



Publicação disponível em: <http://blook.pt/publications/publication/e38a9928dbce/>

# DADOS PESSOAIS: CONCEITO, EXTENSÃO E LIMITES

---

**A. BARRETO MENEZES CORDEIRO**

## ***Dados pessoais: conceito, extensão e limites***

Prof. Doutor A. Barreto Menezes Cordeiro, LL.M

### **1. Introdução**

I. O conceito de dado pessoal – descrito no artigo 4.º, 1), do RGPD<sup>1</sup> como toda a “informação relativa a uma pessoa singular identificada ou identificável” – assume um lugar de destaque no Direito da proteção de dados, tanto numa perspetiva prático-legislativa, como numa perspetiva dogmática<sup>2</sup>. Por um lado, o RGPD tem o seu campo

---

<sup>1</sup> Regulamento (UE) n.º 2016/679, 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 Diretriz 95/46/CE.

<sup>2</sup> Stefan Brink/Jens Eckhardt, *Wann ist ein Datum ein personenbezogenes Datum? – Anwendungsbereich des Datenschutzrechts*, 5 ZD, 2015, 205-212; Tina Krügel, *Das personenbezogene Datum nach der GS-GVO – Mehr Klarheit und Rechtssicherheit?*, 7 ZD, 2017, 455-460. A centralidade do conceito tem sido, nos últimos anos, criticada por alguma doutrina especializada, que advoga a sua substituição, enquanto elemento nuclear deste ramo jurídico, pelo efetivo impacto da recolha e tratamento de informação pessoal na esfera jurídica dos seus titulares. Por todos: Mortiz Karg, *Die Rechtsfigur des personenbezogenen Datums – Ein Anachronismus des Datenschutzes?* 2 ZD, 2012, 255-260. Na origem desta posição encontramos o receio de que o conceito seja excessivamente lato em face da evolução tecnológica contemporânea, podendo culminar numa recondução de toda a informação ao universo dos dados pessoais. Curiosamente, outros Autores, partindo do mesmo panorama, receiam uma diminuição efetiva da proteção em resultado deste suposto recondução. A própria Comissão Europeia parece partilhar desta apreensão: no final de 2016, a Comissão Europeia decidiu apoiar financeiramente, no valor global de € 1 499 650, um projeto científico que parte precisamente deste pressuposto. Atente-se a esta esclarecedora passagem, constante dos objetivos do projeto: “Given modern data collection and processing techniques and unprecedented amounts of data available for analysis, everything can be translated into data and anyone can be identifiable in data sets. Therefore, Personally Identifiable Information-based legal protection will fail, since a law regulating everything is meaningless”. Veja-se, ainda, com uma perspetiva algo diferente, Barbara Schmitz, *Der Abschied vom Personenbezug – Warum der Personenbezug nach der DS-GVO nicht mehr zeitgemäß ist*, 8 ZD, 2018, 5-8: embora a Autora defenda, igualmente, a atribuição de maior relevância ao impacto efetivo da recolha dessa informação, em prejuízo do conceito de dado pessoal, parece-nos que os problemas por si suscitados circunscrevem-se mais ao elemento da identificabilidade e não propriamente à necessidade de identificar um novo núcleo característico do Direito da proteção de dados.

de aplicação circunscrito ao universo da proteção de dados de pessoas singulares, nos exatos termos previstos nos artigos 1.º, 2.º e 3.º<sup>3</sup>. Por outro lado, a função formal do Direito da proteção de dados passa por regular as situações jurídicas relativas a dados pessoais e a sua função material por proteger os seus titulares. Trata-se de um ramo jurídico funcionalizado a este propósito último, embora atente, igualmente, à relevância social e económica destes bens jurídicos<sup>4</sup>.

II. Visando o Direito da proteção de dados apenas regular – formal – e proteger – material – os dados pessoais e os interesses dos seus titulares, da não recondução de uma determinada informação a este conceito só se pode concluir que nem este ramo jurídico, nem o RGPD serão chamados a intervir<sup>5</sup>: a informação anónima não é violadora de qualquer interesse juridicamente atendível<sup>6</sup>.

No presente estudo, pretendemos analisar, partindo da definição legal consagrada no artigo 4.º, 1), do RGPD, as linhas gerais que compõem o conceito de dado pessoal<sup>7</sup>. Trata-se, reconheça-se *ab initio*, de um conceito que vive um processo de mutação constante e que exige, fruto dos avanços tecnológicos, aperfeiçoamentos cirúrgicos pontuais.

Por fim, não pode deixar de ser sublinhado que a sua consolidação dogmática se encontra dependente de estudos mais específicos, nomeadamente e apenas mencionando os que mais tinta têm feito correr, sobre a problemática relativa aos IPs e a geodata. Apesar da sua relevância, estes dois aspetos apenas pontualmente serão referidos no presente artigo.

## 2. Evolução histórica e elementos nucleares do conceito

---

<sup>3</sup> Na realidade e como resulta da conjugação destes três preceitos, nem todos os dados pessoais são regulados pelo RGPD. Importa atender às várias especificidades e exceções aí consagradas.

<sup>4</sup> O considerando 4 do RGPD é esclarecedor, quer em relação à funcionalização material do Direito da proteção de dados, quer da necessidade de considerar a dimensão social e económica dos dados pessoais.

<sup>5</sup> Matthias Bergt, *Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag*, 5 ZD 2015, 365-371, 365.

<sup>6</sup> Judith Nink/Jan Pohle, *Die Bestimmbarkeit des Personenbezugs – Von IP-Adresse zum Anwendungsbereich der Datenschutzgesetze*, 18 MMR, 2015, 563-567, 563.

<sup>7</sup> Tobias Herbst, *Was sind personenbezogene Daten?*, 35 NVwZ, 2016, 902-906, 902: mostrando alguma estupefação pelo facto de o conceito de dado pessoal, tão antigo como o próprio Direito que o pretende regular, permanecer por consolidar.

I. As origens da definição prevista no artigo 4.º, 1), do RGPD remontam à década de 70 do século passado e aos esforços desenvolvidos em conjunto pela OCDE e pelo Conselho da Europa<sup>8</sup>.

A 23 de setembro de 1980, a OCDE publica as *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*<sup>9</sup>. No seu artigo 2, a. constava a seguinte definição<sup>10</sup>:

*“personal data” means any information relating to an identified or identifiable individual (“data subject”).*

A 28 de janeiro de 1981 é, por sua vez, aprovada, no seio do Conselho da Europa, a Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal<sup>11</sup>. A definição avançada para o conceito é idêntica<sup>12</sup>:

*“personal data” means any information relating to an identified or identifiable individual (“data subject”).*

Na versão portuguesa da Convenção consta a seguinte definição:

---

<sup>8</sup> Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, Suíça, 2014, 76 ss. Estes esforços conjuntos são reconhecidos pelas próprias entidades: Council of Europe, *Explanatory Report on the Convention for the Protection of Individual with Regard to Automatic Processing of Personal Data*, Estrasburgo, 1981, 9 ss. e OCDE, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OCDE, Paris, 2001, 26.

<sup>9</sup> *Annex to the Recommendation of the Council of 23<sup>rd</sup> September 1980*. A versão atual das *Guidelines* data de 2013 e podem ser consultadas no sítio da OCDE.

<sup>10</sup> Nos primeiros documentos da OCDE relativo à proteção de dados é utilizada uma outra expressão: *personal information*, constante da Resolução da OCDE (73) 22 (*On the protection of the privacy of individual vis-à-vis electronic data banks in the private sector – Adopted by the Committee of Ministers on 22 September 1973 at the 224<sup>th</sup> meeting of the Ministers’ Deputies*) – *““personal information” means information relating to individuals (physical persons)”* – e da Resolução da OCDE (74) 29 (*On the protection of the privacy of individual vis-à-vis electronic data banks in the private sector – Adopted by the Committee of Ministers on 20 September 1974 at the 236<sup>th</sup> meeting of the Ministers’ Deputies*) – *““personal information” means information relating to individuals (physical persons)”*.

<sup>11</sup> A sua ratificação por Portugal apenas ocorre em 1993: Resolução da Assembleia da República n.º 23/93, de 12 de maio; e Decreto do Presidente da República n.º 21/93, de 9 de julho.

<sup>12</sup> Artigo 2 a.

“Dados de carácter pessoal” significa qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação.

II. A definição avançada nos anos 80, pela OCDE e pelo Conselho da Europa, viria a ser utilizada, pela então Comunidade Europeia, na Diretriz 95/46, de 24 de outubro<sup>13</sup>:

“Dados pessoais”, qualquer informação relativa a uma pessoa singular identificada ou identificável (pessoa em causa)<sup>14-15</sup>.

Na transposição interna da Diretriz, o legislador português optou por fazer uma referência, indicativa, aos tipos de suportes em que a *informação pessoal* poderá constar:

“Dados pessoais”: qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável<sup>16</sup>.

III. É notória uma continuidade do conceito de *dados pessoais*, que remonta, formalmente, às *Guidelines* da OCDE e que se encontra, desde a Diretriz 95/46, consolidado no espaço jurídico Europeu<sup>17</sup>, em torno de quatro elementos distintos e autonomizáveis: (i) qualquer informação; (ii) relativa a; (iii) pessoa singular; e (iv) identificada ou identificável.

---

<sup>13</sup> A atenção despendida pelo legislador europeu à problemática da proteção de dados remonta, pelo menos, a meados da década de 70 do século passado.

<sup>14</sup> Artigo 2.º, a). Versão inglesa: “*personal data*” shall mean any information relating to an identified or identifiable natural person (“*data subject*”).

<sup>15</sup> A definição portuguesa surge já, nesses exatos termos, na *Proposta de Directiva do Conselho relativa à protecção das pessoas no que diz respeito ao tratamento de dados pessoais*: JC, n.º C 277, 5-nov.-1990, 3-12, 5.

<sup>16</sup> Artigo 3.º, a), da Lei n.º 67/98, de 26 de outubro.

<sup>17</sup> O Direito alemão da proteção de dados assume, neste âmbito, algumas especificidades que não se verificam entre nós. No *Bundesdatenschutzgesetz* são utilizadas as expressões determinado (*bestimmt*) e determinável (*bestimmbar*) e no RGPD identificado (*identifiziert*) e identificável (*identifizierbar*). Sobre a (ir)relevância prática e dogmática desta alteração, veja-se: Krügel, *Das personenbezogene Datum*, cit., 455-456.

### 3. Qualquer informação

I. Toda a informação é considerada relevante, para efeitos de aplicação do Direito da proteção de dados<sup>18</sup>. Não há, como há já várias décadas o Tribunal Constitucional alemão reconheceu, informação pessoal não merecedora de proteção jurídica, por muito insignificante ou fútil que possa parecer<sup>19</sup>.

O conceito de informação (pessoal) extravasa, largamente, o sentido que tradicionalmente lhe é atribuído no seio dos direitos de personalidade<sup>20</sup>, mesmo que se assuma, como o faz o Tribunal Europeu dos Direitos do Homem, uma conceção mais flexível<sup>21</sup>. Privacidade não é sinónimo de direitos pessoais, nem a proteção concedida pelo regime jurídico consagrado no artigo 80.º do CC é idêntica à prevista pelo Direito da proteção de dados, em todas as suas diferentes concretizações legislativas.

Tanto se entende, como sendo pessoal, informação relativa à vida privada como à vida profissional e social<sup>22</sup>:

O facto de essa informação se inscrever no contexto de uma atividade profissional não lhe pode retirar a qualificação de conjunto de dados pessoais<sup>23</sup>.

O próprio RGPD faz variadas referências a dados pessoais de trabalhadores e relativas à sua atividade laboral<sup>24</sup>.

---

<sup>18</sup> Manuel Klar/Jürgen Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner, Datenschutz-Grundverordnung*, 2ª ed., Beck, Munique, 2018, Rn. 9.

<sup>19</sup> BVerfG 15-dez.-1983, 37 NJW, 1984, 419-428, 422.

<sup>20</sup> António Menezes Cordeiro, *Tratado de Direito civil*, IV, 4ª ed., com colaboração nossa, Almedina, Coimbra, 2016, 267: “Em rigor, a vida privada abrangerá tudo o que não seja público e profissional ou social”.

<sup>21</sup> TEDH 16-fev.-2000, appl. n.º 27798/95 (*Amann v Switzerland*), 65: “the term “private life” must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of “private life””. Com indicação de outra jurisprudência.

<sup>22</sup> TJUE 30-mai.-2013, proc. C-342/12 (*Worten v ACT*), 18 ss; TJUE 29-jun.-2010, proc. C-28/08 (*Comissão Europeia v The Bavarian Lager*), 68 ss; TJUE 20-mai.-2003, proc. C465/00, C-138/01 e C-139/01 (*Rechnungsof v Osterreichischer Rundfunk*), 64 ss, em especial 73.

<sup>23</sup> TJUE 16-nov.-2015, proc. C-615/13 P (*ClientEarth v PAN Europe*), 30.

<sup>24</sup> Artigos 9.º/2, h), 77.º/1 e, em especial, o artigo 88.º.

II. O conceito de informação pessoal abrange, conseqüentemente, todos os aspetos relativos à nossa pessoa, quer sejam familiares ou sociais, privados ou públicos, físicos ou mentais.

A informação pode respeitar, a título meramente exemplificativo, a elementos identificativos da pessoa – nome, data de nascimento, número de cartão de cidadão ou morada – características físicas – género, altura, peso, cor dos olhos ou do cabelo – considerações íntimas – crenças, opiniões, desejos, posições políticas ou religiosas – profissionais e académicas – títulos e graus ou estatutos profissionais e laborais – ou patrimoniais – direitos de propriedade<sup>25</sup>. São infundáveis as modalidades passíveis de serem concebidas.

O conceito de informação, para efeitos de aplicação do RGPD, abrange dados objetivos ou factuais – p.ex.: **A** nasceu em Lisboa – ou subjetivos – **A** não é um trabalhador honesto.

É igualmente irrelevante se os dados compilados e tratados são ou não verdadeiros. Para isso mesmo aponta o direito de retificação consagrado no artigo 16.º.

III. As modalidades variadas de dados pessoais identificadas, pelo legislador europeu, ao longo do RGPD, transmitem-nos, de forma mais fidedigna, o alcance deste primeiro elemento: dados genéticos<sup>26</sup>; dados biométricos<sup>27</sup>; dados relativos à saúde<sup>28</sup>; dados que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, relativos à vida sexual ou orientação sexual<sup>29</sup>; ou dados relacionados com condenações penais e infrações<sup>30</sup>.

---

<sup>25</sup> Klar/Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner*, cit., Rn. 8.

<sup>26</sup> Artigo 4.º, 13): “os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa”.

<sup>27</sup> Artigo 4.º, 14): “dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos”.

<sup>28</sup> Artigo 4.º, 15): “dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde”.

<sup>29</sup> Artigo 9.º.

<sup>30</sup> Artigo 10.º.

IV. O RGPD aplica-se independentemente do formato em que a informação foi recolhida e do suporte em que se encontra armazenada. Como exemplos clássicos de formato, refira-se o alfabético, o numérico, o gráfico ou o acústico e de suporte, o papel, a memória de um computador, uma vídeo cassete, uma *pen* ou um CD<sup>31</sup>.

Também aqui, as decisões do TJUE são esclarecedoras:

- Imagens gravadas em vídeo<sup>32</sup>;
- Atas de reuniões contendo os nomes dos seus participantes<sup>33</sup>;
- Registos dos tempos de trabalhos de trabalhadores de uma empresa<sup>34</sup>;
- Observações de peritos sobre determinado projeto divulgadas em sítio da Internet<sup>35</sup>.

#### 4. Relativa a

I. Para ser considerada um dado pessoal, a informação terá de ser relativa a uma pessoa. Esta intrínseca relação entre a informação e um sujeito exclui, do campo de aplicação do RGPD, toda a informação concernente a realidades jurídicas não subjetiváveis<sup>36</sup>. Assim, informações relativas a objetos – p. ex.: o Evereste é a mais alta montanha do mundo ou o imóvel X custa € 200 00 – são juridicamente irrelevantes, mesmo que o responsável pelo tratamento ou o terceiro conheçam, nos exemplos apresentados, que **A** escalou o Evereste ou que **B** é o proprietário do imóvel X: em ambos os casos a informação não é atinente a qualquer pessoa<sup>37</sup>.

A informação relativa a objetos, quando conjugada com informação respeitante a pessoas, passa a ser tratada como dado pessoal, independentemente de essa informação ser presente ou futura<sup>38</sup>; p.ex: (i) foi feita uma chamada do telemóvel X; e

---

<sup>31</sup> Grupo de Trabalho de Proteção de Dados do Artigo 29.º, Parecer 4/2007 sobre o conceito de dados pessoais, WP 136, 8-9.

<sup>32</sup> TJUE 11-dez.-2014, proc. C-212/13 (*Ryneš v Úřad pro ochranu osobních údajů*), 22.

<sup>33</sup> TJUE 29-jun.-2010, proc. C-28/08 (*Comissão Europeia v The Bavarian Lager*), 68 ss.

<sup>34</sup> TJUE 30-mai.-2013, proc. C-342/12 (*Worten V ACT*), 18 ss.

<sup>35</sup> TJUE 16-nov.-2015, proc. C-615/13 P (*ClientEarth v PAN Europe*),

<sup>36</sup> Veja-se o ponto 5/l.

<sup>37</sup> Klar/Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner*, cit., Rn. 12.

<sup>38</sup> Krügel, *Das personenbezogene Datum*, cit., 457-458.

(ii) o telemóvel X pertence a A. A conjugação de (i) com (ii) converte (i) em dado pessoal<sup>39</sup>.

Os dados ditos factuais poderão igualmente ser reconduzidos ao universo dos dados pessoais, sempre que da informação recolhida conste algum elemento que permita identificar um sujeito<sup>40</sup>. Por fim, a informação factual será sempre pessoal quando é armazenada nesses termos, ou seja, identificando *ab initio* o seu titular<sup>41</sup>.

Quanto à informação recolhida no âmbito dos processos M2M – *Machine to Machine* –, esta poderá ser considerada relativa a pessoas, dependendo, naturalmente, do seu conteúdo e natureza<sup>42</sup>.

II. Seguindo a sistematização proposta pelo Grupo de Trabalho do Artigo 29.º, a expressão *relativa a* abrange três situações distintas: (i) conteúdo; (ii) finalidade; ou (iii) resultado<sup>43</sup>. Trata-se de elementos alternativos e não cumulativos<sup>44</sup>.

Por conteúdo, entende-se toda a informação que incida sobre uma pessoa, ou seja, é a própria pessoa que é *objeto de análise*. Atente-se aos seguintes exemplos: (i) análises clínicas → o doente; (ii) avaliação profissional de um trabalhador → o trabalhador; (iii) registo criminal → o cidadão<sup>45</sup>.

Na segunda situação – finalidade –, embora não seja a pessoa o *objeto de análise*, os dados recolhidos permitem “avaliar, tratar de determinada forma ou influenciar o estatuto ou o comportamento de uma pessoa”<sup>46</sup>:

---

<sup>39</sup> Klar/Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner*, cit., Rn. 13.

<sup>40</sup> Este problema coloca-se com especial evidência no campo da geodata: Nikolaus Forgó/Tina Krügel, *Der Personenbezug von Geodaten – Cui bono, wenn alles bestimmbar ist?*, 13 MMR, 2010, 17-23.

<sup>41</sup> Krügel, *Das personenbezogene Datum*, cit., 457-458.

<sup>42</sup> Andreas Grünwald/Christoph Nüßing, *Machine To Machine (M2M)-Kommunikation – Regulatorische Fragen bei der Kommunikation im Internet der Dinge*, 18 MMR, 2015, 378- 383, 382-383: na maioria das vezes será informação relativa a sujeitos, para mais, acrescentamos nós, se atendermos aos critérios elencados pelo Grupo de Trabalho do Artigo 29.º; Volker Lüdemann, *Connected Cars: Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück*, 5 ZD, 2015, 247-254: o Autor, partindo dos dados automobilísticos recolhidos, analisa a adequação dos modelos regulatórios vigentes, os seus limites e os problemas suscitados, em face da realidade prática. Veja-se, ainda, Ralf Weisser/Claus Färber, *Rechtliche Rahmenbedingungen bei Connected Car – Überblick über die Rechtsprobleme der automobilen Zukunft*, 18 MMR, 2015, 506-512, 508-509.

<sup>43</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 10 ss.

<sup>44</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 12.

<sup>45</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 11.

<sup>46</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 11.

- Retribuições pagas por certas entidades<sup>47</sup>;
- Historial das entradas em e de saídas de um determinado país<sup>48</sup>;
- Dados que constam de um registo de tempos de trabalho relativos, para cada trabalhador, aos períodos de trabalho diário e aos períodos de descanso<sup>49</sup>;
- Dados recolhidos por empresas do sector automóvel<sup>50</sup>.

Por fim, como resultado entende-se toda a informação que não incida sobre uma pessoa (conteúdo) e que não vise avaliá-la ou influenciá-la (finalidade), mas que, em abstrato, o permita fazer. O exemplo apresentado pelo Grupo de Trabalho do Artigo 29.º é, uma vez mais, elucidativo<sup>51</sup>: uma empresa de táxis instalou um sistema de localização de satélite para melhor gerir a sua frota. Apesar de não ser essa a sua finalidade, os dados recolhidos permitem avaliar o desempenho dos motoristas.

III. A expressão *relativa a* não abrange apenas situações em que o titular dos dados surge individualizado. Informações pessoais relativas a grupos de sujeitos poderão, igualmente, ser merecedoras de proteção jurídica, consoante os exatos contornos dos casos<sup>52</sup>. Vejamos dois exemplos: **Informação A**: “A taxa de natalidade em Portugal, no ano 2015, foi de X”; **Informação B**: “A taxa de natalidade dos trabalhadores da Empresa A, no ano de 2015, foi de X”. A **Informação A** não respeita, certamente, a um ou mais sujeitos identificados, já a **Informação B** poderá, dependendo do número de trabalhadores da Empresa A.

---

<sup>47</sup> TJUE 20-mai.-2003, proc. C-465/00, C-138/01 e C-139/01 (*Rechnungsof v Osterreichischer Rundfunk*): este caso poderia ser remetido para a primeira situação – conteúdo –, na medida em que para além dos pagamentos, constava, ainda, o nome do beneficiário.

<sup>48</sup> TJUE 16-dez.-2008, proc. C-524/06 (*Heinz Huber v Bundesrepublik Deutschland*), este caso poderia, também, ser remetido para a primeira situação – conteúdo –, na medida em que para além dos registos de entradas e saídas, constava a seguinte informação: (i) apelido, nome próprio, data e local do nascimento, estado civil, sexo; (ii) historial das entradas no território alemão e das saídas desse território, estatuto de residente; (iii) indicações relativas aos sucessivos passaportes; (iv) historial das declarações de domicílio anteriores, e (v) referências do Bundesamt, indicações dos serviços que transmitiram os dados e referências desses serviços: 31.

<sup>49</sup> TJUE 30-mai.-2013, proc. C-342/12 (*Worten v ACT*), em especial 19.

<sup>50</sup> Karsten Kinast/Christina Kühni, *Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten*, NJW, 2014, 3057-3060, em especial 3058.

<sup>51</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 11-12.

<sup>52</sup> Klar/Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner*, cit., 15.

## 5. Pessoa singular

I. O campo de aplicação material do RGPD abrange apenas as pessoas singulares, independentemente da sua nacionalidade ou local de residência<sup>53</sup>. Esta delimitação inicial deixa de fora todas as pessoas coletivas<sup>54</sup> e, evidentemente, demais realidades jurídicas não subjetiváveis, como as coisas<sup>55</sup> e os animais<sup>56</sup>. O próprio nome completo do RGPD é conclusivo: “relativo à proteção das pessoas singulares”.

Tem sido, de resto, esta a interpretação classicamente assumida pelas autoridades europeias. O TJUE, confrontado com a necessidade de interpretar o alcance do artigo 8.º/1 da Carta dos Direitos Fundamentais da União Europeia – “Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito” – pronunciou-se em igual sentido<sup>57</sup>.

O não reconhecimento de uma proteção aos dados pessoais de pessoas coletivas contrasta com os avanços recentes no campo dos direitos de personalidade clássicos<sup>58</sup>. É hoje aceite, pacificamente, pelos tribunais portugueses que também as pessoas coletivas são titulares de alguns direitos de personalidade<sup>59</sup>, caso do direito ao nome<sup>60</sup>,

---

<sup>53</sup> Considerando 14. A conjugar, naturalmente, com o campo de aplicação espacial previsto no artigo 3.º.

<sup>54</sup> Considerando 14: “O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva”.

<sup>55</sup> Nem sempre é fácil determinar se os dados recolhidos respeitam a uma coisa, por exemplo uma máquina, ou à pessoa que a opera. Uma resposta a esta questão irá depender da própria natureza, características e extensão dos dados: Information Commissioner’s Office, *Determining what is personal data* (Net), 2012, 20-21. Veja-se, ainda, a nota 42.

<sup>56</sup> Sobre os avanços recentes do campo do Direito dos animais, veja-se o nosso artigo *A natureza jurídica dos animais à luz da Lei n.º 8/2017, de 3 de março*, 2 RDC 2017, 317-335.

<sup>57</sup> TJUE 9-nov.-2010, proc. C-92/09 e C-93/09 (*Volker und Markus Schecke GbR/Hartmut Eifert v Land Hessen*) 52-53. Gregor Heißl, *Können juristische Personen in ihrem Grundrecht auf Datenschutz verletzt sein?*, EuR 20017, 561-571: análise completa à problemática, de um ponto de vista dogmático e prático.

<sup>58</sup> Por todos: Menezes Cordeiro, *Tratado*, IV, cit., 119 ss.

<sup>59</sup> STJ 9-jul.-2014 366/12 (João Bernardo), proc. n.º 366/12; STJ 12-set.-2013 (Oliveira Vasconcelos), proc. n.º 372/08.9; RGm 16-fev.-2017 (Higina Castelo), proc. n.º 346/12.3: “as pessoas coletivas gozam da tutela de direitos de personalidade”; RLx 8-mai.-2012 (Ana Resende), proc. n.º 115/07.4: “as pessoas coletivas gozam dos direitos e estão sujeitas aos deveres compatíveis com a sua natureza, devendo-lhe ser reconhecidos alguns direitos especiais de personalidade”.

<sup>60</sup> RGm 16-fev.-2017 (Higina Castelo), proc. n.º 346/12.3; RLx 8-mai.-2012 (Ana Resende), proc. n.º 115/07.4

o direito ao bom nome comercial<sup>61</sup> e o direito à privacidade empresarial, que abrange, pelo menos, o sigilo da correspondência, as particularidades de organização e de funcionamento e o *know-how* de uma entidade coletiva<sup>62</sup>.

Também o Tribunal Europeu dos Direitos do Homem tem vindo a reconhecer uma proteção às pessoas coletivas à sua *privacidade* (artigo 8.º da CEDH)<sup>63</sup>, embora sem a subjetivar: não são as pessoas coletivas que têm um direito à privacidade, mas os Estados que têm, o dever de não ultrapassar certos limites; por exemplo: proteção contra violações de domicílio<sup>64</sup>, proteção contra consultas de correspondência<sup>65</sup> e busca e apreensão de dados informáticos<sup>66</sup>.

Apesar da posição clássica do Direito europeu, alguns sistemas jurídicos nacionais assumiam, internamente, a extensão da proteção concedida às pessoas coletivas, caso da Itália ou da Áustria. Contudo, este movimento encontra-se hoje, fruto da posição assumida no RGPD e da necessidade de adaptação dos Direitos internos dos Estados Membros ao Direito europeu, em manifesto retrocesso: tanto artigo 4/1, *b*), do *Codice in materia di protezione dei dati personali*<sup>67</sup> como o § 1 do renovado *Datenschutzgesetz*<sup>68</sup> circunscrevem o seu campo de aplicação às pessoas singulares.

A informação sobre pessoas coletivas apenas se encontra sujeita ao RGPD quando respeite, direta ou indiretamente, a pessoas singulares, p. ex.: o nome do sócio ou sócios conste da denominação da pessoa coletiva<sup>69</sup>.

---

<sup>61</sup> REv 11-set.-2013 (Moura Santos), proc. n.º 2747/08.4: o tribunal distingue o direito ao crédito do direito ao bom nome: “Ofende o crédito da pessoa colectiva a divulgação jornalística de factos susceptíveis de diminuir a confiança nela quanto ao cumprimento de obrigações, e o seu bom nome se forem susceptíveis de abalar o seu prestígio ou merecimento no meio social e económico em que se insere”.

<sup>62</sup> STJ 12-set.-2013 (Oliveira Vasconcelos), proc. n.º 372/08.9.

<sup>63</sup> Peter Oliver, *Companies and Their Fundamental Rights: A Comparative Perspective*, 64 ICLQ, 2015, 661-696, 676-678.

<sup>64</sup> TEDH 16-abr.-2012, appl. n.º 37971/97 (*Colas v France*); TEDH 18-abr.-2013, appl. n.º 26419/10 (*Saint-Paul Luxembourg S.A. v Luxembourg*).

<sup>65</sup> TEDH 14-mar.-2013, appl. n.º 24117/08 (*Bernh Larsen v Norway*).

<sup>66</sup> TEDH 16-out.-2007, appl. n.º 74336/1 (*Wiese v Austria*).

<sup>67</sup> “*dato personale*”, *qualunque informazione relativa a persona fisica*”.

<sup>68</sup> “*Jede natürliche Person hat Anspruch auf Geheimhaltung der sie betreffenden personenbezogenen Daten*”.

<sup>69</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 25. TJUE 9-nov.-2010 C-92/09 e C-93/09 *Volker und Markus Schecke GbR/Hartmut Eifert v Land Hessen*, 53-54: “as pessoas colectivas só podem invocar a protecção dos artigos 7.º e 8.º da Carta a respeito de tal identificação desde que a denominação legal da pessoa colectiva identifique uma ou mais pessoas singulares. É o que se passa com a recorrente na causa principal no processo C-92/09. Com efeito, a denominação legal da sociedade identifica directamente pessoas singulares, que são sócios dessa sociedade”.

A recondução do direito aos dados pessoais ao universo dos direitos de personalidade, tanto numa perspetiva constitucional – artigo 26.º da CRP – como, e em especial, numa perspetiva civilística – artigo 70.º do CC –, permite, todavia, a invocação dos regimes jurídicos vigentes de forma a proteger as pessoas coletivas<sup>70</sup>.

II. Não é feita no texto do RGPD ou nos extensos considerandos que o antecedem qualquer referência à aplicação do diploma aos nascituros. O legislador europeu terá optado por *delegar* essa decisão nos Estados-Membros<sup>71</sup>.

É inegável que, no mundo contemporâneo, são recolhidas diversas informações respeitantes aos nascituros, desde ecografias a análises ao líquido amniótico<sup>72</sup>. A dúvida não está, assim, em determinar se estes dados são merecedores de proteção jurídica, mas apenas a que título: como dados pessoais do nascituro ou dados pessoais da mãe<sup>73</sup>?

O problema, embora intrinsecamente relacionado com a natureza jurídica dos nascituros – têm ou não personalidade jurídica –, extravasa esta discussão clássica e com ela não se confunde. Recorde-se que, nos termos do artigo 66.º/2 do CC, os direitos que a lei legitima aos nascituros apenas dependem do seu nascimento<sup>74</sup>. Deste modo, poderemos sempre considerar que, independentemente da pessoa a quem a titularidade é atribuída, no período que medeia a conceção e o nascimento completo, após o *corte do cordão umbilical*<sup>75</sup>, esses dados pessoais serão igualmente pertencentes ao até então nascituro.

III. O âmbito de aplicação material do RGPD circunscreve-se a informação relativa a pessoas vivas. O conceito de dados pessoais do diploma não inclui, conseqüentemente, os dados pessoais de pessoas falecidas<sup>76</sup>.

---

<sup>70</sup> Com idêntica posição: Peter Gola, *Anotação ao artigo 4.º do RGPD* em Gola, *Datenschutz-Grundverordnung*, Beck, Munique, 2017, Rn. 23.

<sup>71</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 24.

<sup>72</sup> Hans Hermann Schild, *Anotação ao artigo 4.º do RGPD* em BeckOK *Datenschutzrecht*, coord. Heinrich Amadeus Wolff/Stefan Brink, 22ª ed., Beck, Munique, 2017, Rn. 9.

<sup>73</sup> Wolfgang Ziebarth, *Anotação ao artigo 4.º do RGPD* em Sydow, *Europäische Datenschutzgrundverordnung*, Nomos, Baden-Baden, 2017, Rn. 12.

<sup>74</sup> Schild, *Anotação ao artigo 4.º do RGPD* em BeckOK, cit., 9.

<sup>75</sup> Utiliza-se a expressão *corte do cordão umbilical* com um propósito meramente simbólico. Nunca poderá ser esse corte que determina a aquisição de personalidade jurídica: Menezes Cordeiro, *Tratado*, IV, cit., 372 ss.

<sup>76</sup> Considerando 27: “O presente regulamento não se aplica aos dados pessoais de pessoas falecidas”.

O legislador europeu abre, todavia, as portas para o seu tratamento interno, i.e., ao nível do Direito dos Estados-Membros<sup>77</sup>. Atualmente, alguns países europeus reconhecem já um nível de proteção às pessoas falecidas análogo ao concedido às pessoas vivas, veja-se o caso paradigmático da Bulgária, onde os direitos do titular falecido podem ser exercidos pelos seus herdeiros<sup>78</sup>; ou da Estónia, onde a proteção foi alargada para os 30 anos após o falecimento do titular dos dados<sup>79</sup>, estando a sua utilização, durante esse período, dependente de consentimento expresso por parte dos seus herdeiros<sup>80</sup>. Alguma doutrina alemã, por invocação do princípio basilar da dignidade da pessoa humana, previsto no § 1(1) da Constituição local<sup>81</sup>, e através de uma interpretação sistemática do Direito da proteção de dados, advoga, já hoje, o reconhecimento de uma proteção generalizada aos dados pessoais de pessoas falecidas<sup>82</sup>. A necessidade de acautelar estes dados pessoais assume hoje a preferência da grande maioria dos autores que têm dedicado maior atenção ao problema<sup>83</sup>.

Entre nós, refira-se o entendimento, já antigo, da CNDP de limitar o acesso a dados de saúde de titulares de dados já falecidos quer às seguradoras – exige-se um consentimento expresso do titular – quer aos próprios familiares – apenas podem aceder, sem o consentimento expresso do titular, “ao relatório da autópsia ou à causa

---

<sup>77</sup> Considerando 27: “Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas”.

<sup>78</sup> Artigo 28(3) da Lei de Proteção de Dados búlgara. Versão inglesa: “*In case the individual dies, his or her rights . . . shall be exercised by his or her heirs*”, consultável no sítio [www.legislationline.org](http://www.legislationline.org).

<sup>79</sup> § 12(6) da Lei de Proteção de Dados estoniana. Versão inglesa: “*The consent of a data subject shall remain valid during the lifetime of the data subject and for thirty years after the death of the data subject unless the data subject has decided otherwise*”, consultável no sítio [www.legislationline.org](http://www.legislationline.org).

<sup>80</sup> § 13(1) da Lei de Proteção de Dados estoniana. Versão inglesa: “*After the death of a data subject, processing of personal data relating to the data subject is permitted only with the written consent of the successor, spouse, descendant or ascendant, brother or sister of the data subject, except if consent is not required for processing of the personal data or if thirty years have passed from the death of the data subject. If there are more than one successor or other persons specified in this section, processing of the data subject's personal data is permitted with the consent of any one of them but each one of the successors has the right to withdraw the consent*”, consultável no sítio [www.legislationline.org](http://www.legislationline.org).

<sup>81</sup> Bettina Spilker, *Postmortaler Datenschutz*, DÖV 2015, 54-60.

<sup>82</sup> Thorsten Culmsee, *Postmortaler Datenschutz und postmortaler Datenntzung*, DSRITB 2013, 413-428: o Autor, de forma a sustentar a sua posição, analisa diversos diplomas legislativos em que os dados de pessoas falecidas surgem acautelados.

<sup>83</sup> Para além dos autores alemães já referidos, veja-se, sem pretensões exaustivas: J.C. Buitelaar, *Post-Mortem Privacy and Informational Self-Determination*, 19 *Ethics Inf Technol*, 2017, 129-142 e Edina Harbinja, *Post-Mortem Privacy 2.0: Theory, Law, and Technology*, 31 *IRLCT*, 2017, 26-42: com inúmeras referências bibliográficas.

da morte”<sup>84</sup>. A CNPD não admite, contudo, a existência de um direito *post mortem*, na aceção mais técnica do termo, mas a permanência de deveres de confidencialidade, na esfera jurídica da instituição de saúde<sup>85</sup>. Do conteúdo desta deliberação não será excessivo considerar que a CNPD aceitará uma proteção aos dados de titulares já falecidos sempre que se demonstre a existência de deveres de confidencialidade, com origem legal ou contratual.

Ainda no campo do RGPD e do Direito da proteção de dados, a informação sobre pessoas falecidas deixa de poder ser livremente utilizada se afetar pessoas vivas, caso paradigmático de informação médica ou genética hereditária, i.e., que respeite, igualmente, aos descendentes vivos do *de cuius*<sup>86</sup>. Neste caso, não se está a acautelar os dados pessoais do falecido, mas os dados pessoais de um titular vivo.

Fora do universo dos dados pessoais, recorde-se o disposto no artigo 71.º do CC, nomeadamente o seu número 1: “os direitos de personalidade gozam igualmente de proteção depois da morte do respetivo titular”<sup>87</sup>; a criminalização das ofensas à memória de pessoa falecida, consagrada no artigo 185.º do CP<sup>88</sup>; e, no geral, todas as obrigações cuja eficácia se mantenha após a morte do sujeito protegido, *maxime*, deveres de sigilo e de confidencialidade<sup>89</sup>.

## 6. identificada ou identificável: enquadramento

---

<sup>84</sup> Deliberação n.º 51/2001 e Deliberação n.º 72/2006. Ambas consultáveis no sítio da CNPD, no separador *Orientações*.

<sup>85</sup> Deliberação n.º 51/2001, 23.

<sup>86</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 23. Os dados genéticos e médicos são, de resto, merecedores de uma especial proteção, por intermédio do artigo 9.º do RGPD.

<sup>87</sup> Trata-se, reconheça-se, de um direito em relação ao qual os familiares têm de exigir o respeito pelo descanso e pela memória dos seus mortos”: Menezes Cordeiro, *Tratado*, IV, cit., 530-549. Johann Bizer, *Postmortaler Persönlichkeitsschutz? – Rechtsgrund und Länge der Schutzfristen für personenbezogene Daten Verstorbener nach den Archivgesetzen des Bundes und der Länder*, 12 NVwZ, 1993, 653-656: o Autor advogava, já então, uma aplicação da solução civilística clássica à problemática dos dados pessoais, ou seja, uma circunscrição da proteção aos familiares do falecido.

<sup>88</sup> Moldura penal: pena de prisão até 6 meses ou com pena de multa até 240 dias. Nos termos do número 3: “a ofensa não é punível quando tiverem decorrido mais de 50 anos sobre o falecimento”.

<sup>89</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 23.

I. Dos quatro elementos que compõem o conceito de dado pessoal, apenas este último e somente em relação à expressão identificável é objeto de maiores explicações. No texto do Regulamento<sup>90</sup>:

[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<sup>91</sup>.

e nos Considerandos<sup>92</sup> que o acompanham:

Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica<sup>93</sup>.

O cuidado e a atenção dispensados pelo legislador europeu são demonstrativos, por um lado, da maior complexidade que rodeia este elemento e, por outro lado, da sua importância para o preenchimento do conceito de dado pessoal<sup>94</sup>.

II. O legislador europeu não densifica o que se entende por *identificada* nem em que medida concreta se distingue esta da expressão *identificável*. Do ponto de vista prático, esta diferenciação não é, à primeira vista, determinante: independente de ser

---

<sup>90</sup> A mesma preocupação havia já sido manifestada na Diretriz 95/46/CE. Vejam-se as referências nas notas seguintes.

<sup>91</sup> Artigo 4.º, 1). Diretriz 95/64/CE, Artigo 2.º, a): “é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social”.

<sup>92</sup> Atente-se, ainda, ao Considerando 30.

<sup>93</sup> Considerando 26. Diretriz n.º 95/64/CE, Considerando 26: “para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios susceptíveis de serem razoavelmente utilizados, seja pelo responsável pelo tratamento, seja por qualquer outra pessoa, para identificar a referida pessoa”.

<sup>94</sup> Herbst, *Was sind personenbezogene Daten*, cit., 902: descreve-o nestes exatos termos; Krügel, *Das personenbezogene Datum*, cit., 456: quase que circunscreve toda a problemática que rodeia o conceito de dado pessoal a este elemento; Nink/Pohle, *Die Bestimmbarkeit des Personenbezugs*, cit., 565.

identificada ou identificável, a proteção concedida é a mesma<sup>95</sup>. Contudo, o não esclarecimento de cada uma das expressões impossibilita o entendimento cabal do conceito de dado pessoal e, conseqüentemente, a própria aplicação do RGPD.

III. A Ciência Jurídica especializada tem preenchido o conceito *identificada* através da locução diretamente<sup>96</sup>. O TJUE considerou, recentemente, não constituir o endereço de IP dinâmico “uma informação relativa a uma “pessoa singular identificada”, na medida em que esse endereço não revela diretamente a identidade da pessoa singular proprietária do computador a partir do qual se efetua a consulta de um sítio na Internet, nem a de outra pessoa que possa utilizar esse computador”<sup>97</sup>.

Assim, uma determinada informação respeita diretamente a uma pessoa sempre que seja suficiente para a identificar de forma inequívoca, ou seja, sempre que não sejam necessários dados adicionais<sup>98</sup>. O nome completo de uma pessoa, admitindo que seja único, o número do cartão de identificação, o número de segurança social, o número de contribuinte fiscal ou as impressões digitais<sup>99</sup> são informações relativas a uma pessoa identificada. Já o primeiro e último nome são – em princípio –, só por si e sem mais informação, insuficientes para identificar uma pessoa concreta, salvo, naturalmente, quando o titular dos dados em causa seja uma figura pública<sup>100</sup>, ou que, à luz dos demais elementos, respeite, inequivocamente, a um sujeito concreto<sup>101</sup>.

A identificação ou não identificação do titular dos dados irá depender das circunstâncias concretas e do grau de autossuficiência da informação detida<sup>102</sup>.

---

<sup>95</sup> Stefan Ernst, *Anotação ao artigo 4.º do RGPD em Paal/Pauly, Datenschutz-Grundverordnung – Bundesdatenschutzgesetz*, 2ª ed., Beck, Munique, 2018, Rn. 8.

<sup>96</sup> Klar/Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner*, cit., Rn. 18; Schild, *Anotação ao artigo 4.º do RGPD em BeckOK*, cit., Rn. 16.

<sup>97</sup> TJUE 19-out.-2016, proc. C-582/14 (*Breyer v Bundesrepublik Deutschland*), 38. Como veremos oportunamente, o TJUE considerou, à luz dos elementos do caso concreto, que se tratava de informação relativa a pessoa identificável.

<sup>98</sup> Ziebarth, *Anotação ao artigo 4.º do RGPD em Sydow*, cit., Rn. 14.

<sup>99</sup> TJUE 17-out.-2014, proc. C-291/12 (*Chwarz v Bochum*), 27: “As impressões digitais enquadram-se neste conceito, uma vez que contêm objetivamente informações únicas sobre pessoas singulares e permitem a sua identificação exata”.

<sup>100</sup> TEDH 19-fev.-2015, appl. n.º 53649/09 (*Ernst August von Hannover v Alemanha*), 44 ss: assumindo, precisamente, esta conceção, no que ao direito à intimidade da vida privada respeita.

<sup>101</sup> TJUE 16-dez.-2008, proc. C-73/07 (*Tietosuojaaltuutettu v Oy*), 35: primeiro e último nome mais rendimentos.

<sup>102</sup> Ziebarth, *Anotação ao artigo 4.º do RGPD em Sydow*, cit., Rn. 14.

IV. Em relação à expressão *identificável* e partindo de ambos os trechos acima transcritos, a informação – que pode consistir em mais do que um elemento – será relativa a pessoa determinável sempre que haja uma probabilidade razoável de o responsável pelo tratamento ou de terceiros conseguirem identificar, através da conjugação de mais informação, a identidade do titular dos dados<sup>103</sup>, ou seja, que torne a identificação possível<sup>104</sup>, à luz de um juízo de razoabilidade.

Em relação à expressão *identificável*, importa distinguir dois problemas distintos: (i) probabilidade razoável e fatores; e (ii) a relevância da informação detida por terceiros.

## 7. Identificável: probabilidade razoável e fatores

I. Independentemente dos fatores e meios relevantes, o critério geral de determinação da possibilidade de a identidade do titular de um delimitado dado anónimo ser desvendada é o da razoabilidade. Caberá ao intérprete-aplicador determinar, à luz dos factos e do contexto concreto se é expectável que da conjugação de outros elementos a identidade do titular desses dados anónimos possa ser deslindada. A razoabilidade não respeita aos meios utilizados, mas à identificabilidade do titular<sup>105</sup>.

A assunção de um critério de razoabilidade é um reflexo da impossibilidade fáctica de garantir a anonimidade absoluta dos dados recolhidos<sup>106</sup>.

II. O TJUE, no acórdão *Breyer v Bundesrepublik Deutschland* considerou, seguindo a posição manifestada pelo Advogado Geral<sup>107</sup>, que não deveria ser tida em consideração a possibilidade de serem empregues, pelo responsável pelos dados ou por um eventual terceiro, informações obtidas ilicitamente, ou seja, apenas fatores lícitos

---

<sup>103</sup> Klar/Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner*, cit., Rn. 19.

<sup>104</sup> Schild, *Anotação ao artigo 4.º do RGPD em BeckOK*, cit., Rn. 17.

<sup>105</sup> Ziebarth, *Anotação ao artigo 4.º do RGPD em Sydow*, cit., Rn. 23.

<sup>106</sup> Jürgen Kühling/Manuel Klar, *Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität*, 66 NJW, 2013, 3611-3617, 3613.

<sup>107</sup> *Conclusões do Advogado-Geral no proc. C-582/14 (Breyer v Bundesrepublik Deutschland)*, 68.

relevam para efeitos de preenchimento do elemento da *identificabilidade*<sup>108</sup>. Esta posição, merecedora de um certo apoio<sup>109</sup>, tem sido criticada por uma parte importante da doutrina especializada.

Entre os diversos argumentos esgrimidos, destacam-se: a disponibilidade tecnológica, técnica e humana que as empresas têm à sua disposição<sup>110</sup>; os dados recolhidos por uma entidade europeia poderem ser acedidos por entidades sedeadas fora do espaço europeu<sup>111</sup>; as diferenças legislativas existentes entre os vários países: o que é ilícito à luz do Direito europeu pode ser considerado lícito num outro ordenamento jurídico<sup>112</sup>; ou a ocorrência frequente de ataques informáticos<sup>113</sup>. Em suma, sendo o critério último o da razoabilidade, importa atender a todas as condutas ilícitas desde que se possa razoavelmente contar com elas<sup>114</sup>.

Esta conclusão é suportada pelos elementos interpretativos que temos à nossa disposição<sup>115</sup>: (i) elemento literal: a expressão razoabilidade não exclui ilicitudes: há ilicitudes que são expectáveis de serem cometidas; (ii) elemento teleológico: o objetivo do RGPD e do próprio Direito da proteção de dados é proteger, de forma preventiva, a devassa dos dados pessoais das pessoas singulares; e (iii) elemento sistemático: o Direito da proteção de dados foi concebido precisamente porque se reconhece que os dados pessoais de cada pessoa podem ser obtidos ilicitamente.

III. A posição manifestada pelo Grupo de Trabalho do Artigo 29.º no célebre Parecer 4/2007 sobre o conceito de dados pessoais<sup>116</sup> tem sido igualmente citada como sendo favorável à desconsideração da utilização de meios ilícitos, para efeitos do preenchimento do requisito da identificabilidade. Recorde-se o exemplo apresentado:

---

<sup>108</sup> TJUE 19-out.-2016, proc. C-582/14 (*Breyer v Bundesrepublik Deutschland*), 46.

<sup>109</sup> Kühling/ Klar, *Unsicherheitsfaktor Datenschutzrecht*, cit., 3613.

<sup>110</sup> Achim Klabunde, *Anotação ao artigo 4.º do RGPD em Ehmann/Selmayr, Datenschutz-Grundverordnung*, Beck, Munique, 2017, Rn. 12.

<sup>111</sup> Ziebarth, *Anotação ao artigo 4.º do RGPD em Sydow*, cit., Rn. 23.

<sup>112</sup> Ziebarth, *Anotação ao artigo 4.º do RGPD em Sydow*, cit., Rn. 23.

<sup>113</sup> Krügel, *Das personenbezogene Datum*, cit., 456, 459-460.

<sup>114</sup> Ziebarth, *Anotação ao artigo 4.º do RGPD em Sydow*, cit., Rn. 38.

<sup>115</sup> Segue-se de perto o raciocínio apresentado por Patrick Breyer, *Personenbezug von IP-Adressen - Internetnutzung und Datenschutz*, 4 ZD, 2014, 400-405, 402.

<sup>116</sup> Grupo de Trabalho de Proteção de Dados do Artigo 29.º, *Parecer 4/2007 sobre o conceito de dados pessoais*, WP 136.

Determinados hospitais ou médicos transferem dados de registos médicos dos seus doentes para uma empresa para fins de investigação médica. Não são utilizados os nomes dos doentes, apenas os números de série, atribuídos aleatoriamente a cada caso clínico, de forma a assegurar a coerência e evitar confusão entre a informação sobre diferentes doentes. Os nomes dos doentes mantêm-se exclusivamente na posse dos respectivos médicos vinculados pelo sigilo profissional. Os dados não contêm qualquer informação adicional que possa tornar a identificação dos doentes possível por combinação. Adicionalmente, foram tomadas todas as medidas, sejam elas jurídicas, técnicas ou organizacionais, para evitar que as pessoas em causa sejam identificadas ou se tornem identificáveis. Nestas circunstâncias, uma Autoridade de Protecção de Dados poderá considerar que, no tratamento efectuado pela empresa farmacêutica, não existem meios susceptíveis de serem razoavelmente utilizados para identificar as pessoas em causa<sup>117</sup>.

Ora, deste exemplo não se pode concluir pela defesa, por parte do Grupo de Trabalho do Artigo 29.º, da irrelevância da utilização de meios ilegais – que nestes casos consistiria na divulgação ou obtenção da informação confidencial apenas conhecida dos médicos –, mas somente não ser expectável que esses mesmo médicos violem o Juramento de Hipócrates<sup>118</sup>.

IV. No Considerando 26 do RGPD, o legislador europeu indicou, a título exemplificativo – a utilização da expressão “todos os fatores objetivos, como” é inequívoca –, alguns fatores que poderão ser atendidos: custos económicos, tempo necessário e tecnologia despendida. Não é apenas a tecnologia presente que deve ser tida em consideração, mas também a tecnologia futura – “tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica” –, à luz, naturalmente, de um juízo de razoabilidade<sup>119</sup>.

O Grupo de Trabalho do Artigo 29.º apresenta outros fatores a ter em consideração: “O objectivo pretendido, a forma como o tratamento está estruturado, a vantagem esperada pelo responsável pelo tratamento, os interesses em causa para as pessoas, bem como o risco de disfunções organizacionais (ex.: quebra do dever de confidencialidade) e falhas técnicas, deverão todos ser tidos em consideração”<sup>120</sup>.

---

<sup>117</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 16.

<sup>118</sup> “Prometo solenemente. . . Mesmo após a morte do doente respeitarei os segredos que me tiver confiado”.

<sup>119</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 16; Klar/Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner*, cit., Rn. 23; Klabunde, *Anotação ao artigo 4.º do RGPD em Ehmann/Selmayr*, cit., Rn. 12.

<sup>120</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 16.

Por fim, serão sempre considerados pessoais, os dados que possam a todo o tempo desanonimizados pelo respetivo responsável<sup>121</sup>.

IV. Sendo este um exercício casuístico<sup>122</sup> e realista – atividades teóricas e rebuscadas devem ser descartadas<sup>123</sup> –, o intérprete-aplicador deve atender à natureza dos próprios dados e às pretensões do responsável pelo tratamento. Por exemplo: o responsável pelo tratamento dos dados pode recolher informação com o preciso intuito de identificar os respetivos titulares<sup>124</sup> ou pode ter um especial interesse em fazê-lo, quer pelos benefícios económicos ou outros que daí julga poder retirar<sup>125</sup>, quer pela notoriedade do próprio titular: quanto maior relevância social tiver o titular dos dados maior será o interesse em identificá-lo e os potenciais benefícios<sup>126</sup>. Ambas as situações, entre outras, justificam o dispêndio de quantias monetárias e de tempo que de outro modo não seriam razoáveis<sup>127</sup>.

## 8. Identificável: a teoria subjetiva e a teoria objetiva

I. Não restam dúvidas nem ninguém contesta que o sujeito será determinável sempre que o responsável pelo tratamento de dados possa aceder a informação adicional que, conjugada com a informação por si já detida, permita identificar a identidade do titular dos dados<sup>128</sup>. A dúvida e a discussão, jurisprudencial e doutrinária, reside na irrelevância ou relevância dos conhecimentos e dos meios detidos por terceiros<sup>129</sup>.

---

<sup>121</sup> Ziebarth, *Anotação ao artigo 4.º do RGPD em Sydow*, cit., Rn. 32.

<sup>122</sup> Kühling/ Klar, *Unsicherheitsfaktor Datenschutzrecht*, cit., 3613.

<sup>123</sup> Nink/Pohle, *Die Bestimmbarkeit des Personenbezugs*, cit., 565; Patrick Breyer, *Personenbezug von IP-Adressen – Internetnutzung und Datenschutz*, 4 ZD, 2014, 400-405, 400.

<sup>124</sup> Grupo de Trabalho do Artigo 29.º, *Parecer 4/2007*, cit., 16-17.

<sup>125</sup> Kühling/ Klar, *Unsicherheitsfaktor Datenschutzrecht*, cit., 3613.

<sup>126</sup> Klar/Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner*, cit., Rn. 22.

<sup>127</sup> Kühling/ Klar, *Unsicherheitsfaktor Datenschutzrecht*, cit., 3613.

<sup>128</sup> Matthias Bergt, *Die Bestimmbarkeit als Grundproblem des Datenschutzrechts: Überblick über den Theorienstreit und Lösungsvorschlag*, 5 ZD 2015, 365-371, 365.

<sup>129</sup> Para um apanhado geral da problemática e das várias soluções preconizadas, vejam-se os seguintes escritos: Judith Nink/Jan Pohle, *Die Bestimmbarkeit des Personenbezugs – Von IP-Adresse zum Anwendungsbereich der Datenschutzgesetze*, 18 MMR, 2015, 563-567; Matthias Bergt, *Die*

São duas as grandes teorias que se confrontam: (i) a teoria relativa: circunscreve a análise de razoabilidade aos meios e conhecimentos detidos pelo responsável pelos dados; e (ii) a teoria objetiva: defende uma análise abstrata que considere os meios e os conhecimentos detidos pelo responsável e por terceiros. Ambas as teorias estão, naturalmente, sujeitas a diversas variações<sup>130</sup>.

II. Independentemente da posição sustentada, algumas situações não levantam especiais dúvidas, sendo, com um elevado grau de certeza, defendidas pelos partidários de ambas as teorias.

Se o titular dos dados recolhidos anonimamente puder ser determinado através de informação extra disponível ao público em geral – p.ex.: *online* –, então serão dados pessoais e o seu titular identificável<sup>131</sup>.

A solução será a mesma se o responsável pelos dados os transmitir a terceiros que detenham especiais conhecimentos ou meios, que com ele trabalhem<sup>132</sup> ou não<sup>133</sup>.

III. Embora se anteveja, se não uma mudança de posição, pelo menos uma adaptação à posição do TJUE, a maioria da doutrina<sup>134</sup> e da jurisprudência<sup>135</sup> alemã mostra-se favorável à teoria relativa.

---

*Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag*, 5 ZD 2015, 365-371, 365.

<sup>130</sup> Bergt, *Die Bestimmbarkeit*, cit., 365-367 e Herbst, *Was sind personenbezogene Daten*, cit., 903-905.

<sup>131</sup> Klar/Kühling, *Anotação ao artigo 4.º do RGPD em Kühling/Buchner*, cit., Rn. 27.

<sup>132</sup> Nink/Pohle, *Die Bestimmbarkeit des Personenbezugs*, cit., 564.

<sup>133</sup> Nink/Pohle, *Die Bestimmbarkeit des Personenbezugs*, cit., 564.

<sup>134</sup> A título meramente exemplificativo: Alexander Roßnagel/Philip Scholz, *Datenschutz durch Anonymität und Pseudonymität – Rechtsfolgen der Verwendung anonymer und pseudonymer Daten*, 3 MMR, 2000, 721-731, 722-723; Per Meyerdierks, *Sind IP-Adressen personenbezogene Daten?*, 12 MMR, 2009, 8-13; Paul Voigt, *Datenschutz bei Google*, 12 MMR, 2009, 377-382, 379; Stefan Krüger/Svenja-Ariane Maucher, *Ist die IP-Adresse wirklich ein personenbezogenes Datum? – Ein falscher Trend mit großen Auswirkungen auf die Praxis*, 14 MMR, 2011, 433-439, 436; Paul Voigt/Setafn Alich, *Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber*, 64 NJW, 2011, 3541-3544, 3542; Peter Gola/Christoph Klug/Barbara Körffer, *Anotação ao § 3 do BDSG em Gola/Schomerus, Bundesdatenschutzgesetz*, 12ª ed., Beck, Munique, 2015, Rn. 10; Kühling/ Klar, *Unsicherheitsfaktor Datenschutzrecht*, cit., 3614.

<sup>135</sup> AG München 30-set.-2008, proc. 133 C 5677/08, BeckRS 2008, 23037: limitando a identificabilidade aos conhecimentos e meios detidos pelo responsável; AG Bamberg 1-mar.-2012, proc. 101 C 1912/11, 3 ZD, 2013, 603-631: fazendo expressa referência ao acórdão do AG München; LG Frankenthal, 21-mai.-2008, proc. 6 O 156/08, 11 MMR, 2008, 687-691; LG Wuppertal 19-out.-2010, proc. 20 Qs 10 Js 1977/08-177/10, 14 MMR 2011, 65-66. Para um apanhado mais completo, vide Bergt, *Die Bestimmbarkeit*, cit., 367.

De entre os vários argumentos apresentados, destacam-se os seguintes: da aplicação da teoria objetiva, pelo menos no seu estado mais puro, todos os dados seriam considerados pessoais<sup>136</sup>; a atribuição de relevância aos meios e conhecimentos detidos por terceiros impossibilitaria que o responsável pelos dados conhecesse se está ou não a respeitar a legislação aplicável, na medida em que o próprio não controla a sua anonimidade: esta é determinada por um terceiro, que o responsável pode nem sequer conhecer<sup>137</sup> – no limite, a lei estaria sempre a ser violada, com a agravante de a recolha dessa informação merecer o beneplácito das autoridades de supervisão responsáveis<sup>138</sup>; tornaria todo o processo de supervisão, pelas entidades responsáveis, excessivamente pesado ou mesmo de impossível concretização<sup>139</sup>; reconduziria a problemática a uma *simples* situação de colisão de interesses – pessoais e coletivos – ou de direitos<sup>140</sup> – p.ex.: proteção de dados pessoais vs livre iniciativa económica; violaria princípios económicos basilares das Constituições ocidentais<sup>141</sup>; colocaria os próprios interesses económicos da União Europeia e dos seus Estados-Membros em causa, em face do processo de globalização contemporâneo<sup>142</sup>.

A estas e a outras críticas, respondem os defensores da teoria objetiva<sup>143</sup> que esta nunca seria verdadeiramente objetiva, na aceção mais pura do termo, na medida em que o critério último será sempre o da razoabilidade.<sup>144</sup>

IV. O Considerando 26 do RGPD – e também o Considerando 30 – aponta, inequivocamente, para a relevância dos conhecimentos e meios detidos por terceiros. Contudo, não é claro que terceiros são abrangidos: todos os sujeitos com capacidade jurídica ou apenas uma categoria bem determinada, por exemplo, como acima já

---

<sup>136</sup> Ziebarth, *Anotação ao artigo 4.º do RGPD em Sydow*, cit., Rn. 39.

<sup>137</sup> Meyerdierks, *Sind IP-Adressen*, cit., 10.

<sup>138</sup> Nink/Pohle, *Die Bestimmbarkeit des Personenbezugs*, cit., 565.

<sup>139</sup> Kühling/ Klar, *Unsicherheitsfaktor Datenschutzrecht*, cit., 3614.

<sup>140</sup> Kühling/ Klar, *Unsicherheitsfaktor Datenschutzrecht*, cit., 3614.

<sup>141</sup> Karg, *Die Rechtsfigur des personenbezogenen Datums*, cit., 260.

<sup>142</sup> Nink/Pohle, *Die Bestimmbarkeit des Personenbezugs*, cit., 567.

<sup>143</sup> Ernst, *Anotação ao artigo 4.º do RGPD em Paal/Pauly*, cit., 10-11; Klabunde, *Anotação ao artigo 4.º do RGPD em Ehmann/Selmayr*, cit., Rn. 12; Herbst, *Was sind personenbezogene Daten*, cit.; Bergt, *Die Bestimmbarkeit*, cit.; Breyer, *Personenbezug von IP-Adressen*, cit.

<sup>144</sup> Por todos: Herbst, *Was sind personenbezogene Daten*, cit., 904-905. Meyerdierks, *Sind IP-Adressen*, cit., 11: o Autor argumenta, precisamente, nesse sentido, ou seja, o de que a teoria absoluta desconsidera os próprios limites da legislação aplicável.

identificámos, quem com o responsável pelos dados trabalha? O conteúdo do Considerando 26 não responde, só por si, a esta questão<sup>145</sup>.

Alguma doutrina pretende ainda ler nas entrelinhas do exemplo das farmácias, acima apresentado, a defesa, pelo Grupo de Trabalho do Artigo 29.º, da teoria objetiva<sup>146</sup>. Embora se consiga acompanhar esta raciocínio, até certo ponto, a mesma dúvida permanece: mas que terceiros?

O TJUE, no incontornável acórdão *Breyer*<sup>147</sup>, veio tomar posição, ao reconhecer a relevância jurídica dos conhecimentos e meios detidos por terceiros – “para qualificar uma informação como dado pessoal, não é necessário que essa informação permita, por si só, identificar a pessoa em causa”<sup>148</sup> – e ao considerar serem os IPs dinâmicos dados pessoais na medida em que o prestador de serviços de meios de comunicação em linha “disponha de meios legais que lhe permitam identificar a pessoa em causa graças às informações suplementares que o fornecedor de acesso à Internet dessa pessoa dispõe”<sup>149</sup>. A posição sufragada pelo TJUE não é fácil de catalogar, na medida em que rejeita a teoria relativa, mas, ao mesmo tempo, a teoria objetiva no seu estado mais puro<sup>150</sup>.

## 9. A relevância da informação detida por terceiros: solução preconizada

I. Na busca por uma solução para a presente disputa doutrinária, o intérprete-aplicador terá sempre de atender aos elementos interpretativos clássicos, comuns aos

---

<sup>145</sup> Klar/Kühling, *Anotação ao artigo 4.º do RGPD* em Kühling/Buchner, cit., Rn. 26: permite ambas as interpretações. Nink/Pohle, *Die Bestimmbarkeit des Personenbezugs*, cit., 564: sustentam que o Considerando 26 reconhece a relevância jurídica de todo e qualquer conhecimento, independentemente do terceiro em questão; Peter Schantz, *Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht*, 69 NJW, 2016, 1841-1847, 1843: mostra-se dividido, embora inclinado para o reconhecimento da teoria objetiva.

<sup>146</sup> Nink/Pohle, *Die Bestimmbarkeit des Personenbezugs*, cit., 565.

<sup>147</sup> TJUE 19-out.-2016, proc. C-582/14 (*Breyer v Bundesrepublik Deutschland*).

<sup>148</sup> Em 41.

<sup>149</sup> Em 48 e conclusões.

<sup>150</sup> Ziebarth, *Anotação ao artigo 4.º do RGPD* em Sydow, cit., Rn. 37.

vários sistemas jurídicos europeus<sup>151</sup> e ao Direito europeu<sup>152</sup>: (i) elemento literal; (ii) elemento teleológico; (iii) elemento sistemático; e (iv) elemento histórico. Este último, em face da ausência de trabalhos preparatórios que o densifiquem, assume uma reduzida relevância. Também o elemento literal não nos fornece especiais pistas, o texto do preceito permite ambas as interpretações. Restam-nos, assim, os elementos teleológico e sistemático.

II. A funcionalização<sup>153</sup> do Direito da proteção de dados à proteção dos interesses dos titulares de dados pessoais implica que tanto o legislador, como o intérprete-aplicador, como a própria doutrina se devam guiar por esta conceção. Do ponto de vista da interpretação da lei, a funcionalização impõe que, em caso de dúvida, se assumo o sentido que acautela os interesses dos titulares de dados pessoais de forma mais efetiva<sup>154</sup>.

Esta funcionalização encontra-se, como introdutoriamente sublinhámos, demarcada – mas não subordinada – pelos interesses económicos envolvidos. O confronto entre os interesses individuais e os interesses coletivos está longe de ser uma novidade: consiste, de resto, na marca mais distintiva do Direito privado contemporâneo: social e regulamentado.

Assim, numa perspetiva puramente teológica, a solução encontra-se, *ab initio*, condicionada: deverá ser a que acautela de forma mais efetiva os interesses dos titulares dos dados.

III. Numa perspetiva sistemática, importa atender ao preceito enquanto um todo, primeiro, e ao próprio RGPD na sua globalidade, de seguida.

No artigo 4.º, 1), do RGPD não é feita qualquer menção à relevância dos conhecimentos detidos por terceiros. Esta indicação é-nos fornecida pelo Considerando

---

<sup>151</sup> Direito continental: António Menezes Cordeiro, *Tratado de Direito civil*, I, 4ª ed., Almedina, Coimbra, 2012, 671. Direito anglo-saxónico: A. Barreto Menezes Cordeiro, *A interpretação da lei no Direito inglês*, 2017, Net: apesar das diferenças terminológicas, os elementos empregues são idênticos.

<sup>152</sup> Por todos: Christian Baldus/Thomas Raff, *Richterliche Interpretation des Gemeinschaftsrechts em Europäisches Privat- und Unternehmensrechts*, coord., Martin Gebauer/Christoph Teichmann, Nomos, Baden-Baden, 2016, 153-218, em especial 184 ss.

<sup>153</sup> Sobre o conceito de funcionalização, veja-se o nosso: *Manual de Direito dos valores mobiliários*, Almedina, Coimbra, 2016, 81 ss.

<sup>154</sup> *Manual*, cit., 91.

26: “Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados . . . quer pelo responsável pelo tratamento quer por outra pessoa”. Da leitura do trecho ora transcrito não é possível concluir pela assunção, pelo legislador europeu, da teoria objetiva pura: apenas poderão ser considerados os meios ditos razoáveis e não todos os meios. Ou seja, deverão, efetivamente, ser considerados os meios detidos por terceiros, mas não todos: apenas os “meios suscetíveis de ser razoavelmente utilizados”. Isso mesmo é reconhecido pelo TJUE no acórdão *Breyer*.

Esta delimitação, à luz de critérios de razoabilidade, sai reforçada pelo segundo grande pilar do Direito europeu da proteção de dados e que acaba por ajustar a proteção dos direitos dos titulares de dados pessoais: a dimensão económica e social da recolha e subsequente tratamento dos dados pessoais. A Economia europeia não *sobreviveria* num mundo globalizado se os dados pessoais não pudessem ser objeto de uma anonimidade.

IV. Esclarecidas as linhas gerais do modelo interpretativo adequado, importa concretizá-lo à luz de, pelo menos, três situações concretas:

1. Qualquer pessoa tem os meios necessários para aceder a mais informação, *maxime*, por essa informação ser pública;
2. O responsável pelo tratamento tem os meios necessários para aceder a mais informação – situação discutida no acórdão *Breyer*;
3. Um terceiro concreto tem os meios necessários para aceder a mais informação.

A primeira é de fácil resolução: se qualquer pessoa tem os meios necessários à sua disposição para desvendar a identidade dos titulares de dados anónimos detidos pelo responsável, então esses dados não são anónimos, mas pessoais.

A segunda e a terceira merecem uma resposta idêntica: os dados serão anónimos sempre que o responsável (segunda situação) ou o terceiro concreto (terceira situação) disponham dos meios necessários para desvendar a identidade dos titulares de dados anónimos.

Contudo, nem todos os meios têm relevância jurídica, mas somente os que, para o declaratório normal, sejam expectáveis de serem utilizados. Neste ponto, não podemos concordar com o TJUE quando este afirma que apenas os meios lícitos devem ser considerados. Assumimos como nossos os muitos argumentos, acima apresentados, que sustentam a posição inversa<sup>155</sup>. O critério legal é o da razoabilidade e não o da razoabilidade + licitude.

V. Por fim, importa resolver um último aspeto, circunscrito à terceira situação: como pode o responsável pelo tratamento, ou as respetivas entidades de supervisão, conhecerem os meios detidos por cada terceiro<sup>156</sup>?

Uma resposta fundada e satisfatória a esta questão só é possível se assumirmos uma conceção gradual da teoria objetiva<sup>157</sup>: devemos atender aos meios detidos por todos os sujeitos, mas limitando a nossa análise aos conhecimentos que, razoavelmente, esses terceiros tenham à sua disposição. Na prática, os dados poderão ser pessoais ou anónimos consoante o sujeito que esteja a ser avaliado<sup>158</sup>.

Do ponto de vista do responsável, ele apenas poderá ser responsabilizado se, para o declaratório normal e atendendo aos exatos contornos do caso, fosse expectável que um terceiro tivesse à sua disposição os meios necessários para desvendar a identidade dos titulares dos dados anónimos por ele detidos. Na prática, estamos a aplicar um conceito com o qual os nossos tribunais trabalham diariamente: o da boa-fé subjetiva ética. O responsável estará de boa-fé – não podendo, conseqüentemente, ser responsabilizado – sempre que não conheça e desconheça sem culpa os especiais conhecimentos e meios detidos por terceiros.

---

<sup>155</sup> Ponto 7/II.

<sup>156</sup> Herbst, *Was sind personenbezogene Daten*, cit., 905.

<sup>157</sup> Herbst, *Was sind personenbezogene Daten*, cit., 905-906.

<sup>158</sup> Roßnagel/Scholz, *Datenschutz durch Anonymität*, cit., 722-723.