar corte a tais propósitos. Tal é assim porque as Administrações Públicas nacionais, quando aplicam direito da União, encontram-se a atuar também na sua veste de Administrações Públicas funcionalmente europeias[16] e a instituição, o órgão ou o organismo da União chamado materialmente à colação poderá ser reputado como Administração Pública organicamente europeia. Neste contexto, torna-se particularmente premente que as Administrações Públicas dos diversos Estados-Mem-

---

14 Comissão Europeia, *Mercado Único Digital*, *in* https://ec.europa.eu/commission/priorities/digital-single-market_pt [acesso: 25.01.2019].

15 A economia europeia dos dados assenta num quadro de fluxo livre de dados não pessoais. No entanto, para a sua ativação foi necessária a competente delimitação e proteção dos dados que são considerados pessoais e, bem assim, a sua sujeição a um padrão de jusfundamentalidade mais elevado. Para mais informações sobre a economia europeia dos dados, Comissão Europeia, *Building a European data economy*, *in* https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy [acesso: 25.1.2019].

16 Tal nomenclatura é adotada por alusão à dicotomia "tribunais nacionais enquanto tribunais funcionalmente europeus" que Alessandra Silveira tem vindo a sedimentar. A propósito, A. Silveira, *Princípios de direito da União Europeia. Doutrina e Jurisprudência*, 2.ª ed., Lisboa: Quid Iuris. Na realidade, os tribunais nacionais são funcionalmente europeus quando aplicam direito da União Europeia enquanto os tribunais que compõem o Tribunal de Justiça da União Europeia são tribunais organicamente europeus. No mesmo diapasão, as Administrações Públicas nacionais serão consideradas como funcionalmente europeias quando aplicam direito da União enquanto as Instituições, órgãos e organismos da União serão administrações organicamente europeias porque a sua orgânica, funcionamento, criação e extinção é ditada integralmente pelo direito da União, não se observando, quanto a estas, o princípio geral de direito da União da autonomia institucional dos Estados-Membros.

bros se considerem entrosadas neste fenómeno sob pena de frustrar, em primeira linha, os objetivos de prosperidade para a Europa através do seu empenho no digital[17].

A Comissão Europeia promoveu um fórum de auscultação dos agentes interessados, em 2016, designado *Digital4EU Stakeholder Forum*, onde se contemplou que o caminho passaria, em primeira linha, pelo estabelecimento de serviços públicos digitais[18]. Na realidade, segundo o Relatório da Atividade, verificou-se que, apesar de "os serviços [públicos digitais] terem melhorado, também as expectativas dos utilizadores aumentaram", havendo diferenças consideráveis entre Estados-Membros[19]. Por outro lado, denotou-se algum desconhecimento quanto à oferta de serviços públicos digitais: ficou patente que "1 em cada 5 utilizadores europeus não sabem que certos serviços *online* existem", que há "problemas relacionados com a disponibilidade dos serviços, a sua qualidade e a transparência associada" e que não são facilmente acessíveis[20]. Apostou-se, assim, numa tendência de as Administrações Públicas nacionais tornarem os seus serviços votados a um desígnio digital para que o seu uso se torne mais "fácil e simples"[21], fixando-se que este seria o primeiro caminho a seguir.

---

17 J. Covelo de Abreu, "Digital Single Market under EU political and constitutional calling: European electronic agenda's impact on interoperability solutions", *UNIO – EU Law Journal*, Vol. 3, No. 1 (2017), 124, *in* http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%203/UNIO%203%20EN/Joana%20Covelo%20de%20Abreu%20(1).pdf [acesso: 25.01.2019].

18 Comissão Europeia, *#Digital4EU Stakeholder Forum Report*, Bruxelas, 25 de fevereiro de 2016, p. 14. Afinal, adianta-se no Relatório, relativamente aos serviços públicos digitais, que "*digital should be first for all public services*".

19 Comissão Europeia, *#Digital4EU Stakeholder*, p. 12 (tradução livre).

20 Comissão Europeia, *#Digital4EU Stakeholder*, p. 12 (tradução livre).

21 Comissão Europeia, *#Digital4EU Stakeholder*, p. 12 (tradução livre).

É neste contexto que surge o método da interoperabilidade – terminologia conhecida e já sedimentada no âmbito das tecnologias de informação[22] – através da Decisão n.º 2015/2240[23], que estabeleceu o Programa ISA[2] e que visou criar um plano sobre soluções de interoperabilidade para as Administrações Públicas, as empresas e os cidadãos europeus como meio de modernização do setor público. Afinal, "[a] interoperabilidade facilita uma execução bem-sucedida das políticas e tem um grande potencial para evitar barreiras eletrónicas transfronteiriças, favorecendo a emergência de serviços públicos"[24]. Cabe-nos, por conseguinte, escrutinar esta terminologia e o seu impacto jurídico-administrativo nas relações entre os Estados-Membros e a União Europeia.

2. A interoperabilidade administrativa e o paradigma da Administração Pública em linha: estado da arte

O artigo 2.º, n.º 1 da Decisão relativa ao Programa ISA[2] diz-nos que se deverá entender por interoperabilidade "a capacidade de organizações díspares e diversas interagirem com vista à consecução de objetivos comuns com benefícios mútuos, definidos de comum acordo, implicando a partilha de informações e conhecimentos entre si, no âmbito dos processos administrativos a que dão apoio, mediante o intercâmbio de dados entre os respetivos sistemas de TIC". Tal demanda "uma intercone-

22 Y. Charalabidis, *Interoperability in Digital Public Services and Administration: Bridging e-Government and e-Business*, Hershey: New York, 2011.

23 Decisão (UE) n.º 2015/2240, do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, que cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus (Programa ISA[2]) como um meio para modernizar o setor público.

24 Decisão n.º 2015/2240, considerando 4.

xão efetiva entre os componentes digitais" já que "a interoperabilidade é necessária para colocar os serviços públicos a trabalhar num contexto transfronteiriço"[25] sob pena de comprometer o bom funcionamento do Mercado Interno e a observância das liberdades de circulação[26]. A interoperabilidade busca, assim, que os Estados-Membros criem e reconvertam as suas plataformas digitais, a fim de promover a sua interconexão e a sua ligação a uma unidade tecnológica central que permitirá que as autoridades nacionais e europeias possam usufruir de redes comuns em diferentes campos de atuação, criando-se um ambiente protegido, nomeadamente em sede de dados pessoais[27], que facilita o acesso transfronteiriço a documentos e informações relevantes[28].

Afinal, visou-se o estabelecimento de um paradigma – o da Administração Pública em linha (*e-Government*) – cujo aproveitamento pleno se poderá atingir através de soluções de interoperabilidade, pois possibilita "a prestação de serviços públicos transparentes de extremo-a-extremo,

---

25 J. Covelo de Abreu, "Digital Single Market", UNIO, p. 133.

26 Comissão Europeia, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions –EU eGovernment Action Plan 2016-2020 – Accelerating the digital transformation of government*, Bruxelas, 19 de abril de 2016, COM(2016) 179 final, p. 1.

27 A propósito, o artigo 4.º, alínea b), § 5, da Decisão n.º 2015/2240, que estatui: "As ações lançadas ou prosseguidas ao abrigo do Programa ISA² devem: b) respeitar os seguintes princípios: § 5 segurança, respeito da privacidade e proteção de dados".

28 A propósito, artigos 16.º, n.ºs 1 e 5 do Regulamento (CE) n.º 1071/2009, do Parlamento Europeu e do Conselho, de 21 de outubro de 2009, que estabelece regras comuns no que se refere aos requisitos para o exercício da atividade de transportador rodoviário e que revoga a Diretiva 96/26/CE, do Conselho, que determinava a ligação de todos os Estados-Membros a um sistema comum de controlo das exigências impostas, aos transportadores rodoviários, à luz do Regulamento; e Diretiva n.º 2006/126/CE, do Parlamento Europeu e do Conselho, de 20 de dezembro de 2006, relativa à carta de condução (Reformulação) que determinava a obrigação dos Estados-Membros promoverem a sua ligação à RESPER, uma rede telemática a ser estabelecida na União Europeia.

o que conduzirá à redução dos encargos administrativos e dos custos"[29]. Nesta senda, a interoperabilidade passou a ser mais do que "o método", "a engrenagem" que estabelece e fortalece a Administração Pública em linha – a par de outros princípios gerais aplicáveis às interações de natureza administrativa, a interoperabilidade figura também como um princípio a ser observado. Há uma nova dinâmica principiológica associada às dimensões digitais: ao lado dos princípios tradicionais da acessibilidade e inclusão e da confiança e transparência, surgem os princípios do digital por defeito (*digital by default*), da interoperabilidade por defeito (*interoperability by default*) e da uma única vez (*once only*). O princípio do digital por defeito demanda que as Administrações Públicas sejam capazes de facultar os seus serviços por via digital como opção prioritária e através de um balcão único intuitivo. Já o princípio da uma única vez visa que as Administrações Públicas assegurem que os cidadãos e as empresas apenas terão de facultar as informações uma única vez, procedendo-se ao reaproveitamento de dados, em total observância da proteção de dados pessoais, evitando assim que sejam os particulares a terem de iniciar novos procedimentos para fornecer as mesmas informações ou os mesmos documentos. Já o princípio da interoperabilidade por defeito determina que "os serviços públicos devem ser desenvolvidos para trabalhar perfeitamente no Mercado Interno, através de pontes de comunicação organizacional, baseando-se na livre circulação de dados e de serviços digitais na União Europeia"[30]. Tais intentos voltaram a ser reafirmados na Declaração Ministerial sobre Administração Pública em linha, assinada em Talin, em Outubro de 2017.

29 Decisão n.º 2015/2240, considerando 30.

30 Comissão Europeia, *Accelerating the digital transformation*, p. 3 (tradução livre).

A fim de promover os princípios da acessibilidade, transparência e do digital por defeito, tais intervenientes ministeriais estabeleceram que iriam assegurar que "os cidadãos europeus e as empresas poderão interagir digitalmente com a administração pública quando aqueles assim o escolham e quando seja exequível e apropriado em termos de custo-benefício e numa perspetiva de proteção do utilizador"[31], o que também implica sensibilizar os utilizadores para as novas demandas digitais. Já quanto ao princípio da uma única vez, tal seria objeto de implementação em alguns serviços públicos sinalizados, figurando, pelo menos, como uma opção para o administrado[32]. Quanto aos princípios da confiança e da segurança, visaram demonstrar que as soluções interoperáveis e assentes nas novas tecnologias de informação a serem usadas pelas Administrações Públicas teriam de ser construídas assentes em padrões elevados de segurança e de privacidade, através de soluções atuais, apostando também em produtos associados à certificação eletrónica através do documento de identificação[33]. A transparência e a abertura seriam potenciadas pela possibilidade de os cidadãos e as empresas poderem gerir (pedindo alterações, apagamento, restrições, correções) os dados pessoais objeto de tratamento pelas Administrações Públicas[34]. Por último, no que diz respeito à observância do princípio da interoperabilidade por defeito, os Ministros assumiram o compromisso de "trabalhar nos quadros nacionais de interoperabilidade baseados no Quadro Europeu da Interoperabilidade (QEI), ainda que respeitando padrões relevantes nacionais, e aderir aos serviços públicos transfronteiriços do QEI"[35].

---

31 *Tallinn Declaration on e-Government at the ministerial meeting during the Estonian Presidency of the Council of the EU*, Talin, 6 de outubro de 2017, p. 3 (tradução livre).

32 *Tallinn Declaration on e-Government*, p. 3.

33 *Tallinn Declaration on e-Government*, p. 3.

34 *Tallinn Declaration on e-Government*, p. 3.

35 *Tallinn Declaration on e-Government*, p. 3 (tradução livre).

Nesta senda, o Índice de Digitalidade da Economia e da Sociedade (IDES) de 2018 – "índice compósito que sumaria os indicadores relevantes quanto à performance digital da Europa e que rastreia o progresso dos Estados-Membros quanto à sua competitividade digital"[36] – organiza-se em cinco vetores ou dimensões relativos a "Conetividade", "Capital Humano", "Uso de serviços de internet", "Integração de tecnologia digital" e "Serviços públicos digitais". No que diz respeito aos serviços públicos digitais, a Comissão Europeia concluiu que a Finlândia apresentava os indicadores mais elevados, seguida da Estónia, Dinamarca e Espanha. Neste contexto, o indicador relativo aos utilizadores de serviços de Administração Pública em linha mede "em percentagem, aqueles utilizadores da internet que precisam submeter formulários à Administração Pública"[37]. Portugal ocupa o décimo sexto lugar no Índice de 2018, fazendo "parte do grupo de países com desempenho médio"[38], estando acima da média europeia em termos de serviços públicos digitais. Para o efeito, quanto ao vetor relativo à utilização de serviços caracterizadores de uma Administração Pública em linha, nomeadamente quanto ao "nível de serviços concluídos em linha", a Comissão demonstrou que "Portugal [é] um dos líderes da UE a esse respeito", tendo mantido o seu percentual praticamente inalterado[39]. Contudo, concluiu-se que "esta situação pode explicar-se pela percentagem relativamente elevada da população com competências digitais insuficientes e que não utiliza a Internet ou apenas o faz raramente"[40].

---

36 Comissão Europeia, *Digital Economy and Society Index Report 2018 – Digital Public Services*, p. 2 (tradução livre).

37 Comissão Europeia, *Digital Economy and Society*, p. 3 (tradução livre).

38 Comissão Europeia, *O Índice de Digitalidade da Economia e da Sociedade (IDES) de 2018 – Relatório por País, Portugal*, *in* https://ec.europa.eu/digital-single-market/en/scoreboard/portugal [acesso: 28.1.2019].

39 Comissão Europeia, *O Índice de Digitalidade*, p. 10.

40 Comissão Europeia, *O Índice de Digitalidade*, p. 10.

Neste contexto, resulta evidente que, paralelamente, a União Europeia está determinada ao estabelecimento de uma oferta digital pública, desde que devidamente caracterizada por padrões elevados de proteção, nomeadamente dos dados pessoais dos administrados. Na realidade, os seus dados passam a estar integrados numa base de dados transfronteiriça a que têm acesso as Administrações Públicas de outros Estados-Membros mas também a instituição ou o órgão da União que materialmente é competente e que controla o sistema interativo de natureza transfronteiriça. Assim, coloca-se a questão de saber qual será efetivamente tal padrão de proteção, sobretudo quando se vivem tempos relativamente novos quanto à proteção de dados pessoais na União Europeia. Afinal, as Administrações Públicas nacionais dos Estados-Membros encontram-se sujeitas ao padrão de proteção decorrente da aplicação do Regulamento n.º 2016/679[41], mormente conhecido como Regulamento Geral sobre a Proteção de Dados (doravante RGPD). Por sua vez, as instituições e órgãos da União – chamados à colação pelo fenómeno da Administração Pública em linha por conta da implementação de soluções de interoperabilidade – encontram-se sujeitos ao recente Regulamento n.º 2018/1725[42], sucedâneo do Regulamento n.º 45/2001.

Cabe, portanto, refletir sobre tais instrumentos de proteção de dados numa perspetiva macro, baseando-se nas dificuldades decorrentes do fe-

41 Regulamento (UE) N.º 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

42 Regulamento (UE) n.º 2018/1725, do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE.

nómeno da interoperabilidade que explica e sedimenta a Administração Pública em linha e, bem assim, atentando aos desígnios de padrão mais elevado de proteção de dados pessoais na União Europeia.

3. A proteção de dados na União Europeia – os Regulamentos n.º 2016/679 (RGPD) e n.º 2018/1725

O RGPD, aplicável desde o dia 25 de maio de 2018, por força do disposto no seu artigo 99.º, n.º 2, determinou uma reforma significativa da proteção de dados pessoais no contexto da União Europeia, sendo capaz de promover a necessária conciliação entre as dimensões económicas em que assentou a aposta na revolução digital europeia – pautada, como vimos, pela implementação do Mercado Único Digital – e a proteção dos direitos fundamentais.

Assim, a proteção dos dados pessoais surge no RGPD, enquanto direito derivado da União, como "direito fundamental autónomo e de reconhecimento normativo próprio"[43], dando observância quer ao artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (doravante CDFUE)[44], quer ao artigo 16.º, n.º 1 do TFUE que patenteia tal desígnio jusfundamental, ao estabelecer que "[t]odas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito". Afinal, o

43 A. Silveira *et al.*, "A reforma do regime de proteção de dados pessoais e a sua implementação no ordenamento jurídico português", *in* R.G. Leal, A. Silveira, C.A. Cano (Eds.), *IV Seminário Internacional Hispano-Luso-Brasileiro sobre direitos fundamentais e políticas públicas*, Bubok editorial, pp. 27-44, p. 28.

44 Recorde-se, a propósito, que, com o Tratado de Lisboa, para além de a CDFUE assumir força juridicamente vinculativa, por força do artigo 6.º, n.º 1 do TUE, o direito fundamental à proteção dos dados pessoais, decorrente do artigo 8.º da CDFUE, também passa a fazer parte integrante do acervo de direito originário, na medida em que a CDFUE "tem o mesmo valor jurídico que os Tratados) vide, a propósito, redação do artigo 6.º, n.º 1 do TUE.

exercício das liberdades de circulação implicou um aumento da recolha, tratamento e circulação de dados pessoais. Ora, "o desenvolvimento da sociedade técnica da informação e os avanços da denominada economia digital aceleraram a necessidade de desenvolver um regime apto a, nas circunstâncias 4.0 em que vivemos, garantir a efetividade do direito fundamental à proteção dos dados pessoais"[45]. Esta realidade concretiza-se pelos impulsos legislativos do Parlamento Europeu e do Conselho, através do procedimento legislativo ordinário, conforme veiculado no artigo 16.º, n.º 2 do TFUE. Quer o RGPD, quer o Regulamento n.º 2018/1725 foram adotados em observância desta disposição.

Neste sentido, para efeitos do RGPD, entende-se como tratamento de dados pessoais, na aceção do artigo 4.º, n.º 2 do RGPD, "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meio automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição". Por sua vez, dados pessoais consubstanciam-se como a "informação relativa a uma pessoa singular identificada ou identificável", sendo "considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou um ou mais elementos específicos da identidade física, genética, mental, económica, cultural ou social dessa pessoa singular" (artigo 4.º, n.º 1 do RGPD). Tais definições conheceram redações idênticas e próximas no Regulamento n.º 2018/1725, aplicável às instituições e órgãos da União Europeia.

45 A. Silveira *et al*., *IV Seminário Internacional Hispano-Luso-Brasileiro*, p. 31.

Para a reflexão que nos ocupa, cabe-nos fazer considerações relativas, nomeadamente, ao âmbito material de aplicação do RGPD e do Regulamento n.º 2018/1725, bem como às atribuições do Comité Europeu para a Proteção de Dados e da Autoridade Europeia para a Proteção de Dados. Por fim, faremos incursões sintomáticas aos tribunais materialmente competentes para conhecer dos litígios emergentes de cada um dos Regulamentos.

Assim, determina o artigo 2.º do RGPD que este se aplica "ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados". Por sua vez, o n.º 2 do mesmo artigo explicita, de forma taxativa, um conjunto de matérias objeto de exclusão do âmbito de aplicação do RGPD: considera-se excluído o tratamento de dados pessoais que seja efetuado a) no exercício de atividades não sujeitas à aplicação do direito da União; b) pelos Estados-Membros no exercício de atividades relativas à Política Externa e de Segurança Comum [título V, capítulo 2 do Tratado da União Europeia (doravante TUE)]; c) por pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas; d) pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública[46]. Tais exclusões deverão ser lidas em conjugação com o artigo 23.º do RGPD que estabe-

46 O tratamento de dados pessoais para tais fins – investigação criminal e deteção e prevenção de infrações / ameaças à segurança pública – recebeu tratamento legislativo autónomo paralelo, por força da Diretiva n.º 2016/680. Para maiores desenvolvimentos, Diretiva (UE) n.º 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro n.º 2008/977/JAI, do Conselho. Para mais considerações e precisões, nomeadamente quanto à sua articulação com as limitações decorrentes do artigo 23.º do RGPD, A. Silveira *et al.*, *IV Seminário Internacional Hispano-Luso-Brasileiro*, pp. 36 e seguintes.

lece um regime de limitações à sua aplicação. Na realidade, determina-se que "[o] direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa" as seguintes situações: a) o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º, ou seja, os direitos conferidos ao titular dos dados; b) o alcance do artigo 34.º, que estabelece a obrigação de o responsável pelo tratamento comunicar uma violação ao respetivo titular dos dados pessoais; e c) o alcance do artigo 5.º do RGPD, relativo aos princípios gerais a que o tratamento de dados está sujeito. No entanto, a parte final do artigo 23.º, n.º 1 é claro a demonstrar que tais limitações apenas poderão ocorrer desde que se conduza um juízo de proporcionalidade para aferir se as mesmas respeitam a essência dos direitos e liberdades fundamentais e visam algumas das situações enunciadas nas suas alíneas.

Por sua vez, dispõe o artigo 2.º, n.º 3 do RGPD que "[o] Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98.º". Ora, este número antecipava o notório: a revisão relativa à proteção dos dados pessoais tinha sido pensada como algo transversal e a ser realizada em bloco. Na realidade, tal apenas tinha em vista um padrão mais elevado de proteção dos dados pessoais; para tal já apontava o Estudo de Avaliação do Regulamento n.º 45/2001, realizado pela *Ernst&Young*, a pedido da Comissão Europeia – Direção-Geral de Justiça, de maio de 2015[47].

47 Ernst & Young Associés e Ernst & Young Société d'Avocats, *Evaluation study on Regulation (EC) No 45/2001 – Full Report*, Maio de 2015, in https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51087 [acesso: 28.1.2019].

Nesta senda, verificou-se a necessidade de adaptar as normas do antigo Regulamento n.º 45/2001, relativo à proteção de dados perante as instituições, órgãos e organismos da União, aos novos padrões jusfundamentais que decorriam do RGPD. Por outro lado, havia uma necessidade de potenciar a livre circulação de dados na União Europeia – "revogando o Regulamento (CE) n.º 45/2001, o novo regulamento (que foi assinado e publicado no Jornal Oficial da UE), tem em vista alinhar-se com as normas existentes no moderno RGPD"[48]. Tal Regulamento estabelece, assim, as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais pelas instituições e pelos órgãos da União e estabelece regras sobre a livre circulação desses dados entre essas instituições e órgãos, ou entre essas instituições e órgãos e outros destinatários estabelecidos na União (artigo 1.º, n.º 1).

Na sequência do RGPD, este novo Regulamento – aplicável a partir do dia 12 de dezembro de 2019 pela Eurojust (nos termos do artigo 101.º, n.º 2) – confere direitos mais robustos aos titulares dos dados pessoais (incluindo o direito ao esquecimento, nos termos e para os efeitos do artigo 19.º) e especifica as obrigações dos responsáveis pelo tratamento (ou seja, as instituições e os órgãos da União). Do mesmo modo, logo no artigo 1.º, n.º 2 estabelece-se que o Regulamento tem em vista a proteção dos direitos e das liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

O seu âmbito de aplicação resulta, em termos positivos, do artigo 2.º, n.ºs 1 e 4 onde se estatui que "[o] presente regulamento aplica-se ao

48 Parlamento Europeu, *Legislative train Schedule: area of justice and fundamental rights – JD – Protection of individuals with regard to the processing of personal data by the union institutions, bodies and agencies and on the free movement of such data*, *in* http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-jd-processing-of-personal-data-by-the-union-institutions [acesso: 28.1.2019].

tratamento de dados pessoais por todas as instituições e todos os órgãos da União", que seja realizado "por meios total ou parcialmente automatizados e ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados". Excluem-se parcialmente do seu âmbito de aplicação os dados pessoais tratados por instituições e órgãos da União no âmbito da cooperação judiciária em matéria penal e policial (capítulos 4 e 5 do título V da parte III do TFUE)[49].

Por sua vez, também se exclui do seu âmbito de aplicação o tratamento de dados pessoais levados a efeito pela Europol e pela Procuradoria Europeia, mediante adaptação dos respetivos atos normativos[50] à luz do artigo 98.º do Regulamento. Para o efeito, o artigo 98.º estabelece uma necessidade de reexame, a ser realizada pela Comissão Europeia, a fim de aferir, até 30 de abril de 2022, se os atos normativos adotados são coerentes com os termos deste Regulamento, quais as divergências a suprir sob pena de redundarem em "fragmentação jurídica da legislação sobre a proteção de dados na União", podendo a Comissão apresentar propostas legislativas adequadas.

O Regulamento n.º 2018/1725 também não é aplicável ao tratamento de dados realizado pelas missões desenvolvidas no âmbito da Política Externa e de Segurança Comum (artigos 42.º, n.º, 43 e 44 do TUE).

---

49 O tratamento de dados pessoais, realizado por instituições e órgãos da União em sede de cooperação judiciária em matéria penal e policial, sujeita-se apenas à observância do artigo 3.º (relativo às definições) e do capítulo IX (artigos 70.º e seguintes) do Regulamento n.º 2018/1725.

50 A propósito da Europol, Regulamento (UE) n.º 2016/794, do Parlamento Europeu e do Conselho, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho; e a propósito da Procuradoria Europeia, o Regulamento (UE) n.º 2017/1939, do Conselho, que dá execução a uma cooperação reforçada para a instituição da Procuradoria Europeia.

Por sua vez, na senda do que já se havia verificado à luz do RGPD, o âmbito de aplicação do Regulamento n.º 2018/1725 também terá em mente as limitações decorrentes do artigo 25.º, onde se estabelece que "[o]s atos normativos adotados com base nos tratados ou, em matérias relacionadas com o funcionamento das instituições e dos órgãos da União, as regras internas estabelecidas por estes últimos podem limitar a aplicação":

- "dos artigos 14.º a 22.º", ou seja, as normas que estabelecem os direitos dos titulares dos dados;
- "dos artigos 35.º e 36.º", que dizem respeito à comunicação das violações ao titular dos dados e à confidencialidade das comunicações eletrónicas;
- "e do artigo 4.º, na medida em que as disposições deste artigo correspondem aos direitos e às obrigações previstos nos artigos 14.º a 22.º".

No entanto, para que tais limitações se possam efetivar, terá de ser conduzido um juízo de proporcionalidade atendendo a razões ponderosas elencadas nas alíneas do n.º 1 do artigo 25.º.

Posto isto, antevê-se um caminho articulado entre estas soluções legislativas derivadas mobilizáveis em sede de proteção de dados. Num âmbito que pressupõe o estabelecimento de serviços públicos digitais através de soluções de interoperabilidade, há que equacionar se tal propósito de alteamento da proteção de dados pessoais no contexto europeu poderá ser alcançado na prática e se os administrados, convidados a interagir digitalmente com as Administrações Públicas (funcional e organicamente europeias), serão capazes de sentir os seus direitos transversalmente observados. Na realidade, o RGPD vincula as Administrações

Públicas nacionais à sua observância, por força do artigo 4.º, n.º 7, na medida em que serão reputadas como responsáveis pelo tratamento; por sua vez, o Regulamento n.º 2018/1725 perspetiva as instituições e órgãos da União como responsáveis pelo tratamento, nos termos do artigo 3.º, n.º 8. A fim de evitar conflitos de competência – positivos e negativos –, há a necessidade de clara articulação entre a Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados e entre estes e as autoridades de controlo. Para o efeito, tal parece estar formalmente acautelado na medida em que o Comité é composto pelo diretor de uma autoridade de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados (artigo 68.º, n.º 3 do RGPD), constando, por sua vez, nas prerrogativas da Autoridade a participação nas atividades do Comité (artigo 57.º, n.º 1, k) do Regulamento n.º 2018/1725). Nesta senda, também é sua atribuição a realização de investigações sobre a aplicação do Regulamento n.º 2018/1725, nomeadamente com base em informações recebidas de outras autoridades de controlo ou de outras autoridades públicas. Da mesma forma, o RGPD estabelece, entre as atribuições do Comité, que lhe caberá, por iniciativa própria ou a pedido de um dos seus membros da Comissão, dirimir qualquer questão relativa à aplicação do RGPD e emitir diretrizes, recomendações e melhores práticas, a fim de incentivar a sua aplicação – artigo 70.º, n.º 1, e) do RGPD. Ainda nesta senda, compete à Autoridade Europeia cooperar com as autoridades nacionais de controlo, na medida do necessário, para o exercício das respetivas funções, em especial, através da partilha de informações relevantes e da resposta aos pedidos que lhe tenham sido apresentados (artigo 61.º do Regulamento n.º 2018/1725). Da leitura combinada dos dois normativos resulta clara uma pensada articulação entre as entidades mobilizáveis e, como tal, a possibilidade de dirimir problemas resultantes do tratamento de dados através de plata-

formas interoperáveis disponíveis quer para as Administrações Públicas nacionais, quer para as instituições ou os órgãos da União.

Assim, depois de dirimidas as questões inerentes aos respetivos âmbitos de aplicação, serão competentes, por um lado, o Tribunal de Justiça, quanto ao conhecimento de violações de dados pessoais pelas instituições e órgãos da União (artigo 64.º do Regulamento n.º 2018/1725) e, por outro, os tribunais nacionais, quanto às violações de dados pessoais decorrentes da atividade das autoridades públicas nacionais (artigos 78.º, n.º 3 e 79.º, n.º 2 do RGPD).

Neste cerne, cabe, por último, antecipar se estes dois normativos, num contexto de Administração Pública em linha potenciada pela adoção de plataformas e bases de dados interoperáveis, serão capazes de dar observância ao padrão mais elevado de proteção de dados pessoais.

4. O padrão mais elevado de proteção de dados pessoais – reflexões

Os desígnios económicos ditaram as primeiras sensibilidades da União Europeia em termos de proteção de dados pessoais que "surg[iram] como resposta à necessidade de fazer circular informações pessoais, consequência do funcionamento do mercado interno e do aumento do fluxo transfronteiriço de dados que acompanha a circulação de mercadorias, de pessoas, de serviços e de capitais"[51]. Se foi assim durante algum tempo, mais recentemente verificou-se um tendencial e inegável aumento do valor económico (e comercial) dos dados pessoais já que

51 C. Sarmento e Castro, "Anotação ao artigo 8.º", *in* A. Silveira e M. Canotilho (Coord.), *Carta dos Direitos Fundamentais da União Europeia Comentada*, Almedina, 2013, pp. 120 e seguintes, p. 121.

"à medida que o desenvolvimento tecnológico e digital se intensifica, aperfeiçoam-se os meios técnicos de recolha, renovando-se permanentemente o leque (cada vez mais ilimitado) de possibilidades de criação de valor económico dos dados recolhidos"[52]. Sob este desígnio, o Mercado Único Digital foi implementado, tendente a promover um aproveitamento das dimensões digitais e potenciando a economia na União Europeia, mas não desconsiderando o elevado grau de proteção dos direitos fundamentais neste domínio.

Ora, o direito fundamental à proteção de dados pessoais encontra-se inserido, na CDFUE, no capítulo relativo às liberdades, e de forma autonomizada relativamente ao direito à intimidade da vida privada e familiar (plasmado no artigo 7.º do mesmo normativo). Para a sua consagração como direito fundamental foram relevantes as influências decorrentes das tradições constitucionais comuns aos Estados-Membros[53], dos instrumentos de proteção de direitos humanos de caráter internacional e da atividade jurisprudencial a eles associadas. Assim, apesar de a Convenção Europeia dos Direitos do Homem não fazer referência expressa a tal direito, o Tribunal Europeu dos Direitos do Homem[54] foi-o recortando a partir dos termos do artigo 8.º daquela Convenção, que consagra o direito ao respeito pela vida privada e familiar, reconhecendo-lhe ínsita "uma especial vertente que impõe o respeito da privacidade em relação

52 A. SILVEIRA *et al.*, *IV Seminário Internacional Hispano-Luso-Brasileiro*, p. 31.

53 Veja-se, a propósito, as considerações feitas por CATARINA SARMENTO E CASTRO, Anotação ao artigo 8.º, pp. 120 e seguintes, sobretudo quando à autonomização do direito fundamental à proteção de dados pessoais relativamente à intimidade da vida privada e familiar em alguns ordenamentos jurídicos nacionais.

54 A propósito, Acórdãos (TEDH) Leander vs. Sweden, de 26 de março de 1987, processo n.º 9248/81; Amann vs. Swizerland, de 16 de fevereiro de 2000, processo n.º 27798/95; e Rotaru vs. Romania, de 4 de maio de 200, processo n.º 28341/95.

aos tratamentos de dados pessoais"[55]. Por sua vez, também foi relevante a Convenção 108 do Conselho da Europa[56] que estabelece um conjunto de princípios que influenciaram o quadro inerente à proteção de dados refletida na anterior Diretiva 95/46/CE[57].

Daqui se depreende que a sua consagração resultou, nestes parâmetros, das influências jusfundamentais recíprocas e comunicativas, explicáveis à luz do fenómeno da interconstitucionalidade[58]. Na União Europeia, "o bloco de jusfundamentalidade [...] congrega direitos fundamentais de distintas fontes: normas de proveniência europeia (constantes dos tratados constitutivos – e especialmente a CDFUE), normas de proveniência nacional (correspondentes às tradições constitucionais comuns aos Estados-Membros, isto é, constantes das Constituições nacionais), e normas de proveniência internacional"[59], nomeadamente a Convenção Europeia dos Direitos do Homem. No entanto, como bem nos foi alertando a doutrina autorizada[60], a aplicação concreta de normas de direitos fundamen-

---

55 C. Sarmento e Castro, *Carta dos Direitos Fundamentais*, p. 120.

56 Convenção 108 do Conselho da Europa, de 28 de janeiro de 1981, relativa à proteção das pessoas singulares no que diz respeito ao tratamento automatizado de dados pessoais.

57 Diretiva n.º 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, ora revogada pelo RGPD.

58 Para maiores desenvolvimentos, entre outros, J.J. Gomes Canotilho, *«Brancosos» e a interconstitucionalidade. Itinerários dos discursos sobre a historicidade constitucional*, Almedina, 2006.

59 A. Silveira, *Princípios de Direito*, p. 80.

60 A propósito, e para maiores incursões, M. Luísa Duarte, *União Europeia e Direitos Fundamentais – no espaço da internormatividade*, AAFDL, 2016; J.J. Gomes Canotilho, *"Brancosos" e Interconstitucionalidade*; P. Rangel, *O estado do Estado. Ensaios de política constitucional sobre justiça e democracia*, Dom Quixote, 2009; e J.J. Gomes Canotilho, Estado de direito e internormatividade, *in* A. Silveira (Coord.), *Direito da União Europeia e Transnacionalidade*, Quid Juris, 2010.

tais de distintas fontes revela-se complexa na medida em que acabam por revelar âmbitos sobrepostos de aplicação. No entanto, estamos em crer que, atenta «a lógica da interjusfundamentalidade que inspira o modelo de proteção dos direitos fundamentais na União, é expectável que o TJUE dê continuidade ao exercício de "concordância prática" que tem marcado a sua jurisdição integradora ao longo do tempo»[61]. À luz destas considerações, há que concretizar se a proteção de dados pessoais será potenciada à luz destes dois atos normativos – recorde-se, o RGPD e o Regulamento n.º 2018/1725 – e se a União Europeia será capaz de concretizar o *standard* mais elevado de proteção deste direito fundamental. Iremos ainda refletir se, neste contexto de interoperabilidade administrativa que também demanda o tratamento em linha de dados pessoais dos administrados entre as Administrações Públicas nacionais e as instituições e os órgãos da União, se, em caso de violações, os tribunais (orgânica e funcionalmente europeus) poderão continuar a operar como uma ponte de transição entre as ordens jurídicas nacionais e europeia a fim de dar cumprimento ao fenómeno da interconstitucionalidade vivificado neste contexto, promovendo a tutela mais efetiva do direito fundamental à proteção dos dados pessoais.

Tais interações reflexivas entre diferentes padrões de jusfundamentalidade conduziram a que o legislador da União consagrasse, no artigo 53.º da CDFUE, o princípio do "*standard* mais elevado de proteção"[62] "que deve ser compreendido como um princípio de preferência pela nor-

61 A. Silveira, *Princípios de Direito*, p. 82.

62 M. Canotilho, "Anotação ao artigo 53.º", *in* A. Silveira e M. Canotilho (Coords.), *Carta dos Direitos Fundamentais da União Europeia Comentada*, Almedina, 2013, pp. 606 e seguintes, p. 607.

ma mais favorável"[63] na medida em que nos casos em que seja passível de aplicação mais do que um dos padrões de jusfundamentalidade mobilizáveis, o artigo 53.º parece intuir que se aplicará aquele que ofereça uma proteção mais elevada ao titular do direito em causa numa dinâmica de influências mútuas e recíprocas entre ordenamentos jurídicos distintos. Tal disposição tem de ser lida em conjugação com o artigo 52.º, n.ºs 3 e 4 da CDFUE[64], já que estabelece que, à CDFUE, não fica vedada a possibilidade de conferir um padrão de proteção mais amplo do que o que decorre da proteção internacional de direitos humanos e, por identidade de razão, do que decorre das Constituições nacionais, numa lógica de tendencial superação mútua a que não é despiciendo o quadro normativo em análise nesta reflexão. Na realidade, os Regulamentos em apreço (RGPD e Regulamento n.º 2018/1725) têm em vista pontuar a proteção de dados pessoais como efetivo direito fundamental – para isso é contundente o argumento literal inerente aos primeiros considerandos de cada um dos normativos, que ovacionam o artigo 8.º da CDFUE. Acresce que, enquanto o Regulamento n.º 2018/1725 não havia sido adotado, vigorava a regra interpretativa decorrente do artigo 2.º, n.º 3 do RGPD que demandava que o anterior Regulamento n.º 45/2001 fosse adaptado aos princípios e regras do RGPD. Assim, apesar de representar uma difícil leitura e compatibilização, já se lançava, no próprio RGPD, as primeiras pedras para que o *standard* de proteção fosse igualado quer o tratamento se realizasse por autoridades públicas nacionais (e os demais responsáveis pelo tratamento, nos termos do RGPD), quer se realizasse por instituições e órgãos da União. Ora, num contexto em que a aposta

63 A. Silveira, *Princípios de Direito*, p. 83.

64 Para maiores desenvolvimentos e concretização, A. Silveira, Anotação ao artigo 52.º da CDFUE, *in* A. Silveira e M. Canotilho (Coords.), *Carta dos Direitos Fundamentais da União Europeia Comentada*, Almedina, 2013, pp. 590 e seguintes, p. 590.

digital passa pela partilha de dados e informações entre as autoridades nacionais e europeias, através de canais interoperáveis, tal preocupação redunda numa efetivação de um padrão de proteção jusfundamental evidentemente mais elevado, na medida em que se compatibilizam, por cima, os padrões de proteção das pessoas singulares – administrados – que interagem administrativamente com as autoridades nacionais e europeias através de componentes digitais. Acresce que, das enunciações antecedentes, resulta evidente que os conflitos de competência serão facilmente balizados pelo entrosamento – nos próprios órgãos – das autoridades competentes em matéria de proteção de dados. Como tivemos oportunidade de explicitar, quer o Comité Europeu para a Proteção de Dados, quer a Autoridade Europeia interagem entre si; das suas atribuições resulta evidente a necessidade de, a pedido ou por iniciativa própria, esclarecerem dúvidas quanto ao âmbito de aplicação de cada um dos Regulamentos; e, por último, há um acompanhamento próximo das atividades realizadas pelas autoridades nacionais de controlo, o que determinará que, na prática, o padrão de jusfundamentalidade também poderá ser mantido e, quiçá, alteado. Ora, tal *standard* elevado de proteção decorre de mecanismos do direito da União Europeia, cabendo, portanto, no seu âmbito de aplicação.

Aqui surge a nossa segunda reflexão tendente à criação da convicção de que se poderá promover uma elevação da proteção de dados no contexto da União Europeia: quando tais dinâmicas começam a ganhar lastro transfronteiriço – especialmente, se potenciadas à luz dos desígnios digitais ora encetados pela União Europeia, através do método e princípio da interoperabilidade administrativa –, surge a preocupação que se continue a promover uma tendencial aplicação uniforme do direito da União e, bem assim, uma interpretação harmoniosa dos seus termos. Assim, a proteção de dados pessoais, quer à luz do RGPD, quer do Regu-

lamento n.º 2018/1725, cai no âmbito de aplicação do direito da União – desde logo porque se tratam de atos normativos diretamente aplicáveis, nos termos do artigo 288.º do TFUE, conduzindo à tendencial uniformização do direito aplicado –, o que significa que, se dúvidas surgirem sobre a sua aplicação, tais merecerão articulação com a instituição capaz de as dirimir: o Tribunal de Justiça. Ora, o Tribunal de Justiça tem sido o motor da proteção jusfundamental na União – mesmo antes de a CDFUE ter assumido força juridicamente vinculativa, este tribunal foi deduzindo jurisprudencialmente a proteção de direitos fundamentais através da sua proclamação como princípios gerais de direito da União[65]. Como nos ensina Alessandra Silveira, "o TJUE converte os princípios gerais em válvulas de escape da tutela jurisdicional efetiva dos particulares"[66], cabendo quer a este tribunal, quer aos tribunais nacionais, quando aplicam direito da União, exercerem a proteção jusfundamental. Para o efeito, e a fim de evitar diferentes fundamentos decisórios e, concomitantemente, diferentes *standards* de proteção, há um mecanismo de "diálogo formal"[67] entre os tribunais nacionais e o Tribunal de Justiça que poderá sair indiretamente propiciado por conta da intervenção direta do Tribunal de Justiça à luz do Regulamento n.º 2018/1725: o reenvio prejudicial.

---

65 Mais recentemente, o Tribunal de Justiça voltou a contribuir para tal acervo jusfundamental, com os acórdãos BAWAG, de 25 de janeiro de 2017, processo n.º C-375/15 e Manni, de 9 de março de 2017, processo n.º C-398/15; e Nowak, de 20 de dezembro de 2017, processo n.º C-434/16. Para mais desenvolvimentos, Tribunal de Justiça da União Europeia, Relatório Anual 2017 – Atividade Judiciária, Luxemburgo, 2018, in https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/ra_2017_pt_web.pdf, [acesso: 29.1.2019], pp. 73 e seguintes.

66 A. Silveira, *Princípios de Direito*, pp. 78-79.

67 C. Timmermans, "Multilevel judicial co-operation", *in* P. Cardonnel, A. Rosas e N. Wahl (Eds.), *Constitutionalising the EU judicial system: Essays in honour of Pernilla Lindh*, Hart Publishing, 2012, p. 16.

O reenvio prejudicial é um mecanismo ao dispor dos tribunais nacionais, enquanto tribunais comuns da União Europeia, para demandarem, junto do Tribunal de Justiça, a interpretação / aferição de validade do direito da União Europeia tendente à resolução do caso *sub judice* (artigos 19.º do TUE e 267.º do TFUE). Como o próprio Tribunal de Justiça explicou aos tribunais nacionais, "[o] reenvio prejudicial é o mecanismo fundamental do direito da União Europeia, que tem por finalidade fornecer aos órgãos jurisdicionais dos Estados-Membros o meio de assegurar uma interpretação e uma aplicação uniformes deste direito em toda a União"[68], sem que tal represente qualquer relação de hierarquia entre o primeiro e os segundos[69]. Trata-se, assim, de "um instrumento de cooperação direta entre o Tribunal de Justiça e os órgãos jurisdicionais nacionais"[70].

Nesta senda, já nos pronunciamos sobre as potencialidades de o reenvio prejudicial ser capaz – ainda que não a título privativo – de assegurar a observância do padrão de direitos fundamentais expectável na União Europeia[71]. Neste contexto – e ainda que balizados à observância de um direito fundamental em específico, o direito à proteção de dados pessoais –, a realidade é que o reenvio prejudicial poderá continuar a alicerçar tal proteção mais audaz dos dados pessoais.

---

68 Tribunal de Justiça da União Europeia, *Recomendações à atenção dos órgãos jurisdicionais nacionais, relativas à apresentação de processos prejudiciais*, (2012/C 338/01), Luxemburgo, 6 de novembro de 2012, p. 1.

69 A. Dashwood *et al.*, *European Union Law*, 6.ª Edição, Hart Publishing, 2011, pp. 209 a 2010 e 216.

70 M.E. Martins de Nazaré Rodrigues, "Anotação ao artigo 267.º do TFUE", *in* M.L. Porto e G. Anastácio (Coords.), *Tratado de Lisboa Anotado e Comentado*, Almedina, 2012, p. 963.

71 Para maiores desenvolvimentos, J. Covelo de Abreu, "An approach to today's EU constitutionality control – understanding this EU interjurisdictional phenomenon in light of effective judicial protection", *UNIO – EU Law Journal*, Vol. 3, No. 2, Julho de 2017, pp. 104-124.

Por um lado, à luz do RGPD, determinam os artigos 78.º, n.º 3 e 79.º, n.º 2 que serão competentes os tribunais do Estado-Membro em cujo território se encontram, respetivamente, estabelecidas as autoridades de controlo ou o responsável pelo tratamento. Neste contexto, quando seja proposta uma ação nestes termos perante os tribunais funcionalmente europeus, e a estes se coloquem dúvidas relativas à interpretação ou à validade de disposições de direito da União mobilizáveis para a boa solução do litígio, tais tribunais deverão articular-se com o Tribunal de Justiça a fim de assegurar a interpretação e aplicação uniformes do direito da União e evitar fenómenos de fragmentação do direito aplicado.

No entanto, a jurisprudência do Tribunal de Justiça pode ganhar o relevo ainda mais marcante, decorrente quer da sua intervenção no âmbito do reenvio prejudicial, quer enquanto instância jurisdicional "competente para apreciar todos os litígios relacionados com o disposto" no Regulamento n.º 2018/1725, "incluindo as ações de indemnização" (artigo 64.º, n.º 1), como dos recursos interpostos contra as decisões da Autoridade Europeia para a Proteção de Dados e para impugnação das coimas aplicadas (artigo 64.º, n.ºs 2 e 3 do Regulamento n.º 2018/1725).

Da mesma forma, o artigo 58.º, n.º 4 do Regulamento n.º 2018/1725 determina ainda a possibilidade de a Autoridade Europeia para a Proteção de Dados submeter questões à apreciação do Tribunal de Justiça, nas condições previstas nos Tratados, para além de poder intervir em processos judiciais intentados junto do Tribunal de Justiça. Neste sentido, antevê-se aqui uma clara articulação entre a mencionada Autoridade e o Tribunal de Justiça que não será estranha à determinação do padrão de proteção dos dados pessoais. No entanto, na medida em que o Tribunal de Justiça intervém, enquanto órgão jurisdicional, para conhecer dos litígios emergentes do âmbito de aplicação do Regulamento n.º 2018/1725,

tal determinará que o acervo jurisprudencial aproveitável aos tribunais nacionais será alargado e estes poderão beneficiar da sua jurisprudência consolidada nestes termos. Acresce que as sensibilidades que serão suscetíveis de emergir nos litígios nacionais poderão ser coincidentes às que se colocam, em primeira linha, ao Tribunal de Justiça. Na realidade, as disposições de um e outro Regulamento, em sede de definições e de direitos reconhecidos aos titulares dos dados, são muito aproximadas, determinando que o Tribunal de Justiça e os tribunais nacionais possam estabelecer, entre si, um diálogo que vai para além do reenvio prejudicial, embora não esgote este mecanismo e que até intensifique as interações que, no seu cerne, já eram usuais. Deste modo, haverá uma nova dinâmica de interjurisdicionalidade[72] que não se esgotaria no reenvio prejudicial, mas que se continuaria a pautar por uma fecundação da produção jurisprudencial dos órgãos jurisdicionais nacionais pelas influências interpretativas do Tribunal de Justiça.

5. Notas conclusivas

A *internet* redefiniu a perceção das variadas dimensões da vida em sociedade, apresentando-se como um facto de emergência de novos desafios económicos a que a União Europeia não ficou indiferente, tendo-se empenhado nas dimensões digitais como um dos objetivos da Estratégia Europa 2020.

Para potenciar o desenvolvimento desta Agenda Digital para a Europa, a União apostou na emergência de um Mercado Único Digital no âmbito

72 Para maiores desenvolvimentos, J. Covelo de Abreu, *Tribunais nacionais e tutela jurisdicional efetiva: da cooperação à integração judiciária no Contencioso da União Europeia*, Almedina, 2019 (no prelo).

das suas competências partilhadas tendentes ao aperfeiçoamento do Mercado Interno. Afinal, a União chegou à conclusão de que tais desideratos tecnológicos e digitais acarretavam efeitos económicos inegáveis.

Assim, enquanto interesse público primário, o estabelecimento e desenvolvimento de um Mercado Único Digital foi acolhido pelos agentes políticos nacionais e europeus, tendo sido necessário fixar quais os interesses públicos secundários a serem prosseguidos na sua esteira. Tornou-se, então, evidente a necessidade de entrosar quer as Administrações Públicas nacionais (que, quando aplicam direito da União Europeia, atuam como Administrações Públicas funcionalmente europeias) e as instituições e órgãos da União na sua prossecução. Assim, o primeiro passo foi o de apostar no estabelecimento de serviços públicos que tivessem a capacidade de operar e interagir através de componentes digitais. O método aprioristicamente adotado foi o da interoperabilidade administrativa, alavancado pela adoção do Programa ISA[2]. Neste cerne, a interoperabilidade demanda que se criem meios de interação tecnológica e bases de dados comuns às Administrações Públicas dos diversos Estados-Membros e a sua ligação central à instituição ou ao órgão da União materialmente competente. Tal implicou a emergência de uma nova principiologia que se pautou, por um lado, pelo reaproveitamento de informações já facultadas pelos administrados em momentos anteriores – quer perante a mesma entidade pública, quer perante a sua congénere de outro Estado-Membro –, de acordo com o princípio da uma única vez; e pela necessidade de as interações serem, em princípio, feitas por via digital, entre os administrados e as autoridades públicas, de acordo com o princípio do digital por defeito. Neste seguimento, a interoperabilidade foi também elevada a princípio geral, de modo a poder ter o impacto

organizacional, semântico e técnico pretendido[73]. Com esta aposta nos serviços públicos digitais, desenvolveu-se o paradigma da Administração Pública em linha tendente à flexibilização, transparência e simplificação das relações entre administrados e as Administrações Públicas funcional e organicamente europeias, redundando numa redução de encargos administrativos. Tal arquétipo tem sido acompanhado por uma leitura numérica atualizada através do Índice de Digitalidade da Economia e da Sociedade que, em 2018, revelou que, quanto aos serviços públicos digitais, Portugal se encontrava acima da média europeia e que, ao nível dos serviços concluídos em linha, este mesmo Estado-Membro era um dos líderes (embora algumas falhas se pudessem explicar por uma população com competências digitais insuficientes).

Todos estes incrementos foram acompanhados por uma preocupação com um elevado padrão de jusfundamentalidade no que aos dados pessoais diz respeito. Para o efeito, foram adotados dois Regulamentos – o RGPD e o Regulamento n.º 2018/1725 – que adequaram normativamente as exigências de proteção de dados pessoais às novas demandas tecnológicas.

A partir deste estado da arte, coube uma reflexão aprofundada sobre o padrão de proteção daquele direito fundamental deles decorrente e a sua compatibilidade / uniformidade num contexto caracterizado por interações digitais permanentes entre as Administrações Públicas nacionais e as instituições e os órgãos da União que se encontram, respetivamente, sujeitas ao âmbito de aplicação de um e de outro ato legislativo.

Do périplo realizado, tornou-se manifesto que existe quadro normativo suficiente para que se estabeleçam articulações entre as autoridades

73 Para maiores desenvolvimentos, C.E. Jiménez-Gómez e M. Gascó-Hernández, *Achieving open justice through citizen participation and transparency*, Hershey, 2017, p. 160.