

Direitos do titular dos dados pessoais: o direito à portabilidade

GRAÇA CANTO MONIZ*

Resumo: Este texto analisa os direitos do titular de dados pessoais, destacando um novo direito consagrado no Regulamento (UE) 2016/679: o direito à portabilidade. Num primeiro momento debruçamo-nos, de forma sintética, sobre os direitos específicos do titular dos dados pessoais, conforme estão previstos no regulamento para depois apreciarmos os traços essenciais do direito à portabilidade. Veremos as suas dimensões fundamentais, uma individual e outra económica, as faculdades que confere, o âmbito material de aplicação e, por fim, afloramos algumas dificuldades da sua aplicação prática.

Palavras-chave: *Regulamento Geral sobre a Proteção de dados pessoais; titular dos dados; direitos específicos; portabilidade.*

Abstract: This article aims to analyze data subject's rights, focusing the new right to data portability. First it briefly looks at the data subject specific rights present at the Regulation (EU) 2016/679 and, secondly, it describes with detail the right to data portability, highlighting its key dimensions, one individual and the other economic, the claims it recognizes to the data subject, its material scope, and, lastly, some of the practical problems regarding portability's implementation.

Keywords: *General Data Protection Regulation; Data Subject; special rights; portability.*

* Doutoranda na NOVA Direito onde investiga o tema “A extraterritorialidade do Regime Geral de Proteção de dados pessoais”, membro do CEDIS – Centro de I & D sobre Direito e Sociedade da Faculdade de Direito da Universidade Nova de Lisboa e coordenadora do Observatório de Proteção de Dados Pessoais. Este artigo teve o apoio uma bolsa da Fundação para a Ciência e Tecnologia.

Introdução: a *jusfundamentalização* da proteção de dados pessoais na União Europeia

Em larga medida, a legislação sobre proteção de dados pessoais parte de um pressuposto geral: a posição de vulnerabilidade e de desvantagem estrutural das pessoas singulares numa sociedade marcada pela circulação de fluxos informacionais, de várias origens, com vários destinos e finalidades. A necessidade de institucionalizar meios de controlo do uso da informação pessoal, tendo em vista a tutela dos direitos e liberdades fundamentais, é anterior a fenómenos dos nossos tempos como o *Big Data*, a computação em nuvem ou a internet das coisas. Porém, o convulsivo contexto de digitalização da vida social a que vimos assistindo nas últimas décadas, incrementou a dispersão da informação pessoal dificultando, na prática, as possibilidades de conhecimento e controlo do seu titular. O imperativo da proteção de dados pessoais tem sido, justamente, assegurar esse conhecimento e controlo¹.

O compromisso da UE com este imperativo, renovado em 2010², tornou-se inequívoco desde a *jusfundamentalização* da proteção de dados pessoais. Não devemos ignorar que o ordenamento jurídico da UE, paredes meias com o direito ao respeito pela vida privada e familiar (art. 7.º da CDFUE) autonomizou o direito fundamental à proteção de dados pessoais, consagrado no art. 8.º daquele diploma e no art. 16.º do TFUE³. Sendo legítimas as dúvidas suscitadas sobre a autonomia destes dois direitos⁴, certo é que o direito à proteção de dados é concretizado, em legislação secundária, por uma cartilha de direitos específicos, previstos no RGPD, que outorgam ao

¹ Sobre a ideia do “controlo individual sobre os dados pessoais”, v., *inter alia*, LYNKEY, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015, pp. 177 e ss.

² Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, “Uma abordagem global da proteção de dados pessoais na União Europeia”, de 4 de novembro de 2010, p. 5 e Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, “Proteção da privacidade num mundo interligado. Um quadro europeu de proteção de dados para o século XXI”, de 25 de janeiro de 2012, p. 2.

³ Noutras latitudes a proteção de dados pessoais não goza deste estatuto, v. KUNER, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press, 2013, p. 63.

⁴ LYNKEY, Orla. *The Foundations of EU Data Protection Law*, cit., pp. 89 e ss.

titular dos dados⁵ as faculdades necessárias para participar e decidir sobre o destino dos seus dados pessoais.

Contudo, como tem sublinhado o TJ⁶, o direito à proteção de dados pessoais não é absoluto, devendo ser perspetivado em relação à função desempenhada na sociedade, exigindo-se uma ponderação com outros direitos fundamentais, em sintonia com o princípio da proporcionalidade⁷.

1. Os direitos específicos do titular dos dados pessoais

Assente num princípio liberal de autonomia deliberativa, a legislação de proteção de dados pessoais reconhece um lugar de relevo à vontade individual. De facto, um princípio nodal daquela é a *participação* do titular dos dados, o que, por um lado, lhe garante uma medida de *influência* nas operações de tratamento⁸ e, por outro, se reflete numa cartilha de direitos assegurados mesmo nos casos em que a licitude do tratamento não decorre do consentimento do titular dos dados. Este acompanhamento das operações de tratamento consubstancia um controlo individual sobre os dados pessoais, independentemente do fundamento jurídico do tratamento⁹.

⁵ A definição de “titular dos dados” e de “dados pessoais” encontram-se densificadas no próprio regulamento, no art. 4.º, n.º 1, onde se lê: “informação relativa a uma pessoa singular identificada ou identificável (“titular dos dados”); é 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 a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular”.

⁶ Acórdão do TJ, C-275/06, ECLI:EU:C:2008:54, *Promusicae*, de 29 de janeiro de 2008, a propósito do direito à proteção efetiva da propriedade intelectual.

⁷ Considerando 4 do RGPD.

⁸ BYGRAVE, Lee. *Data Protection Law. Approaching Its Rationale, Logic and Limits*. The Hague: Wolters Kluwer, 2003, pp. 63 e ss.

⁹ Commission Staff Working Paper, “Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)”, de 25 de janeiro de 2012, p. 53.

O RGPD herda da Diretiva 95/46¹⁰ este conjunto de direitos. Além de algumas novidades, a haver diferenças em relação à diretiva, residem não tanto no seu enunciado quanto nas particularidades e modalidades do seu exercício, detalhadamente expressas no art. 12.º, onde se prescreve o princípio da transparência das informações e das comunicações e as regras para o exercício destes direitos específicos, nomeadamente os prazos que vinculam o responsável pelo tratamento. Tal como na diretiva, estes encontram-se obrigados a adotar medidas adequadas para facilitar o exercício dos direitos do titular dos dados¹¹. Por outro lado, nota-se uma particular preocupação do legislador em relação a crianças¹². Em sintonia com o que dissemos sobre a natureza relativa do direito à proteção de dados pessoais, o direito da União ou dos Estados-Membros pode impor restrições a princípios específicos e a direitos individuais do titular, em face do imperativo da salvaguarda de interesses gerais, como a segurança do Estado entre outros. Naturalmente, estas restrições devem observar a CDFUE e a Convenção Europeia para a Proteção dos Direitos Humanos¹³. É também de salientar que a Autoridade Europeia para a Proteção de Dados criticou o art. 23.º do RGPD por consubstanciar uma ampliação do âmbito destas restrições¹⁴.

O objetivo da reforma de 2012, em matéria de direitos do titular dos dados foi duplo¹⁵: por um lado, o RGPD corrige as divergências nacionais de implementação da diretiva¹⁶, com ganhos significativos ao nível da segurança

¹⁰ Directiva 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, doravante “diretiva”.

¹¹ Nos termos do n.º 8 do art. 12.º a Comissão Europeia é competente para adotar atos delegados para determinar procedimentos-tipo para o exercício dos direitos individuais, deste modo eliminando divergências entre os Estados-Membros.

¹² Considerando 38 do RGPD.

¹³ Art. 23.º e considerando 73 do RGPD.

¹⁴ Autoridade para a Proteção de Dados, “Parecer sobre o pacote de reforma legislativa sobre a proteção de dados”, de 7 de março de 2012, p. 160.

¹⁵ Uma notável crítica aos objetivos da reforma encontra-se em KOOPS, B. “The Trouble with European Data Protection Law”, *International Data Privacy Law*, n.º 4, 2014, pp. 250 e ss.

¹⁶ Comissão Europeia, “Relatório da Comissão. Primeiro relatório sobre a implementação da diretiva relativa à proteção de dados 95/46/CE”, adotado a 15 de maio de 2003, p. 18. Disponível em: <https://www.cnpd.pt/bin/actividade/Pri_rel_implementaDIR.pdf> (acedido a 8/12/2017).

jurídica e da uniformização das garantias do titular dos dados na União¹⁷; por outro lado, reforçou a transparência das operações de tratamento, com reflexo nas obrigações que recaem sobre o responsável pelo tratamento¹⁸, proporcionando às pessoas singulares meios eficazes para assegurar que estão plenamente informadas quanto ao que sucede aos seus dados pessoais e facilitando o exercício dos seus direitos¹⁹.

1.1. O direito à informação

As informações sobre o tratamento devem ser fornecidas ao titular dos dados no momento da sua recolha (art. 13.º) ou, não sendo esta efetuada junto do titular, dentro de um prazo, dependendo das circunstâncias do caso (art. 14.º). Seja como for, o legislador prevê o conteúdo mínimo da informação a prestar, designadamente a identidade e contacto do responsável pelo tratamento, as finalidades do tratamento, o fundamento jurídico, os destinatários dos dados, a existência de um direito de acesso, retificação, de portabilidade e a (não) obrigatoriedade de responder às questões. O RGPD expande as categorias de informação a prestar com o fim de garantir um “tratamento equitativo e transparente”, assumindo particular importância a informação prestada sobre a “existência de decisões automatizadas, incluindo a definição de perfis” e “informações úteis relativas à lógica subjacente” dos perfis. Trata-se de um *direito à explicação* de decisões adotadas com base em algoritmos ou em sistemas automatizados e de inteligência artificial²⁰. De resto, do n.º 5.º do art. 14.º decorrem as exceções que dispensam o responsável pelo tratamento desta obrigação de informar.

¹⁷ N.º 2 do art. 288.º do TFUE sobre os efeitos do RGPD.

¹⁸ Em sintonia, aliás, com a tendência desta reforma de incutir maior responsabilidade (a ideia de *accountability*) no responsável pelo tratamento de dados pessoais. v. Comunicação da Comissão, “Proteção da privacidade num mundo”, cit., p. 7.

¹⁹ KUNER, Christopher. “The European Commission’s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law”, *Bloomberg BNA Privacy and Security Law Report*, de 6 de fevereiro de 2012, p. 10.

²⁰ HILDEBRANDT, Mireille. “The New Imbroglia – Living with Machine Algorithms”, *The Art of Ethics in the Information Society*. Amsterdam: Amsterdam University Press, 2016, pp. 55 e ss.

A prestação de informação e o acesso aos dados pessoais – que veremos de seguida – são condições indispensáveis para o titular dos dados exercer os demais direitos e efetuar as verificações necessárias no sentido de escrutinar e apreciar a licitude do tratamento, sujeita aos critérios do art. 6.º. Por isso, estes direitos foram descritos como o núcleo da proteção de dados pessoais, permitindo que os titulares identifiquem os dados sobre si, conhecidos por terceiros, os usos a que estão acometidos, a veracidade e qualidade dos mesmos e a licitude do tratamento²¹.

1.2. O direito de acesso

O âmbito deste direito, previsto no art. 15.º, não se restringe ao mero acesso aos dados. O titular pode obter, do responsável pelo tratamento, a confirmação da (in) existência do tratamento e um conjunto de informação suplementar que coincide, em larga medida, com aquela que deve constar da notificação ao abrigo do direito à informação: finalidades do tratamento, categorias de dados, destinatários, prazo de conservação, etc. Devemos salientar aqui a importância que assume, o direito à informação previsto no n.º 2 do art. 15.º, no caso de transferências para um país terceiro ou organização internacional. Sempre que os dados pessoais atravessam fronteiras do território da UE, há um risco acrescido de o titular não conseguir exercer os direitos que lhe assistem²².

Do ponto de vista prático, o titular dos dados deverá, em primeiro lugar, identificar a quem submeter o pedido de acesso (*i. e.*, o responsável pelo tratamento) e, em segundo lugar, determinar o procedimento a seguir para esse efeito (online, por correio normal ou formulário específico fornecido pelo responsável pelo tratamento, etc.)²³. Para facilitar este procedimento,

²¹ LORBER, Steven. “Data Protection and Subject Access Requests”, *Industrial Law Journal*, vol. 33, 2004, pp. 179 e ss. e L’HOIRY, Xavier e NORRIS, Clive. “The honest data protection officer’s guide to enable citizens to exercise their subject access rights: lessons from a ten-country European Study”, *International Data Privacy Law*, vol. 5, issue 3, 2015, pp. 190 e ss.

²² Considerando 116 do RGPD.

²³ Sobre esta componente prática v. L’HOIRY, X. e NORRIS, C. “The honest data protection officer’s guide to enable citizens to exercise their subject access rights: lessons from a ten-country European Study”, *cit.*, p. 192.

sempre que for possível, o responsável pelo tratamento deverá facultar um sistema seguro, por via eletrónica, que possibilite o acesso direto aos dados²⁴.

O acesso abre caminho a uma revisão do tratamento de dados pessoais, realizada diretamente pelo seu titular, para que conheça quais os dados tratados, verifique a qualidade e veracidade dos mesmos bem como a licitude do tratamento.

1.3. O direito de retificação e de apagamento

Verificando a qualidade dos dados e constatando a sua inexatidão ou incompletude, o titular tem o direito de os retificar, nos termos do art. 16.º. Diga-se também que, constatando a inexistência de um fundamento jurídico para o tratamento, sem prejuízo das outras situações dispostas no n.º 1 do art. 17.º, pode requerer o apagamento dos dados. Em bom rigor e verdade, este direito a ser esquecido é uma extensão do direito ao apagamento previsto na alínea b) do art. 12.º da diretiva²⁵. Porém, anotam-se três diferenças: (i) em face da “desarmonização” tolerada pela diretiva, o exercício do direito ao apagamento era mais fácil em alguns Estados-Membros²⁶; (ii) depois, é manifesta a preocupação com crianças que, quando consentem, não estarão totalmente cientes dos riscos inerentes ao tratamento²⁷; (iii) por fim, uma garantia adicional para o titular dos dados pessoais encontra-se plasmada no n.º 2 do art. 17.º, para dados *públicos*, sob a forma de uma obrigação de informação aos “responsáveis pelo tratamento efetivo dos dados” do pedido de apagamento. Antecipando as dificuldades técnicas do controlo da informação no ambiente online, o legislador introduziu critérios de razoabilidade, disponibilidade tecnológica e de custos, flexibilizando esta obrigação e aproximando-a de uma *obrigação de meios* e não de resultado. Esta moderada consagração do apagamento de dados explica-se à luz dos desafios colocados pela internet: multiplicação instantânea e ubiquidade

²⁴ Considerando 63 do RGPD.

²⁵ Acórdão do TJ, *Google Spain*, C-131/12, ECLI:EU:C:2014:317, de 13 de maio de 2014.

²⁶ A Comissão recebeu muitas queixas de indivíduos que não conseguiram retirar os seus dados pessoais dos fornecedores de serviços online, designadamente fotografias. v. Comunicação da Comissão, “Uma abordagem global”, cit., p. 7.

²⁷ Considerando 65 do RGPD.

de informação, de difícil controlo em termos técnicos e em relação ao conteúdo²⁸. Por outro lado, é uma resposta do legislador à tendência de travar, em sintonia com o TJ²⁹, a retenção de dados pessoais³⁰.

1.4. O direito à limitação do tratamento

Ao abrigo da diretiva, o titular dos dados dispunha do direito de bloquear os dados pessoais³¹. Uma faculdade semelhante encontra-se no art. 18.º através de uma restrição³² das operações de tratamento, nos casos enumerados no n.º 1. Em certa medida, poderá assumir uma natureza *cautelar* bastante útil enquanto o titular dos dados pondera uma estratégia de defesa judicial³³.

O responsável pelo tratamento deverá indicar de forma bem clara, no sistema informático, que o tratamento daqueles dados se encontra restringido, através da “inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro³⁴” podendo, nos termos do considerando 67, socorrer-se de “métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados”. O efeito desta limitação não tem implicações na conservação dos dados,

²⁸ ZANFIR, Gabriela. “The right to data portability in the context of the EU data protection reform”, *International Data Privacy Law*, vol. 2, issue 3, 2012, p. 8.

²⁹ Acórdão do TJ, C-293/12 e C-594/12, ECLI:EU:C:2014:238, *Digital Rights*, de 8 de abril de 2014.

³⁰ WARNER, Jeremy. “The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps”, *University Ottawa Law and Technology Journal*, vol. 2, 2005, p. 75.

³¹ Alínea b), do art. 12.º da diretiva.

³² DE HERT, Paul e PAPA KONSTANTINOY, Vangelis. “The new General Data Protection Regulation: Still a sound system for the protection of individuals?”, *Computer Law & Security Review*, vol. 32, 2016, Southampton, pp. 189 e ss.

³³ *Idem*, p. 189.

³⁴ N.º 3, do art. 4.º do RGPD.

mas afeta todas as demais operações de tratamento que só podem ser realizadas, excecionalmente, nas situações previstas no n.º 2 do art. 18.º.

1.5. O direito de oposição

O titular dos dados pessoais goza, nos termos do art. 21.º, do poder de se opor ao tratamento de dados, em qualquer momento, por razões preponderantes e legítimas relacionadas com a sua situação particular. Sendo um reconhecimento do direito à autodeterminação, por um lado, o seu exercício não é absoluto – com a exceção dos tratamentos para efeitos de comercialização direta³⁵ – e, por outro, a sua aplicação não é geral. Desde logo, depende do *juízo de ponderação* entre as “razões imperiosas e legítimas” para o tratamento, invocadas pelo responsável, e os “interesses, direitos e liberdades do titular dos dados”. Depois, a previsão legal inclui apenas quatro situações determinadas pelos fundamentos jurídicos do tratamento conforme as alíneas e), f) e o n.º 4 do art. 6.º.

O tratamento de dados para efeitos de comercialização direta é autonomizado nos n.º 2 e 3 do art. 21.º, tal como o tratamento para fins de investigação científica ou história ou para fins estatísticos, no n.º 6 do art. 21.º. Compreende-se esta diferenciação e flexibilização de regimes, já que a comercialização direta se enquadra no ambiente de ubiquidade informacional contemporâneo e os tratamentos de investigação científica e fins semelhantes gozam de um regime legal específico, como se depreende do considerando 156³⁶.

1.6. Decisões individuais e automatizadas

A criação de perfis, incluída na categoria das decisões automatizadas, constitui um tipo de tratamento de dados pessoais destinado a avaliar determinados aspetos da personalidade do titular dos dados ou a analisar e/ou prever a sua capacidade profissional, situação financeira, localização,

³⁵ N.º 2 e 3 do art. 21.º do RGPD.

³⁶ HERT, Paul e PAPAΚONSTANTINOY, Vagelis. “The new General Data Protection Regulation: Still a sound system for the protection of individuals?”, cit., p. 189.

saúde, preferências pessoais, fiabilidade ou comportamento³⁷. O art. 22.º baseia-se no anterior art. 15.º, da diretiva, e na recomendação do Conselho da Europa sobre a criação de perfis³⁸, ensaiando uma inversão numa tendência, registada em processos decisórios das organizações, para a tomada de decisões exclusivamente com base em perfis e sem o conhecimento do titular dos dados. A criação de perfis é um tema que tem suscitado acesos debates: os apologistas da proteção de dados destacam os riscos decorrentes de processos decisórios automatizados; já os seus defensores apontam-lhe os méritos que se sobrepõem àqueles riscos e que, em todo o caso, podem ser mitigados e controlados³⁹. Também se tem dito que o problema central não é a definição de perfis *per se* mas a falta de informação acerca da lógica algorítmica que desenvolve esses perfis e afeta o titular dos dados⁴⁰. Nessa medida, o RGPD não proíbe esta prática, mas propõe-se prevenir riscos decorrentes de uma decisão alcançada *sem qualquer intervenção humana*. Daí que se reconheça ao titular dos dados o direito a não ficar sujeito a uma decisão (i) tomada exclusivamente com base num tratamento automatizado, incluindo a definição de perfis e que (ii) produza efeitos na sua esfera jurídica ou que o afete significativamente. Assim, o titular dos dados tem direito a obter a intervenção humana, a expressar o seu ponto de vista e a obter uma explicação sobre a lógica da decisão, podendo sindicá-la.

Como noutros casos, este não é um direito geral e absoluto, sendo o seu campo de aplicação determinado em função do fundamento jurídico invocado para o tratamento dos dados, com se depreende do n.º 2, do art. 22.º do RGPD. Porém, o responsável pelo tratamento deverá sempre,

³⁷ A definição encontra-se no n.º 4 do art. 4.º do RGPD. Sobre os problemas que coloca, v. *inter alia*, HILDEBRANDT, Mireille e GUTWIRTH, Serge (eds.). *Profiling the European Citizen. Cross-Disciplinary Perspective*. London: Springer, 2008, pp. 17 e ss.

³⁸ Conselho da Europa, “Recommendation of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling”, de 23 de novembro de 2010. Disponível em: <<https://wcd.coe.int/ViewDoc.jsp?p=&id=1929429&Site=CM&direct=true>> (acedido a 8/12/2017).

³⁹ DE HERT, Paul e PAPA-KONSTANTINOY, Vagelis. “The new General Data Protection Regulation: Still a sound system for the protection of individuals?”, p. 189.

⁴⁰ No mesmo sentido, v. Autoridade Europeia para a Proteção de Dados, “Parecer 3/2015, A grande oportunidade da Europa. Recomendações da AEPD sobre as opções da UE para a reforma da proteção de dados”, de 28 de julho de 2015. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_pt.pdf> (acedido a 8/12/2017).

pelo menos, adotar “medidas adequadas” para salvaguardar os direitos e liberdades fundamentais, designadamente a intervenção humana e a participação do visado no processo decisório e na sua contestação (art. 22.º, n.º 2).

1.7. Reclamações e recursos judiciais

Para terminar esta explicação perfunctória sobre os direitos do titular dos dados, há que dizer que o titular dos dados pode apresentar uma *reclamação* a uma autoridade de controlo, designadamente no Estado-Membro da sua residência habitual⁴¹. Tem também o direito a intentar uma *ação judicial*, nos termos do art. 47.º da CDFUE, peticionando a violação dos direitos que lhe são conferidos pelo RGPD pelo responsável pelo tratamento ou subcontratante ou, ainda, se a autoridade de controlo não responder a uma reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as iniciativas necessárias para proteger os seus direitos⁴².

O art. 82.º prevê também o direito de indemnização. O responsável pelo tratamento ou o subcontratante devem reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o RGPD.

2. O direito à portabilidade dos dados pessoais

Inicialmente, “portabilidade” era um termo exclusivamente usado nas discussões entre os entusiastas da tecnologia⁴³. Nos dias de hoje, representa uma nova geração de conceitos acolhidos na gramática jurídica da proteção de dados pessoais. O debate sobre a portabilidade gira à volta dos mecanismos de mobilização de categorias de informação transmitida para o ambiente online, entre diferentes sítios da internet, como listas de

⁴¹ Art. 77.º do RGPD.

⁴² Considerandos 141 e ss. e arts. 78.º e 79.º.

⁴³ Existem vários tipos de portabilidade noutras áreas, v. G29, “Guidelines on the right to data portability”, adotadas a 13 de dezembro de 2016 e revisto no dia 5 de abril de 2017. Desenvolvendo as origens da portabilidade, v. VAN DER AUWERMEULEN, Barbara. “How to attribute the right to data portability in Europe: A comparative analysis of legislations”, *Computer Law & Security Review*, vol. 33, 2017, pp. 57 e ss.

contactos ou endereços de email⁴⁴. Acontece também que, há medida que se banalizou a utilização da computação em nuvem, o interesse neste instituto foi crescendo⁴⁵ até a um recente apelo à intervenção dos Estados na criação de políticas públicas uniformes para estimular a interoperabilidade e portabilidade dos serviços de computação em nuvem⁴⁶.

Mas a portabilidade é também – e sobretudo – uma “porta de entrada” no ambiente digital para o controlo do utilizador e titular de dados⁴⁷. Com a tendência para a digitalização das atividades humanas e interações sociais, há quem proponha que os dados pessoais, sobretudo quando combinados através de técnicas de *data mining*, constituem uma continuação da personalidade individual no mundo digital, suscitando problemas complexo ao direito⁴⁸. Outros, mais céticos, invocam a incapacidade do utilizador para, num ambiente já bastante complexo, acompanhar e controlar as transmissões dos seus dados entre serviços e a falta de transparência destas operações, além de preocupações com a segurança e, cada vez mais, com o roubo de identidade⁴⁹. Em qualquer caso, consagrada no art. 20.º, a portabilidade é uma das novidades do RGPD.

⁴⁴ DE HERT, Paul e PAPA KONSTANTINO, Vagelis. “The new General Data Protection Regulation: Still a sound system for the protection of individuals?”, cit., p. 189.

⁴⁵ O G29 define a “computação em nuvem” como o “conjunto de tecnologias e modelos de serviços centrados na utilização e fornecimento via Internet de aplicações informáticas, de capacidade de tratamento e armazenamento e de espaço de memória”. Existe, nos dias de hoje, um consenso alargado sobre as implicações da computação em nuvem para a proteção de dados pessoais. Se, por um lado, as normas de proteção de dados poderão, até certo ponto, dificultar a utilização e o desenvolvimento deste tipo de serviços, por outro lado, a computação em nuvem evidencia limitações nos esquemas lógicos da proteção de dados. Esta dificuldade foi reconhecida pelo G29 e por algumas autoridades de supervisão de proteção de dados pessoais, v. “Parecer 5/2012 sobre Computação na Nuvem”, de 1 de julho de 2012.

⁴⁶ ZANFIR, Gabriela. “The right to data portability in the context of the EU data protection reform”, cit., p. 3.

⁴⁷ Autoridade Europeia para a Proteção de Dados, Parecer 3/2015, cit., pp. 3 e ss.

⁴⁸ Gabriela Zanfir apela, por exemplo, à incorporação do conceito jurídico de personalidade digital, *The right to Data*, cit., pp. 3 e 13, tal como ROSENDAAL, Arnold. *Digital Personae and Profiles, in Law: Protecting Individuals Rights*. Online Contexts, Wolf Legal Publishers, 2013.

⁴⁹ VAN DER AUWERMEULEN, Barbara. “How to attribute the right to data portability in Europe: A comparative analysis of legislations”, cit., p. 60.

2.1. Ratio: *dimensão individual e económica*

Percebe-se que a dimensão preponderante da portabilidade seja de natureza *individual*, situando-se o seu objetivo imediato na perspetiva do titular dos dados, na sua capacitação, no reforço do controlo sobre os seus dados no ambiente digital ou no “ecossistema de dados⁵⁰”. Este direito vem criar uma ferramenta de *autogestão* para o titular determinar os destinos da informação sobre si, de acordo com a sua vontade e os seus interesses, assemelhando-se por isso a uma *extensão do exercício efetivo da manifestação e revogação do consentimento*⁵¹. A portabilidade permite-lhe reajustar o equilíbrio da relação, estruturalmente desigual, entre o responsável pelo tratamento/prestador do serviço e o titular dos dados, posicionando o segundo no lugar de mediador dos fluxos de dados que lhe digam respeito. Em cenários complexos, como a computação em nuvem, o titular dos dados permanecerá minimamente no controlo da informação sobre si, o que, seguramente, tem impacto na confiança depositada nestes serviços, elemento essencial de uma economia digital⁵².

Acresce, também, a importante *dimensão económica* da portabilidade. A intenção de eliminar obstáculos à circulação de dados pessoais na UE continua a ser um dos objetivos do RGPD⁵³, pelo que a simplificação da transmissão direta de dados pessoais entre responsáveis pelo tratamento cria condições para facilitar os fluxos de dados e para assegurar e estimular a concorrência entre responsáveis pelo tratamento, prestadores de serviços online, de computação em nuvem e para promover a confiança na economia digital⁵⁴. Note-se que a Comissão Europeia fundamentou a introdução deste direito com a necessidade de contornar as dificuldades de transmitir dados pessoais entre aplicações ou serviços, dando nota da

⁵⁰ G29, *Guidelines on the right*, cit., pp. 3 e ss.

⁵¹ DE HERT, Paul e PAPA-KONSTANTINOY, Vagelis. “The new General Data Protection Regulation: Still a sound system for the protection of individuals?”, cit., p. 189.

⁵² De acordo com a Comissão europeia, só 12% dos Europeus que utilizam serviços online se sentem completamente seguros a fazer transações online. v. COMISSÃO EUROPEIA, “Digital Agenda for Europe”. Disponível em: <http://eige.europa.eu/resources/digital_agenda_en.pdf> (acedido a 8/12/2017).

⁵³ Considerando 10 do RGPD.

⁵⁴ VAN DER AUWERMEULEN, Barbara. “How to attribute the right to data portability in Europe: A comparative analysis of legislations”, cit., pp. 59 e 60.

sua importância enquanto fator de competitividade, como foi evidente noutros segmentos de mercado, como a portabilidade do número no setor das telecomunicações⁵⁵. Aliás, é neste contexto que situamos a discussão em torno da possibilidade de a Comissão reagir a uma situação de abuso de posição dominante por empresas que limitem os seus clientes a transferir os dados para outros prestadores⁵⁶.

Por outro lado, é hoje inegável que os dados pessoais assumem um valor económico enriquecendo o serviço prestado e permitindo adequar a oferta às necessidades do cliente e a oferta de serviços de melhor qualidade⁵⁷. Desta situação nasce um risco de *lock-in* a um certo fornecedor ou serviço que se recusa a fornecer os dados pessoais para reutilização⁵⁸, justificada em limitações técnicas e nos custos à mobilidade e transmissão dos dados. O controlo da reputação dos utilizadores de leilões online, i. é, da acumulação dos resultados das suas transações, evidenciado num caso que envolveu o eBay, é um exemplo do bloqueio à concorrência neste tipo de serviços⁵⁹. É que qualquer limitação à portabilidade dos dados e à

⁵⁵ Commission Staff Working Paper, Impact Assessment, cit., p. 28. Uma ideia reforçada pelo Comissário para a Concorrência, em 2012, v. “Competition and Personal Data Protection”. Disponível em: <http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm> (acedido a 8/12/2017).

⁵⁶ GRAEF, Inge; VERSCHAKELEN, Jeroen e VALCKE, Peggy. “Putting the right to data portability into a competition law perspective”, *Annual review. The journal of the Higher School of Economics*, 2013, pp. 53 e ss. Afastando esta hipótese, VAN DER AUWERMEULEN, Barbara. “How to attribute the right to data portability in Europe: A comparative analysis of legislations”, cit., pp. 61 e ss.

⁵⁷ O que se nota, com particular acuidade, nas indústrias do *Quantified Self* e da *Internet of things*, exemplos que espelham os benefícios (e os riscos...) do cruzamento de dados pessoais sobre os diferentes aspetos das nossas vidas, como a atividade física, o consumo calórico, permitindo uma radiografia completa e precisa sobre a vida do visado, resumida num único ficheiro, v. G29, *Guidelines*, cit., p. 5.

⁵⁸ “Internet social networks operate for the time-being as closed gardens for their users: once in they enjoy all (free) functionalities, but they may never leave”, v. DE HERT, Paul e PAPA-KONSTANTINOU, Vagelis. “The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals”, p. 190 e VAN DER AUWERMEULEN, Barbara. “How to attribute the right to data portability in Europe: A comparative analysis of legislations”, cit., pp. 57 e ss.

⁵⁹ PIKER, Randal. “Competition and Privacy in the Web 2.0 and the Cloud C”, *Coase-Sandor Working Paper Series in Law and Economics*, 2008, p. 9.

interoperabilidade dos sistemas dificulta a migração dos dados entre serviços e, por conseguinte, restringe a faculdade de escolha do consumidor. Por fim, com base em algumas experiências europeias, acredita-se que o controlo e a partilha de dados pelo seu titular dará origem a novos modelos de negócio, estimulando a inovação⁶⁰.

2.2. *Faculdades: receber e transmitir*

O direito à portabilidade reconhece ao titular duas faculdades: a de receber um conjunto de dados pessoais e a de transmitir esses dados entre responsáveis pelo tratamento. Trata-se, antes de mais, do direito a receber um subconjunto de dados pessoais⁶¹, armazenar esses dados num dispositivo privado, sem necessariamente se seguir uma transmissão imediata para outro responsável pelo tratamento. Assim se abrangem não só as situações em que o titular pretende transferir todos os seus dados para outro fornecedor como, também, os casos em que pretende assegurar a interoperabilidade, por exemplo, entre várias “nuvens” que utiliza. Aproximando-se do direito de acesso é, na verdade, mais do que isso: é o seu complemento⁶².

A especificidade da portabilidade é a de oferecer uma ferramenta prática para o titular gerir e reutilizar os dados que lhe digam respeito, de acordo com a sua vontade e interesses⁶³. Daí a importância de cumprir as características técnicas enunciadas no n.º 1: “formato estruturado”, “uso corrente” e “leitura automática”. É que não se pretende apenas facultar o

⁶⁰ G29, *Guidelines*, cit., p. 5. Apontam-se as experiências como o MiData no Reino Unido e a MesInfos/SelfData, pela FING, em França.

⁶¹ Veremos que a portabilidade não abrange todos os dados pessoais do titular dos dados mas apenas um certo tipo de dados, v. G29, *Guidelines*, cit., p. 4.

⁶² Na proposta do Parlamento, encontravam-se fundidos num só artigo, o art. 15.º v. Parlamento Europeu, “Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (GDPR)”, 2012. Disponível em: <<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212>> (acedido a 8/12/2017).

⁶³ G29, *Guidelines*, cit., pp. 4 e 5.

acesso aos dados como, ainda (e sobretudo), possibilitar a sua utilização subsequente e agilizar um controlo efetivo⁶⁴.

A segunda faculdade, “o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir”, foi amplamente disputada nas negociações entre Comissão, Parlamento e Conselho. Inicialmente, a proposta da Comissão reconhecia o direito à transferência *direta* entre os responsáveis pelo tratamento, sem sujeição a nenhuma condição, algo que foi rejeitado pelo Parlamento, que restringiu a transferência *direta* apenas aos casos em que tal seja “tecnicamente possível⁶⁵”. Assim, os dados podem ser transmitidos ao titular ou a outro responsável pelo tratamento, sendo que o G29 propôs para esse efeito algumas soluções, como um servidor SFTP, uma WebAPI ou um WebPortal⁶⁶.

2.3. Âmbito material de aplicação

O RGPD não consagra um direito *geral* à portabilidade⁶⁷. Em rigor, de acordo com o art. 20.º, o seu âmbito material de aplicação depende de um conjunto de condições cumulativas relacionadas com o *tipo* de dados, com o *fundamento jurídico* que enquadra o tratamento e com o *tipo* de tratamento. Uma primeira limitação, particularmente exigente, quanto ao *tipo* de dados abrangidos pela portabilidade: apenas aqueles que “digam respeito” ao titular e que este “tenha fornecido”, com conhecimento e de forma ativa, como a informação pessoal descarregada numa rede social ou preenchida num formulário online. Há, pois, que ter presente que, por exemplo, não são de excluir os dados pseudonimizados já que podem ser relacionados

⁶⁴ O G29 dá vários exemplos: o titular dos dados pretende recuperar a sua playlist de um serviço de *streaming* de música; a sua lista de contactos da aplicação do *webmail* para criar e preparar uma lista de casamento; pretende aceder ao seu historial de compras de um cartão de fidelização ou avaliar a sua pegada de ecológica, v. *Ibidem*.

⁶⁵ Exemplificando, a proposta inicial, que também era especificamente vocacionada para as redes sociais, reconhecia a um utilizador do Facebook o direito de pedir que o Facebook transferisse diretamente para o Google + os seus dados, sem que o titular tivesse de os descarregar para posteriormente os carregar no Google +.

⁶⁶ G29, *Guidelines*, cit., p. 16.

⁶⁷ Considerando 68 e art. 20.º, n.º 3, do RGPD.

com o seu titular⁶⁸. Por outro lado, o G29 recomenda uma interpretação ampla em torno da expressão “dados pessoais que digam respeito ao titular” de modo a abranger, nos dados “portáveis”, informação sobre terceiros, mas neste caso apenas quando o pedido de portabilidade seja para fins pessoais⁶⁹.

Sabendo que os responsáveis pelo tratamento, sobretudo os prestadores de serviços online, não tratam apenas informação que é “fornecida” pelo utilizador, analisando-a também para gerar novo *conhecimento* sobre o titular, colocam-se dúvidas quanto à interpretação a dar à expressão “dados que o titular tenha fornecido”. A este propósito, o G29 identifica duas categorias de dados “fornecidos pelo titular”: (1) os dados ativos e conscientemente transmitidos por si e (2) os dados “observados”, i. é, “fornecidos” pelo titular por via da sua utilização do serviço, plataforma ou aparelho⁷⁰. Na primeira categoria, inserem-se os endereços de email, os nomes de utilizador, a idade, ficheiros descarregados, atualizações de estados, fotografias, etc. Na segunda categoria, o histórico de pesquisas, os dados de tráfego, os dados de localização e dados em bruto, como o batimento cardíaco registado num aparelho de fitness.

Entende também aquela entidade, com base num critério de *origem*, que os dados gerados pelo responsável pelo tratamento com base nos dados fornecidos pelo titular, tais como a criação de um perfil de saúde ou de crédito, um processo de recomendação, a categorização do utilizador, resultados algorítmicos, um perfil de crédito e outro tipo de perfis⁷¹ ou o resultado de uma avaliação sobre a saúde do utilizador⁷², são excluídos da portabilidade. São dados *inferidos* e dados *derivados*, gerados pelo responsável pelo tratamento, a partir dos dados “fornecidos pelo titular”. Ou seja, para efeitos do direito à portabilidade, os dados resultantes da mera *observação* do comportamento e atividade do titular distinguem-se dos dados pessoais

⁶⁸ N.º 2, do art. 11.º do RGPD e G29, *Guidelines*, cit., p. 7.

⁶⁹ Como acontece nos registos de transações bancárias ou nos registos telefónicos, que incluem transações e chamadas recebidas por terceiros. Adiante voltaremos a aflorar este aspeto.

⁷⁰ G29, *Guidelines*, cit., p. 8.

⁷¹ G29, *Guidelines*, cit., p. 10.

⁷² Note-se, porém, que a exclusão do âmbito da portabilidade não exclui a aplicação de outros direitos, como o direito previsto no art. 22.º do RGPD.

criados pela *análise* desse comportamento. Se, por um lado, esta distinção é melindrosa em relação a modelos de negócio dependentes dos dados pessoais “fornecidos” pelo titular, como sucede no *Online Fashion Advisor*⁷³ ou com os avatares criados em jogos online como o *World of Warcraft* e o perfil de vendedor em sites de leilões online⁷⁴; por outro lado, restringue os dados que o utilizador por exigir do prestador de serviços, evidente num exemplo da *internet of things* relativo ao aquecimento de um casa: o titular dos dados pode requerer o rastreamento dos movimentos de ocupação da casa, detetados por um termostato inteligente, mas não o horário algoritmicamente determinado para aquecer a casa⁷⁵.

No que diz respeito ao *fundamento jurídico*, a portabilidade, associada como se viu à vontade individual e à autodeterminação, é aplicável somente quando o fundamento é o *consentimento* ou o *cumprimento* de um contrato⁷⁶. Exemplificando, os títulos dos livros comprados numa livraria online ou a lista de músicas num serviço de *streaming* são exemplos de dados pessoais tratados com base no cumprimento de um contrato⁷⁷. Tal não exclui que, em termos de boas práticas, a portabilidade seja implementada quando o fundamento jurídico seja outro⁷⁸. Exclui-se, isso é certo, a portabilidade nos casos em que uma instituição financeira trate dados pessoais no âmbito de uma obrigação jurídica, por exemplo para o efeito de prevenção e deteção de lavagem de dinheiro e outros crimes financeiros⁷⁹. Já nos casos de

⁷³ VAN DER AUWERMEULEN, Barbara. “How to attribute the right to data portability in Europe: A comparative analysis of legislations”, cit., p. 61.

⁷⁴ *Idem*, p. 70.

⁷⁵ URQUHART, Lachlan; SAILAJA, Neelima e MCAULEY, Derek. “Realising the right to data portability for the domestic Internet of things”. *Personal and Ubiquitous Computing Economics*. London: Springer 2017, pp. 53 e ss.

⁷⁶ Alínea a) do n.º 1, do art. 20.º, do RGPD. Este foi um aspeto criticado pela Autoridade Europeia para a Proteção de Dados no primeiro parecer sobre a proposta de regulamento da Comissão, “Opinion of the European Data Protection Supervisor on the data protection reform package”, de 12 de março de 2012, p. 25. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf> (acedido a 8/12/2017).

⁷⁷ G29, *Guidelines*, cit., p. 7.

⁷⁸ Sendo o interesse legítimo do titular dos dados, v. G29, “Parecer 6/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE”, adotado em 9 de abril de 2014, pp. 47 e 48. Disponível em: <<http://www.gdpd.gov.mo/uploadfile/2015/0803/20150803050042662.pdf>> (acedido a 8/12/2017).

⁷⁹ G29, *Guidelines*, cit., p. 8.

tratamentos de dados pessoais relativos a colaboradores e funcionários impõe-se uma análise casuística, porquanto em muitos casos o tratamento fundamenta-se no interesse legítimo do responsável⁸⁰.

Por último, o exercício do direito à portabilidade é aplicável apenas a tratamentos automatizados, excluindo ficheiros em papel ou o tratamento de dados necessários ao exercício de funções de interesse público ou de autoridade pública⁸¹.

2.4. Problemas específicos da aplicação prática da portabilidade

A este direito são aplicáveis as regras gerais para o exercício dos direitos dos titulares dos dados, previstas no art. 12.º, designadamente a obrigação de responder “sem demora injustificada e no prazo de um mês a contar da data da receção do pedido, bem como o dever de informar a disponibilidade da portabilidade”, nos termos da alínea b), do n.º 2, do art. 13.º e da alínea c), do n.º 2, do art. 14.º, do RGPD⁸². Além disto, deparamo-nos com algumas particularidades em relação à aplicação prática deste direito.

Desde logo, a *portabilidade de dados anónimos*. Ou, melhor dizendo, a relação entre a viabilidade e a eficácia da portabilidade e a anonimização de dados. Aludimos *supra* à exclusão dos dados anónimos do âmbito de aplicação do RGPD pelo que, *prima facie*, tudo indica que a portabilidade não abrange estes dados⁸³. O processo de anonimização constitui um “tratamento ulterior”, exigindo por isso um fundamento jurídico nos termos do art. 6.º do RGPD⁸⁴. Ora, nenhum problema se coloca nos casos em que o titular dos dados exerça o direito à portabilidade *antes* da operação de anonimização. O mesmo não se pode dizer se *consentir* nesta operação de anonimização, pretendendo, posteriormente, exercer o direito à portabilidade. Se, por um lado, o RGPD exclui do seu âmbito de aplicação os dados anónimos, por

⁸⁰ *Idem*, p. 9.

⁸¹ Alínea b), do n.º 1, e n.º 3 do art. 20.º do RGPD.

⁸² O G29 recomenda que, na informação a prestar seja feita uma explicação sobre a distinção entre a portabilidade e o acesso aos dados pessoais. v. G29, *Guidelines*, cit., p. 11.

⁸³ ZANFIR, Gabriela. “The right to Data portability in the context of the EU data protection reform”, cit., pp. 10, 13 e 14.

⁸⁴ G29, Parecer 5/2014, cit., p. 7.

outro lado, um dos objetivos da portabilidade – prevenir uma situação de *lock-in* – será difícil de garantir neste segundo caso⁸⁵.

Ademais, à data em que escrevemos, são ainda evidentes os problemas técnicos em torno da execução ou implementação deste novo direito que dificultam o respetivo cumprimento por parte dos responsáveis pelo tratamento⁸⁶: (i) quais as ferramentas da portabilidade, i. é, as medidas técnicas a adotar pelos responsáveis pelo tratamento de modo a permitir o exercício deste direito e (ii) qual o formato dos “dados portáveis⁸⁷”? Quanto às ferramentas da portabilidade, os responsáveis pelo tratamento deverão implementar um mecanismo de download direto e, sempre que tecnicamente possível, de transmissão direta dos dados para outro responsável. O G29 recomenda a disponibilização de uma IPA ou *Interface de Programação de Aplicações*⁸⁸.

O *formato* dos “dados portáveis” é também um aspeto crucial para a eficácia e viabilidade da portabilidade: o responsável que os “recebe” deve ser capaz de os tratar sem prejuízos para a sua qualidade e rigor. Daí que, segundo o art. 20.^º, n.º 1, o formato tem de permitir a sua reutilização, pelo que deverá ser “estruturado, de uso corrente e de leitura automática⁸⁹”. O considerando 68 acrescenta, ainda, uma característica, a

⁸⁵ ZANFIR, Gabriela. “The right to Data portability in the context of the EU data protection reform”, cit., p. 11.

⁸⁶ *Idem*, pp. 3 e ss.

⁸⁷ G29, *Guidelines*, cit., p. 5.

⁸⁸ Definido como “(...) a set of subroutine definitions, protocols, and tool for building software and applications. It refers to the interfaces of applications or web services made available by data controllers, so that other systems or applications can link and work with their systems”. G29, *Guidelines*, cit., p. 5, nota de rodapé 5.

⁸⁹ Por “leitura automática” deve-se entender “um formato de ficheiro estruturado de modo a ser facilmente possível, por meio de aplicações de *software*, identificar, reconhecer e extrair dele dados específicos. Os dados codificados em ficheiros estruturados num formato legível por máquina são dados legíveis por máquina. Os formatos legíveis por máquina podem ser abertos ou exclusivos; podem ser normas formais ou não. Os documentos codificados num formato de ficheiro que limita o tratamento automático, devido ao facto de ou não ser possível extrair os dados desses documentos ou isso não ser facilmente possível, não deverão ser considerados documentos em formato legível por máquina. Os Estados-Membros deverão, se adequado, encorajar a utilização de formatos abertos legíveis por máquina”. v. Diretiva 2013/37/UE do parlamento europeu e do conselho, de 26 de junho de 2013, que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público, considerando 21.

“interoperabilidade⁹⁰”. Para o G29, as exigências prescritas no n.º 1, daquele artigo, constituem os elementos mínimos para facilitar a interoperabilidade do formato dos dados, i. é, são especificações dos meios para atingir o objetivo da interoperabilidade⁹¹. Diga-se ainda que o n.º 1 recusa a criação de “impedimentos”, como a cobrança de uma taxa⁹².

Na proposta original, a Comissão propunha-se especificar este formato. Contudo, constatando a diversidade de tratamentos, as diferenças do *design* e as características dos vários responsáveis, a imposição de um formato comportava um processo de adaptação excessivo e caro, criando obstáculos à inovação e ao desenvolvimento de novas aplicações. A adequação do formato dos dados portáveis dependerá de setor para setor, devendo, pelo menos, preencher uma exigência: a *interpretabilidade*. Tratando-se de uma estrutura de dados complexa, o responsável pelo tratamento deve garantir que o titular é capaz de compreender a definição, o esquema e a estrutura dos seus dados. Sugere-se que os dados sejam fornecidos de forma sumária, por subconjuntos, e não em bloco, ou seja: “de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples⁹³”.

O fim visado pela portabilidade não é incentivar sistemas compatíveis mas garantir sistemas interoperáveis⁹⁴. Por isso, o RGPD não obriga o responsável pelo tratamento a adotar ou manter um sistema de tratamento de dados tecnicamente compatível com os sistemas dos demais⁹⁵. O legislador entendeu que qualquer solução de standardização da portabilidade

⁹⁰ Recorremos a legislação da UE em vigor para compreender este termo: “a capacidade de organizações díspares e diversas interagirem com vista à consecução de objetivos comuns com benefícios mútuos, definidos de comum acordo e implicando a partilha de informações e conhecimento entre as organizações, no âmbito de processos administrativos a que dão apoio, mediante o intercâmbio de dados entre os respetivos sistemas de TIC”. v. Alínea a), do art. 2.º da Decisão n.º 922/2009/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, sobre soluções de interoperabilidade para as administrações públicas europeias (ISA). A norma ISSO/IEC 2382-01 define também este conceito do seguinte modo: “(...) a capacidade de comunicar, executar ou transferir dados entre várias unidades funcionais de tal modo que o utilizador não necessita de ter conhecimentos sobre as características únicas dessas unidades”.

⁹¹ G29, *Guidelines*, cit., p. 13.

⁹² *Idem*, p. 15.

⁹³ N.º 1 do art. 12.º do RGPD e G29, *Guidelines*, cit., p. 14.

⁹⁴ G29, *Guidelines*, cit., p. 14.

⁹⁵ Considerando 68 do RGPD.

deverá nascer da cooperação e do consenso alcançado pelos membros das indústrias e associações comerciais interessadas, que deverão estabelecer um conjunto comum e consensual de formatos e standards interoperáveis adequados às exigências da portabilidade. É justamente essa a finalidade do *European Interoperability Framework* (EIF), a entidade encarregue de definir uma estratégia concertada sobre a interoperabilidade para as organizações que pretendam prestar certo tipo de serviços. As instituições europeias, nomeadamente a Comissão, atuarão como dinamizadoras, criando pontes entre os vários interessados, o que já tem vindo a suceder através da criação de programas como o “ISA²⁹⁶”. Na falta de consenso num determinado setor industrial, o G20 propôs a utilização de formatos abertos (XML, JSON, CSV, entre outros), juntamente com os metadados possíveis⁹⁷.

Como se depreende do art. 20.º, do n.º 4, o exercício deste direito não prejudica o exercício dos direitos e liberdades de terceiros⁹⁸. Contudo, é possível que a transmissão dos dados entre responsáveis pelo tratamento dificulte o exercício dos direitos de terceiros, como o direito à informação ou ao acesso⁹⁹. Seguindo boas práticas, os responsáveis pelo tratamento, tanto o emissor como o recetor, devem implementar mecanismos que permitam “separar o trigo do joio”, selecionar os dados relevantes e excluir os dados de terceiros. Tenha-se ainda presente que a inclusão de dados de terceiros nos dados portáveis pressupõe, por força do art. 6.º, a identificação de um fundamento jurídico autónomo, como o “interesse legítimo” prosseguido pelo responsável pelo tratamento¹⁰⁰.

Os “direitos e liberdades de terceiros”, aludidos no n.º 4 do art. 20, incluem o segredo comercial, a propriedade intelectual ou o direito de autor, que protegem o software, e/ou o modelo de negócio do responsável pelo tratamento. Exige-se um exercício de ponderação sobre as implicações

⁹⁶ Decisão (EU) 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 ISA²) como um meio para modernizar o setor público.

⁹⁷ G29, *Guidelines*, cit., p. 18.

⁹⁸ Considerando 63 do RGPD.

⁹⁹ Um exemplo em concreto acontece com a portabilidade de dados bancários que inclui informação sobre as transações, incluindo sobre terceiros que transferiram dinheiro para a titular daquela conta. G29, *Guidelines*, cit., p. 9.

¹⁰⁰ Alínea f) do n.º 1, do art. 6.º do RGPD.