BBS

Instituto de Direito Bancário da Bolsa e dos Seguros

UNIVERSIDADE D COIMBRA

EDIÇÃO: BBS ■ DIRECTOR: Filipe Albuquerque Matos ■ PERIODICIDADE: Anual ■ n.º 3 - 2018

REVISTA ONLINE
BANCA, BOLSA E SEGUROS

3

INSTITUTO DE DIREITO BANCÁRIO, DA BOLSA E DOS SEGUROS
FACULDADE DE DIREITO
UNIVERSIDADE DE COIMBRA

BANCA, BOLSA E SEGUROS

DIRECTOR

Filipe Albuquerque Matos

N.º 3 | 2018

INSTITUTO DE DIREITO BANCÁRIO, DA BOLSA E DOS SEGUROS
Faculdade de Direito da Universidade de Coimbra

TÍTULO
BANCA, BOLSA E SEGUROS

DIRECTOR
Filipe Albuquerque Matos

CONSELHO DE REDACÇÃO
Francisco Pereira Coelho
Pedro Maia
Mafalda Miranda Barbosa
Matilde Lavouras

PRODUÇÃO GRÁFICA
C. Duarte

CONTACTOS
bbs@fd.uc.pt
www.bbs.fd.uc.pt
Pátio da Universidade | 3004-528 Coimbra

ISSN
2183-5586

INSTITUTO DE DIREITO BANCÁRIO, DA BOLSA E DOS SEGUROS | FACULDADE DE DIREITO | UNIVERSIDADE DE COIMBRA

A DECLARAÇÃO DE CONSENTIMENTO PRÉ-FORMULADA — ARTICULAÇÃO ENTRE A DIRECTIVA 1993/13/CEE, DE 5 DE ABRIL DE 1993, E O REGULAMENTO 2016/679/UE, DE 27 DE ABRIL DE 2016

Nuno Pinto de Oliveira

SUMÁRIO: 1. Introdução. O considerando n.º 42 do Regulamento Geral de Protecção de Dados (= Regulamento 2016/679/UE, de 27 de Abril de 2016). 2. A relação de semelhança entre a Directiva 1993/13/CEE, de 5 de Abril de 1993, e o Regulamento 2016/679/UE, de 27 de Abril de 2016. 3. a) O controlo formal das declarações de consentimento pré-formuladas. 4. b) O controlo substancial das declarações de consentimento pré-formuladas. 5. Consequências da relação de semelhança entre a Directiva 1993/13/CEE, de 5 de Abril de 1993, e o Regulamento 2016/679/UE, de 27 de Abril de 2016. O contributo da Directiva 1993/13/CEE para a interpretação do Regulamento 2016/579/UE. 6. a) O alcance dos princípios gerais do direito da protecção de dados. 7. b) O sentido do princípio da transparência. 8. c) O sentido dos princípios da licitude, da adequação, da necessidade e da proporcionalidade. 9. d) Consequências substantivas da violação do direito da protecção de dados. 10. e) Consequências processuais da violação do direito da protecção de dados. O contributo da acção inibitória para a efectivação dos princípios gerais do direito da protecção de dados. 11. Conclusão. O considerando n.º 42 do Regulamento 2016/679/UE, de 27 de Abril de 2016, como *reflexo* da relação de complementaridade entre o direito do consumo e o direito da protecção de dados.

As minhas primeiras palavras serão, como devem ser, de agradecimento e de saudação.

Em primeiro lugar, palavras de agradecimento aos coordenadores do colóquio e, em especial, ao Doutor António Pinto Monteiro, ao Doutor Filipe Albuquerque Matos e à Doutora Mafalda Miranda Barboa, pelo convite que me dirigiram.

Em segundo lugar, palavras de saudação — para o Doutor Rui de Alarcão, moderador do painel, para o Doutor Filipe Albuquerque Matos, para o Doutor Alexandre Dias Pereira, para a Doutora Carolina Cunha e para todos os pessoas presentes.

Estando na Faculdade de Direito da Universidade de Coimbra, e num colóquio organizado pelo Instituto de Direito Bancário, da Bolsa e dos Seguros, as palavras comuns, de agradecimento e de saudação, devem ser completadas com uma palavra especial, de homenagem.

O Doutor João Calvão da Silva deixou-nos há pouco, muito pouco, tempo. Se fica a sua obra, e se a sua obra é extraordinária, falta a sua presença. Falta quase tudo.

1. Introdução. O considerando n.º 42 do Regulamento Geral de Protecção de Dados (= Regulamento 2016/679/UE, de 27 de Abril de 2016)

O título da minha comunicação, "A declaração de consentimento previamente formulada", convoca um conceito geral do sistema de protecção de dados — o conceito de *consentimento* ou de *declaração de consentimento*.

A antiga Directiva 1995/46/CEE, de 24 de Outubro de 1995, definia-o como "manifestação de vontade livre, específica e informada, pelo qual a pessoa em causa aceita que dados pessoas que lhe dizem respeito sejam objecto de tratamento" [1].

O novo Regulamento n.º 2016/679, de 27 de Abril de 2016, define-o como "manifestação de vontade livre, específica, informada e explícita, pela qual o titular dos dados aceita, medidante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento" [2].

Enquanto a antiga directiva exigia que o titular dos dados aceitasse o tratamento, sem especificar se a aceitação devia ser pela positiva ou podia ser pela negativa (pelo silêncio), o novo regulamento exige que o titular dos dados o aceite pela positiva — a declaração de consentimento deverá ser explícita, e só poderá ser explícita desde que conste de um acto positivo inequívoco.

Entre todos as declarações de consentimento, tratarei tão-só de algumas — das declarações de consentimento previstamente formuladas.

O considerando n.º 42 do Regulamento Geral de Protecção de Dados é do seguinte teor:

> "... Em conformidade com a Directiva [19]93/13/CEE do Conselho, uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas ...".

[1] Cf. art. 2.º, alínea h), da Directiva 1995/46/CEE, de 24 de Outubro de 1995.

[2] Cf. art. 4.º, alínea (11), do Regulamento n.º 2016/679, de 27 de Abril de 2016.

O texto do considerando n.º 42 do Regulamento Geral de Protecção de Dados Pessoais dá a impressão de estar a dizer algo que não causaria dúvida alguma.

A Directiva 1993/13/CEE, de 5 de Abril de 1993, relativa às cláusulas abusivas em contratos com os consumidores [3], aplicar-se-ia às declarações de consentimento pré-formuladas. Entre as consequências da aplicação da Directiva 1993/13/CEE estariam particulares requisitos de forma e particulares requisitos de fundo.

Os particulares requisitos de forma relacionar-se-iam com a clareza e com a simplicidade da linguagem: "… uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples…". Os particulares requisitos de fundo, esses. relacionar-se-iam com o conteúdo, que a linguagem designa: "… uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida … sem cláusulas abusivas".

Embora o texto do considerando n.º 42 dê a impressão de estar a dizer algo que não causaria dúvida alguma, entre a Directiva 1993/13/CEE e o Regulamento n.º 2016/679/UE há algumas diferenças, estruturais e funcionais, e as diferenças entre os dois instrumentos poderiam fazer com que a aplicação da

[3] Em relação à Directiva 1993/13/CEE, de 5 de Abril de 1993, *vide* António Pinto Monteiro, "O novo regime dos contratos de adesão / cláusulas contratuais gerais", in: *Revista da Ordem dos Advogados*, ano 62 (2002), págs. 111-142; Joaquim de Sousa Ribeiro, *O problema do contrato. As cláusulas contratuais gerais e o princípio da liberdade contratual*, Livraria Almedina, Coimbra, 1999, esp. nas págs. 585 ss.; ou Almeno de Sá, *Cláusulas contratuais gerais e directiva sobre cláusulas abusivas*, 2.ª ed., Livraria Almedina, Coimbra, 2001.

Directiva 1993/13/CEE às declarações de consentimento pré-formuladas ("previamente formuladas") pusesse problemas.

Em primeiro lugar, a directiva aplica-se só a contratos, ou seja, a negócios jurídicos bilaterais, e as declarações de consentimento para o tratamento de dados pessoais não são necessariamente contratos, — não são necessariamente negócios jurídicos bilaterais.

Podem ser compromissos jurídicos autênticos [4], como sucederá nos casos de *consentimento vinculante*, e dentro dos compromissos jurídicos autênticos podem ser negócios jurídicos bilateral ou negócios jurídicos unilaterais [5]; podem ser compromissos jurídicos *sui generis*, como sucederá nos casos de *consentimento autorizante* [6].

Em segundo lugar, a directiva aplica-se só a negócios celebrados por consumidores, e as declarações de consentimento não são necessariamente negócios celebrados por consumidores. O fim da Directiva 1993/13/CEE é a protecção de algumas pessoas singulares, desde que desempenhem a função de consumidores, e o fim do Regulamento 2016/679/UE é a protecção de todas as pessoas singulares, desempenhem ou não a função

[4] Expressão de Orlando de Carvalho, *Teoria geral do direito civil. Sumários desenvolvidos aos alunos do 2.º ano (1.ª turma) do curso jurídico de 1980/81*, Centelha, Coimbra, 1981, pág. 182.

[5] Cf. Carlos Alberto da Mota Pinto / António Pinto Monteiro / Paulo Mota Pinto, *Teoria geral do direito civil*, 4.ª ed., Coimbra Editora, Coimbra, 2005, págs. 215-217 e, por último, Pedro Leitão Pais de Vasconcelos, *A autorização*, Coimbra Editora, Coimbra, 2015, págs. 400-405.

[6] Expressão de Orlando de Carvalho, *Teoria geral do direito civil*, cit., pág. 182 — definindo o *consentimento autorizante* como "constitutivo de um compromisso jurídico *sui generis*, que atribui a outrem um poder de agressão".

de consumidores. Em terceiro lugar, a directiva aplica-se a consumidores para proteger sobretudo os seus interesses económicos e o regulamento aplica-se a todas as pessoas singulares para proteger sobretudo os seus interesses pessoais. O fim da Directiva 1993/13/CEE é a protecção de algumas pessoas singulares (dos consumidores), como titulares de interesses económicos [7] [8], e o fim do Regulamento 2016/679/UE é a protecção de todas as pessoas singulares como titulares de direitos e de liberdades fundamentais, nomeadamente do direito à protecção de dados pessoais [9].

Explicitadas as dúvidas causadas pelo sentido aparente, superficial, do considerando n.º 42, o seu sentido profundo estará porventura em dizer duas coisas que era preciso dizer: que a Directiva 1993/13/CEE se aplica imediatamente a algumas declarações de consentimento pré-formuladas, — às declarações de consentimento pré-formuladas emitidas por *consumidores*; e que, ainda que não se aplique imediatamente, a Directiva 1993/13/CEE contribua para a interpretação do Regulamento 2016/679/UE.

Entre a Directiva 1993/13/CEE e o Regulamento 2016/679/UE há, pelo menos, uma relação de semelhança, de complementação e de esclarecimento — a directiva contribui, pelo menos, para tornar mais claro o sentido do princípio da transparência,

[7] Cf. o considerando n.º 9 da Directiva 1993/13/CEE, de 5 de Abril de 1993.

[8] O termo *protecção de interesses económicos* encontra-se ainda na epígrafe do art. 9.º da Lei n.º 14/96, de 31 de Julho, alterada pela Lei n.º 85/98, de 16 de Dezembro, pelo Decreto-Lei n.º 67/2003, de 8 de Abril, pela Lei n.º 10/2013, de 28 de Janeiro, e pelo Decreto-Lei n.º 47/2014, de 28 de Julho.

[9] Cf. os considerandos n.ºs 1 e 2 e o texto do art. 1.º, em especial do n.º 2 do art. 1.º, do Regulamento 2016/679/UE, de 27 de Abril de 2016.

do princípio da licitude e dos princípios da adequação, da necessidade e da proporcionalidade [10].

2. A relação de semelhança entre a Directiva 1993/13/CEE, de 5 de Abril de 1993, e o Regulamento 2016/679/UE, de 27 de Abril de 2016

Começaria pela relação de semelhança entre a directiva e o regulamento.

Em primeiro lugar, o controlo formal dos contratos com os consumidores, no quadro da directiva, como o controlo formal das declarações de consentimento para o tratamento de dados pessoais, no quadro do regulamento, resultam sobretudo do princípio da transparência.

Em segundo lugar, o controlo substancial dos contratos com os consumidores, como o controlo substancial das declarações de consentimento para o tratamento de dados pessoais, resultam sobretudo dos princípios da licitude, da adequação, da necessidade e da proporcionalidade.

3. a) O controlo formal das declarações de consentimento pré-formuladas

[10] Cf. Natali Helberger / Frederik Zuiderveen Borgesius / Agustin Reyna, "The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law", in: *Common Market Law Review*, vol. 54 (2017), págs. 1427-1465 = in: WWW: < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048844 >. .

O direito da protecção dos consumidores, e em especial o art. 4.º, n.º 2, e o art. 5.º da Directiva 1993/13/CEE, terá sido a fonte de inspiração do princípio da transparência do art. 7.º, n.º 2, do Regulamento 2016/679/UE [11].

A Directiva 1993/13/CEE exige "que as cláusulas se encontrem redigidas de forma inteligível e de fácil acesso, numa linguagem clara", em dois artigos.

Em primeiro lugar, exige-o no art. 4.º, n.º 2, como condição para que as cláusulas relacionadas com o objecto principal do contrato sejam subtraídas ao *controlo de conteúdo*.

> "A avaliação do carácter abusivo das cláusulas não incide nem sobre a definição do objecto principal do contrato nem sobre a adequação entre o preço e a remuneração, por um lado, e os bens ou serviços a fornecer em contrapartida, por outro, *desde que essas cláusulas se encontrem redigidas de maneira clara e compreensível*".

Em segundo lugar, exige-o no art. 5.º, como condição para que as cláusulas não relacionadas com o objecto principal do contrato sejam *válidas* e/ou *eficazes*.

> "No caso dos contratos em que as cláusulas propostas ao consumidor estejam, na totalidade ou em parte, consignadas por escrito, essas cláusulas deverão ser sempre redigidas de forma clara e compreensível" [12].

[11] *Vide* D. C. J. van Caesteren, *Consent Now and Then* (dissertação de mestrado), Universidade de Tilburg, 2017, pág. 23.

O Regulamento 2016/679/UE exige que todas as comunicações e informações relacionadas com o tratamento dos dados pessoais sejam "de fácil acesso" e estejam formuladas em "linguagem clara e simples".

O preâmbulo do regulamento refere-se ao princípio da transparência nos considerandos n.º 39 e n.º 58 e o articulado do regulamento refere-se-lhe no art. 5.º, n.º 1, alínea a), no art. 7.º e no nos arts. 12.º a 15.º — em especial, no art. 7.º e no 12.º.

O primeiro corolário do princípio da transparência resulta art. 7.º, n.º 2.

O pedido de consentimento para o tratamento de dados pessoais deve ser autonomizado ou separado dos demais assuntos considerados no procedimento de negociação para a conclusão de um contrato:

> "Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos…".

[12] O direito português refere-se ao requisito da transparência no art. 9.º, n.º 2, alínea a). da Lei de Defesa dos Consumidores: "Com vista à prevenção de abusos resultantes de contratos pré-elaborados, o fornecedor de bens e o prestador de serviços estão obrigados […] à redacção clara e precisa, em caracteres facilmente legíveis, das cláusulas contratuais gerais, incluindo as inseridas em contratos singulares".

O segundo e o terceiro corolários do princípio da transparência resultam, simultaneamente, dos arts. 7.º e 12.º.

Em termos mais gerais, o art. 12.º requer que todas as comunicações e informações relacionadas com o tratamento de dados sejam apresentadas "de forma concisa, transparente, inteligível e de fácil acesso" [13] e, em termos mais específicos, o art. 7.º requer que todas as comunicações relacionadas com o pedido de consentimento para o tratamento de dados sejam apresentadas "de modo inteligível e de fácil acesso" [14].

Como garantia da transparência, da inteligibilidade e da acessibilidade está o requisito de que todas as comunicações e informações relacionadas com o consentimento sejam formuladas "numa linguagem clara e simples" [15].

4. b) O controlo substancial das declarações de consentimento pré-formuladas

Os critérios de controlo do conteúdo das cláusulas contratuais pré-formuladas definem-se através de dois conceitos indeterminados.

Em primeiro lugar, através do conceito indeterminado de "desequilíbrio significativo, em detrimento do consumidor, entre os direitos e as obrigações das partes decorrentes do contrato" e, em segundo lugar, através do conceito indeterminado de boa fé.

[13] Cf. art. 12.º, n.º 1, do Regulamento 2016/679/UE, de 27 de Abril de 2016.

[14] Cf. art. 7.º, n.º 2, do Regulamento 2016/679/UE, de 27 de Abril de 2016.

[15] Cf. art. 7.º, n.º 2, e art. 12.º, n.º 1, do Regulamento 2016/679/UE, de 27 de Abril de 2016.

O desequilíbrio significativo, em detrimento do consentumidor, entre os direitos e as obrigações das partes decorrentes do contrato só deve fazer com que uma cláusula seja qualificada como abusiva desde que seja conseguido "em detrimento da exigência de boa fé" [16].

O Tribunal de Justiça concretiza o critério da boa fé distinguindo a boa fé procedimental e a boa fé substantiva e concretiza o critério da boa fé substantiva exigindo duas coisas — que o *fim* prosseguido com a cláusula seja um fim legítimo e que os *meios* seleccionados para o prosseguir sejam adequados, necessários e proporcionados [17] [18].

[16] O direito português refere-se ao desequilíbrio significativo no art. 9.º, n.º 2, alínea b), da Lei de Defesa dos Consumidores e à boa fé, nos arts. 15.º e 16.º da Lei das Cláusulas Contratuais Gerais. O art. 9.º, n.º 2, alínea b), da Lei de Defesa dos Consumidores diz que, "[c]om vista à prevenção de abusos resultantes de contratos pré-elaborados, o fornecedor de bens e o prestador de serviços estão obrigados [...] à não inclusão de cláusulas em contratos singulares que originem significativo desequilíbrio em detrimento do consumidor" e os art. 15.º e 16.º da Lei das Cláusulas Contratuais Gerais, que estão obrigados à não inclusão de cláusulas em contratos singulares que sejam contrárias à boa fé. O art. 15.º consagra princípio geral de que são proibidas as cláusulas contratuais gerais contrárias à boa fé e o art. 16.º, duas concretizações ou especificações do princípio geral, ligadas ao princípio da confiança e ao princípio da primazia da materialidade da regulação ou da primazia da materialidade subjacente.

[17] Cf. acórdão do Tribunal de Justiça de 14 de Março de 2013, no processo C-415/11 (*Aziz*).

[18] Sobre a relação entre o princípio civilístico da boa fé e o princípio constitucional da proporcionalidade, *vide*, p. ex., Peter Rott, "Unfair Contract Terms", in: Christian Twigg-Flesner (coord.), *Research Handbook on EU Consumer and Contract Law*, Edward Elgar, Cheltenham (UK) / Northamption (MA), págs. 287-313; Oliver Gerstenberg, "Constitutional Reasoning in Private Law: The Role of the CJEU in Adjudicating Unfair Terms in Consumer Contracts", in: *European Law Journal*, 2015, págs. 599-621; Nuno Manuel Pinto Oliveira,

Entre os critérios de controlo do conteúdo da Directiva 1993/13/CEE e os critérios de controlo do conteúdo do Regulamento 2016/679/UE há divergências sensíveis.

Enquanto que, no quadro da Directiva 1993/13/CEE, o consentimento não é nunca suficiente para que as cláusulas pré-formuladas sejam válidas e eficazes, devendo fazer-se um controlo dos fins e um controlo dos meios, no quadro do Regulamento 2016/679/UE o consentimento do titular dos dados é quase sempre suficiente. Enquanto que, no quadro da Directiva 1993/13/CEE, o controlo do conteúdo do consentimento está ligado ao conceito de desequilíbrio significativo, no quadro do Regulamento 2016/679/UE, não. Se o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas, o tratamento será, quase sempre, lícito [19].

Embora haja divergências, e divergências sensíveis, há alguma convergência em duas coisas.

O controlo dos fins, implicitamente exigido no art. 3.º, n.º 1, da directiva, tem alguma semelhança com o *princípio da limitação das finalidades* explicitamente consagrado no art. 5.º, n.º 1, alínea b), do regulamento [20]. O controlo dos meios, através dos princípios da adequação e da necessidade, implicitamente exigido no art. 3.º, n.º 1, da directiva, tem alguma semelhança com os princípios da *minimização dos dados* e da *limitação da conservação* explicitamente consagrados no art. 5.º, n.º 1, alíneas c) e e), do regulamento.

Com a exigência de que os dados pessoais recolhidos e tratados sejam "[a]dequados [...] às finalidades para as quais são tratados" [21], está a seguir-se o pensamento subjacente ao *princípio da adequação* e, com a exigência de que os dados pessoais recolhidos e tratados sejam "limitados ao que é necessário relativamente às finalidades para as quais são tratados" [22], ou com a exigência de que os dados pessoais só sejam conservados "durante o período necessário para as finalidades para as quais são tratados" [23], está a seguir-se o pensamento subjacente ao *princípio da necessidade*.

"O princípio da boa fé e o princípio da proporcionalidade — o problema das cláusulas abusivas nos contratos com os consumidores entre direito privado e direito público", in: *Revista do Direito* [da Universidade de Santa Catarina], n.º 53 — 2017, págs. 140-152, in: WWW: <https://online.unisc.br/seer/index.php/direito/article/view/11326/6964 >.

[19] Cf. art. 6.º, n.º 1, alínea a), do Regulamento n.º 2016/679/UE, de 27 de Abril de 2016: "O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; [...]".

[20] Em que se diz que "Os dados pessoais são [...] [r]ecolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades [...]".

[21] Cf. art. 5.º, n.º 1, alínea c), do Regulamento 2016/679/UE, de 27 de Abril de 2016 — sobre o princípio da minimização dos dados.

[22] Cf. art. 5.º, n.º 1, alínea c), do Regulamento 2016/679/UE, de 27 de Abril de 2016 — sobre o princípio da minimização dos dados.

[23] Cf. art. 5.º, n.º 1, alínea e), do Regulamento 2016/679/UE, de 27 de Abril de 2016 — sobre o princípio da limitação da conservação.

5. Consequências da relação de semelhança entre a Directiva 1993/13/CEE, de 5 de Abril de 1993, e o Regulamento 2016/679/UE, de 27 de Abril de 2016. O contributo da Directiva 1993/13/CEE para a interpretação do Regulamento 2016/679/UE

Começando, como comecei, pela relação de semelhança, continuaria com as consequências da relação de semelhança para a interpretação do Regulamento 2016/679/UE.

Em rigor, a complementação entre directiva e regulamento é uma complementação recíproca:

— a directiva contribui, ou pode contribuir, para a interpretação do regulamento;

— o regulamento contribui, ou pode contribuir, para a interpretação da directiva.

Assim, p. ex., as cláusulas contratuais não negociadas por que se ponha em perigo a privacidade das pessoas ou a segurança dos dados pessoais, como as cláusulas contratuais não negociadas por que se ponha em perigo a realização dos princípios da limitação da conservação ou da minimização dos dados, podem ser qualificadas como cláusulas abusivas, no sentido do art. 3.º, n.º 1, da Directiva 1993/13/CEE [24].

Em todo o caso, considerando o tema geral do colóquio, concentrar-me-ei no contributo da directiva para a interpretação do regulamento.

[24] Cf. Natali Helberger / Frederik Zuiderveen Borgesius / Agustin Reyna, "The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law", cit., pág. 11.

6. a) O alcance dos princípios gerais do direito da protecção de dados

Em primeiro lugar, parece-me que a Directiva 1993/13/CEE pode contribuir para tornar mais amplo o alcance dos princípios gerais do Regulamento n.º 2016/679.

O regulamento aplica-se exclusivamente às declarações de consentimento relacionadas com o tratamento de dados pessoais, ou seja, com a "informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados')" [25]; a directiva aplica-se a todas as declarações de consentimento, desde que pré-formuladas — e, aplicando-se a todas as declarações de consentimento, desde que pré-formuladas, poderá fazer com que todo o tratamento de dados, pessoais ou não pessoais, fique sujeito a controlo [26].

7. b) O sentido do princípio da transparência

Em segundo lugar, penso que a directiva pode contribuir para tornar mais claro o sentido do princípio da transparência.

A relação de semelhança entre o texto dos arts. 4.º e 5.º da directiva e o texto dos arts. 7.º e 12.º do regulamento sugere que os critérios desenvolvidos pelo Tribunal de Justiça para determinar o sentido do princípio da transparência no quadro

[25] Cf. art. 4º, alínea 1), do Regulamento 2016/679, de 27 de Abril de 2016.

[26] Cf. Natali Helberger / Frederik Zuiderveen Borgesius / Agustin Reyna, "The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law", cit., pág. 17.

da *directiva* sejam aplicados, ainda que com algumas adaptações ou modificações, para determinar o sentido do princípio da transparência no quadro do *regulamento* [27].

O Tribunal de Justiça distingue duas interpretações possíveis dos arts. 4.º, n.º 2, e 5.º da directiva — a primeira faria com que a exigência de que as cláusulas contratuais se encontrassem redigidas de forma clara e compreensível fosse exclusivamente uma exigência formal e a segunda, com que fosse cumulativamente uma exigência formal e uma exigência substancial. Entre as duas interpretações possíveis, o Tribunal de Justiça dá preferência à segunda:

> "a exigência de transparência das cláusulas contratuais [...] não pode ficar reduzida [...] ao carácter compreensível das mesmas nos planos formal e gramatical" [28].

Entendendo-se a exigência "de maneira extensiva", os arts. 4.º e 5.º da directiva significariam que a cláusula contratual deveria colocar um consumidor médio, ou seja, um consumidor "normalmente informado", "razoavelmente atento" e "razoavelmente avisado" [29], em condições de fazer três coisas.

[27] *Vide* D. C. J. van Caesteren, *Consent Now and Then*, cit., pág. 23.

[28] Cf. acórdãos do Tribunal de Justiça de 30 de Abril de 2014, no processo C-26/13 (*Kásler*); de 23 de Abril de 2015, no processo C-96/14 (*van Hove*); de 9 de Julho de 2015, no processo C-348/14 (*Bucura*); e, por último, de 20 de Setembro de 2017, no processo C-186/16 (*Andriciuc*).

[29] Cf. designadamente acórdão do Tribunal de Justiça de 20 de Setembro de 2017, no processo C-186/16 (*Andriciuc*) — parágrafo n.º 47.

Em condições de compreender o "funcionamento concreto do mecanismo ao qual a cláusula em questão se reporta"; — em condições de compreender a relação entre o funcionamento concreto do "mecanismo" ao qual a cláusula em questão se reporta e o funcionamento concreto dos "mecanismos" aos quais se reportam as demais cláusulas do contrato, ou as demais cláusulas dos demais contratos; — em condições de "avaliar, com fundamento em critérios precisos e inteligíveis, as consequências económicas que daí decorrem" [30].

> "... [A] exigência segundo a qual uma cláusula contratual deve ser redigida de maneira clara e compreensível deve ser entendida como impondo também que o contrato exponha com transparência o funcionamento concreto do mecanismo a que a cláusula em questão se reporta e, sendo caso disso, a relação entre este mecanismo e o estabelecido noutras cláusulas, de modo a que esse consumidor possa avaliar, com fundamento em critérios precisos e inteligíveis, as consequências económicas que daí decorrem para ele" [31].

Entre os elementos relevantes para a avaliação do carácter claro e compreensível da linguagem encontrar-se-iam "todas as circunstâncias que, no momento em que aquele foi celebra-

[30] *Vide* sobretudo o acórdão do Tribunal de Justiça de 23 de Abril de 2015, no processo C-96/14 (*van Hove*) — parágrafo n.º 47 — e o acórdão do Tribunal de Justiça de 20 de Setembro de 2017, no processo C-186/16 (*Andriciuc*) — parágrafo n.º 45.

[31] Cf. designadamente acórdão do Tribunal de Justiça de 20 de Setembro de 2017, no processo C-186/16 (*Andriciuc*) — parágrafo n.º 45.

do, rodearam a sua celebração" [32] e, entre as "circunstâncias que, no momento em que o contrato foi celebrado, rodearam a sua celebração", estariam a informação e a publicidade [33]. Os tribunais deveriam "verificar se [...] foram comunicados ao consumidor todos os elementos susceptíveis de ter incidência no alcance do seu compromisso" [34].

Os critérios desenvolvidos pelo Tribunal de Justiça no quadro da *directiva* poderão porventura ser aplicados, com algumas adaptações e/ou modificações, no quadro do *regulamento*, para se sustentar, p. ex., que a exigência de que todas as comunicações e informações relacionadas com o tratamento de dados sejam apresentadas de modo a que o titular dos dados possa avaliar, com fundamento em critérios precisos e inteligíveis, todas as consequências, económicas e não económicas, que daí decorrem para ele.

[32] Cf. art. 4.º, n.º 1, da Directiva 1993/13/CEE, de 5 de Abril de 1993: "Sem prejuízo do artigo 7.º, o carácter abusivo de uma cláusula poderá ser avaliado em função da natureza dos bens ou serviços que sejam objecto do contrato e mediante consideração de todas as circunstâncias que, no momento em que aquele foi celebrado, rodearam a sua celebração, bem como de todas as outras cláusulas do contrato, ou de outro contrato de que este dependa".

[33] Cf. acórdão do Tribunal de Justiça de 20 de Setembro de 2017, no processo C-186/16 (*Andriciuc*) — parágrafo n.º 46.

[34] Cf. acórdão do Tribunal de Justiça de 20 de Setembro de 2017, no processo C-186/16 (*Andriciuc*) — parágrafo n.º 46.

8. c) O sentido dos princípios da licitude, da adequação, da necessidade e da proporcionalidade

Em terceiro lugar, penso que a directiva pode contribuir para tornar mais claro o sentido dos princípios da licitude, da adequação, da necessidade e da proporcionalidade.

O art. 6.º do Regulamento n.º 2016/679/UE distingue o tratamento dos dados pessoais ligado ao consentimento do titular e o tratamento dos dados pessoais desligado do consentimento do titular, com base em algum fundamento legítimo, previsto pelo direito da União Europeia ou dos Estados Membros da União Europeia.

Entre os fundamentos legítimos estão, p. ex., a circunstância de o tratamento ser necessário (i) "para diligências pré-contratuais a pedido do titular dos dados", (ii) para o cumprimento de um dever contratual, (iii) para o cumprimento de um dever legal [35], (iv) para a defesa de interesses vitais do titular de alguma pessoa singular, (v) para o exercício de funções de interesse público, (vi) para a prossecução dos interesses legítimos do responsável pelo tratamento, ou (vii) para a prossecução dos interesses legítimos de terceiros, "excepto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais [...]".

O art. 7.º do Regulamento n.º 2016/679/UE, esse, exige uma atenção e um cuidado especiais para a avaliação da licitude ou

[35] O art. 6.º, n.º 1, alínea c), fala do "cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito" — e, não se tratando de um dever contratual ("de uma obrigação jurídica") necessária ao cumprimento do contrato, tratar-se-á normalmente de um dever legal.

da ilicitude do tratamento de dados ligado *exclusivamente* ao consentimento do titular:

> "Ao avaliar se o consentimento é dado livremente," diz-se no art. 7.º, e em especial no n.º 4 do art. 7.º, "há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato".

A atenção e o cuidado especiais exigidos pelo art. 7.º do regulamento devem ser ainda mais *especiais*, ainda mais extensos e mais intensos, desde que a declaração de consentimento tenha sido previamente formulada pelo responsável pelo tratamento.

As declarações de consentimento previamente formuladas põem um particular perigo — o perigo do *abuso do consentimento* [36] — e o particular perigo posto pelas declarações de consentimento previamente formuladas, de *abuso do consentimento*, poderá e porventura deverá ser prevenido através de um duplo controlo, de um controlo dos fins prosseguidos e de um controlo dos meios seleccionados pelo responsável pelo tratamento.

O considerando n.º 42, em ligação com o n.º 43, depõe fortemente em favor de uma interpretação restritiva do art. 6.º, e de uma interpretação restritiva nos seguintes termos: Caso a

[36] Expressão de Natali Helberger / Frederik Zuiderveen Borgesius / Agustin Reyna, "The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law", cit., pág. 17.

declaração de consentimento tenha sido previamente formulada pelo responsável pelo tratamento, o consentimento do titular não deverá porventura ser considerado como *condição suficiente* para o tratamento dos seus dados pessoais seja lícito.

O considerando n.º 42 sugere-o, ao dizer que, em conformidade com a Directiva 1993/13/CEE, a declaração de consentimento pré-formulada não deve ter cláusulas abusivas.

Ou seja, que a declaração de consentimento pré-formulada não deve conter cláusulas que não sejam adequadas ou que não sejam necessárias para prosseguir interesses legítimos.

O considerando n.º 43 *reforça* aquilo que o considerando n.º 42 *sugere*, ao dizer que

> "[a] fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento".

Quando a declaração de consentimento para o tratamento de dados pessoais esteja ligada a um contrato entre um profissional e um consumidor e, estando ligada a um contrato entre um profissional e um consumidor, tenha sido previamente formulada pelo responsável pelo tratamento (= pelo profissional), não haverá porventura um *desequilíbrio manifesto* [37]?

[37] O facto de o considerando n.º 42 se referir exclusivamente ao caso em que "o responsável pelo tratamento é uma autoridade pública, pelo que é improvável que o consentimento tenha sido dado de livre vontade em

9. d) Consequências substantivas da violação do direito da protecção de dados

Em quarto lugar, parece-me que a Directiva 1993/13/CEE pode contribuir para tornar mais claras as consequências da violação dos princípios e das regras do Regulamento 2016/679/UE.

O art. 7.º, n.º 2, do regulamento diz, na sua primeira frase, que, "[s]e o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples", e continua dizendo, na sua segunda frase, que

> "[n]ão é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento".

Estando em causa declarações de consentimento pré-formuladas, o sentido dos termos "[n]ão é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento" deve relacionar-se com o art. 6.º da Directiva 1993/13/CEE, e o art. 6.º da Directiva 1993713/CEE deve relacionar-se com as disposições da Lei de Defesa das Consumidores e da Lei das Cláusulas Contratuais Gerais sobre o controlo de inclusão e sobre o controlo de conteúdo.

todas as circunstâncias associadas à situação específica em causa", é só por si insuficiente para se sustentar a conclusão contrária — a referência aos casos em que o responsável pelo tratamento é uma autoridade pública é só exemplificativa.

Quando haja uma violação do regulamento, que se concretize na violação do princípio da transparência, o caso relacionar-se-á com o controlo de inclusão.

O que significa que deverá aplicar-se, directamente ou indirectamente, o art. 8.º da Lei das Cláusulas Contratuais Gerais — significa que as cláusulas que tenham sido *afectadas*, as partes da declaração de consentimento que tenham sido *contaminadas* ou *viciadas*, devem considerar-se excluídas do negócio jurídico singular.

Quando haja violação do regulamento, que se concretize na violação dos princípios da licitude ou da proporcionalidade, o caso relacionar-se com o controlo de conteúdo.

O que significa que deverá aplicar-se, directa ou indirectamente, o art. 12.º da Lei das Cláusulas Contratuais Gerais — significa que as cláusulas *afectadas*, que as partes da declaração de consentimento que tenham sido *contaminadas* ou *viciadas* devem considerar-se inválidas e que, dentro das cláusulas inválidas, devem considerar-se nulas [38].

10. e) Consequências processuais da violação do direito da protecção de dados. O contributo da acção inibitória para a efectivação dos princípios e das regras do Regulamento 2016/679/UE, de 27 de Abril de 2016

Em quinto e último lugar, estou convencido de que a directiva pode contribuir para tornar mais eficaz o regulamento.

[38] Cf. Nuno Manuel Pinto Oliveira, *Princípios de direito dos contratos*, Coimbra Editora, Coimbra, 2011, pág. 243.

Como as cláusulas contidas na declaração de consentimento podem ser cláusulas abusivas, parece-me que poderá ser proposta uma acção inibitória para prevenir ou para proibir práticas violadoras do Regulamento 2016/679/UE [39].

O art. 7.º da Directiva 1993/13/CEE constitui os Estados membros da União Europeia no dever de providenciarem para que, "no interesse dos consumidores e dos profissionais concorrentes, existam meios adequados e eficazes para pôr termo à utilização das cláusulas abusivas nos contratos celebrados com os consumidores por um profissional", e o art. 7.º foi transposto para o direito português pelo art. 10.º da Lei de Defesa dos Consumidores e pelos arts. 25.º a 35.º da Lei das Cláusulas Contratuais Gerais.

Entre as consequências da possibilidade de se propor uma acção inibitório está a legitimidade processual, p. ex., das associações de consumidores e do Ministério Público.

Em alguns países, como a Alemanha, as associações de consumidores propuseram acções inibitórias para proibir as cláusulas abusivas contidas em declarações de consentimento para o tratamento de dados pré-formuladas pela Apple, ou por redes sociais como o Facebook, o LinkedIn, o Instagram ou o Twitter [40] — devendo admitir-se que a sua acção se estenda

[39] Cf. Peter Rott, "Data Protection Law as Consumer Law – How Consumer Organisations Can Contribute to the Enforcement of Data Protection Law", in: *Journal of European Consumer and Market Law*, vol. 6 (2017), págs. 113-119; ou Natali Helberger / Frederik Zuiderveen Borgesius / Agustin Reyna, "The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law", cit., págs. 18-19.

[40] Cf. Natali Helberger / Frederik Zuiderveen Borgesius / Agustin Reyna, "The Perfect Match? A Closer Look at the Relationship Between EU Consumer

a todas as declarações de consentimento para o tratamento de dados dos consumidores, contidas em todos os contratos, como, p. ex., contratos de seguro.

II. Conclusão. O considerando n.º 42 do Regulamento 2016/679/UE, de 27 de Abril de 2016, como reflexo da relação de complementaridade entre o direito do consumo e o direito da protecção de dados

O sentido do Regulamento n.º 2016/679/UE, como o de qualquer acto de direito europeu ou de direito nacional, só pode apreender-se relacionando-o com todo o sistema.

O considerando n.º 42 reflecte a relação de complementaridade entre o direito do consumo e o direito da protecção de dados pessoais — entre aquele que é um dos mais importantes de todos os instrumentos do direito europeu do consumo, a Directiva 1993/13/CEE, e aquele que é seguramente o mais importante de todos os instrumentos do direito europeu da protecção de dados pessoais, o Regulamento 2016/679.

Face à relação de complementaridade entre os dois sistemas, o direito do consumo pode contribuir para tornar mais amplo o alcance dos princípios gerais do direito da protecção de dados pessoais; pode contribuir para tornar mais claro o sentido do princípio da transparência; pode contribuir para tornar mais claro o sentido dos princípios da licitude, da adequação, da necessidade e da proporcionalidade; e pode contribuir para tornar mais eficaz o direito da protecção de todas as pessoas

Law and Data Protection Law", cit., págs. 18-19.

singulares, sejam ou não consumidores, contra os perigos do tratamento de dados pessoais.

PROTEÇÃO DE DADOS E APLICAÇÕES MÓVEIS NA ÁREA DA SAÚDE: UM DIAGNÓSTICO SUMÁRIO[*]

Carolina Cunha

1. De que falamos quando falamos de aplicações móveis na área da saúde

As aplicações móveis na área da saúde são a interface mais visível de sistemas ou de redes que integram diversos componentes[1]. Centrar-nos-emos na aplicação enquanto *plataforma que recolhe dados pessoais* — seja a partir da *inserção manual*, directamente pelo utilizador (desde sintomas físicos variados a simples estados de espírito) ou por um profissional de saúde;

[*] O presente texto corresponde, com pequenas alterações, à conferência que proferi no Colóquio "Seguros, Seguradoras e o Novo Regulamento de Protecção de Dados", que teve lugar na Faculdade de Direito da Universidade do Coimbra no dia 14 de Abril de 2018 — o que explica o seu carácter sintético e o estilo predominantemente coloquial.

[1] Para uma caracterização mais alargada e referências bibliográficas diversas, veja-se Carolina Cunha, "O doente sem horário: breve anatomia dos problemas jurídicos suscitados pelas aplicações móveis na área da saúde", *Direito e Robótica* (Actas do Congresso realizado em 16 de Novembro de 2017 na FDUC), em curso de publicação.

seja *automaticamente* a partir de *dispositivos externos*, como pulseiras, relógios, balanças ou outros aparelhos de medição (p. ex., de glicose ou de tensão arterial) ou, mesmo, a partir de *dispositivos internos*, que tanto podem ser aplicados através de adesivos transdérmicos como implicar a inserção de cateteres finíssimos, eléctrodos, microchips e outros equipamentos que podem ser implantados em *pacemakers*, próteses e, inclusivamente, em órgãos artificiais[2].

2. Características relevantes da informação recolhida, finalidades da sua recolha e processamento e benefícios associados

A *informação* assim recolhida apresenta características peculiares. A mais saliente será o grande volume dos dados, associado a um registo temporal alargado[3]. No caso de recolha automática, gera-se um fluxo quase contínuo e de carácter bastante fidedigno. Tipicamente, os dados coligidos são enviados através da internet para uma "central" ou *cloud* onde irão ser guardados, analisados e processados.

Será interessante referir que o mercado das aplicações é dominado por PMEs: 30% dos empresários que as desenvolvem e comercializam são pessoas singulares e 34,3 % são pequenas sociedades (com 2 a 9 trabalhadores)[4].

A recolha e processamento destes dados visa propósitos variados, desde os mais triviais aos mais nobres[5]. O tratamento da informação recolhida pode ter como objectivo gerar *gráficos, sugestões e avisos* para o próprio utilizador, desde os mais inócuos (dormir mais, fazer mais exercício[6]) aos mais relevantes (consultar o médico se a tensão arterial está continuadamente alta; lembrar de tomar a medicação; detectar potenciais melanomas através de fotografias de uma lesão cutânea). Pode também funcionar primordialmente como um sistema de armazenamento destinado a *fornecer dados clínicos* detalhados aos profissionais de saúde, aquando de consultas presenciais

[2] Podem, ainda, tais dispositivos possuir um carácter efémero: recorde-se que, há poucos meses, a *Food and Drug Administration* norte-americana aprovou o primeiro *comprimido digital*. Junto com o princípio activo, possui um sensor do tamanho de um grão de areia que, depois de engolido, é electricamente activado pelos ácidos do estômago; comunica essa informação a um adesivo usado pelo paciente sobre a caixa torácica o qual, em seguida, envia por Bluetooth, para uma *app* de telemóvel, a data e hora a que foi tomado e a dosagem do comprimido. Tal procedimento serve para assegurar que os pacientes, a quem é prescrito o medicamento para tratar problemas como a esquizofrenia ou a desordem bipolar, *efectivamente tomam* o comprimido; para isso, a informação é facultada a determinados terceiros — além do médico, um máximo de quatro pessoas escolhidas pelo paciente. Cfr. a comunicação da entidade reguladora norte-americana em https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm584933.htm

[3] Cfr. *Green Paper on Mobile Health ("Mhealth")*, COM (2014) 219 final, Brussels, 10.4.2014, p. 7-8, fonte essencial na elaboração deste pequeno estudo.

[4] IDC "*Worldwide and U.S. Mobile Applications, Storefronts, Developer, and In-App Advertising 2011-2015 Forecast: Emergence of Postdownload Business Models*", citado pelo *Greenpaper* na nota 10 da p. 7.

[5] Cfr., novamente, Carolina Cunha, "O doente sem horário", *cit*., para outros desenvolvimentos e referências bibliográficas.

[6] É frequente, nestes casos, que a aplicação inclua uma funcionalidade de partilha em redes sociais, de modo a proporcionar, pela interacção, incentivos a um a dieta, plano de exercício ou estilo de vida saudável.

ou no exercício da telemedicina. Cada vez mais difundidas estão as *apps* destinadas a permitir, em função da análise dos dados recolhidos, *intervenções terapêuticas* mediadas por *decisão humana*, seja do próprio paciente (p. ex., sugerir dosagem de insulina ou de outra medicação), seja do médico (por ex., ajustar a dosagem de um medicamento, amiúde até por intermédio de simples sms), ou intervenções *automatizadas*, isto é, determinadas por programas e algoritmos que processam os dados e, depois, executadas por equipamentos "internos" (pensa-se na ligação directa entre o cateter medidor da glicemia, a *app* de controlo e a bomba de insulina que o paciente tem instalada). Relevantes serão ainda as *intervenções de emergência* (pense-se no caso de um idoso que viva sozinho em casa e que dê uma queda ou que tenha um episódio vascular, sendo o evento captado pela pulseira e comunicado pela *app* a uma central médica).

São manifestos os *benefícios* que estes sistemas de recolha e tratamentos de dados proporcionam[7]. Desde logo, aos *próprios utilizadores*, a quem permitem melhorar o seu bem-estar e a sua saúde, de modo mais simples e expedito, com menos transtornos, custos e deslocações. Mas também ao *Estado*, não só pela redução de custos que possibilitam ao nível da prestação de cuidados de saúde (detecção e tratamento de patologias), o que é relevante sobretudo em face de populações cada vez mais envelhecidas e com um número crescente de doenças crónicas, mas também pelo auxílio que trazem a uma melhor gestão da própria saúde pública (através de um maior conhecimento do que se passa no terreno e alargando

[7] Cfr. Carolina Cunha, "O doente sem horário", *cit.*, para referências bibliográficas.

a possibilidade de intervenções em escala no caso de epidemias, surtos de alergia, etc.). Finalmente, na medida em que o manancial de informação fornecido pelos dados recolhidos por estas *apps* é verdadeiramente novo, em termos de volume, de variedade de parâmetros, de fiabilidade e de continuidade temporal, adquire particular utilidade para a *investigação médico-científica*.

O propósito desta breve comunicação é, todavia, equacionar os problemas que estas aplicações (também) colocam no confronto com o regime instituído pelo Regulamento Geral de Protecção de Dados (RGPD).

3. Os dados relativos à saúde no quadro do RGPD

Para efeitos do RGPD, é patente que a informação que estas aplicações coligem ingressa, toda ela, na categoria de *dados pessoais* (art. 4.º1), pois estão em causa dados relativos a uma pessoa singular, identificada ou identificável, e tais dados são não apenas objecto *de tratamento,* na acepção do art. 4.º2, como tipicamente utilizados para a *definição de perfis*, na medida em que são alvo de "tratamento automatizado com vista a avaliar" certas características pessoais, "em particular para analisar ou prever aspetos relacionados com a saúde e comportamentos da pessoa singular" (art. 4.º4). Quanto ao sujeito ou entidade que desenvolve a aplicação tanto pode assumir o papel de *responsável pelo tratamento* (art. 4.º7) como de *subcontratante* (art. 4.º8), podendo inclusive cumular ambos [8].

[8] Como se sublinha na p. 2 da Carta de 10 Abril 2017 endereçada pelo Grupo de Trabalho do art. 29.º ao editor do Projecto de Código de Conduta em matéria

Os dados coligidos pelas aplicações móveis na área da saúde estão, portanto, inequivocamente sob a alçada do RGPD. A questão é a de apurar se todos eles integram a categoria específica dos *dados relativos à saúde*, amplamente definida no art. 4.º15 como compreendendo os "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". Isto porque, como é sabido[9], os dados relativos à saúde são alvo de um *regime especial, bastante mais restritivo* do que o que protege os vulgares dados pessoais

O Grupo de Trabalho sobre a proteção das pessoas no que diz respeito ao tratamento de dados pessoais, instituído pelo artigo 29.º da Diretiva 95/46/CE (Grupo de Trabalho do Art. 29.º), doravante substituído pelo Comité Europeu para a Proteção de Dados (arts. 68.º, ss.), teve oportunidade de se pronunciar sobre o problema, estabelecendo alguns critérios para determinar *em que casos* os dados processados pelas chamadas aplicações de "lifestyle & well-being" (*apps* de bem-estar) deveriam ser considerados *verdadeiros dados relativos à saúde*[10].

Começou por identificar e incluir num *núcleo inquestionável* os dados que incidem sobre a condição de saúde física ou psíquica e que são gerados num contexto médico-profissional,

de privacidade no domínio das aplicações móveis de saúde. Os documentos deste Grupo de Trabalho do Art. 29.º podem ser acedidos em http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

[9] Ver *infra*, n.º 4.

[10] Cfr. p. 2 do Anexo *Health data in apps and devices* da Carta de 5 de fevereiro de 2015 endereçada pelo Grupo de Trabalho do Art 29.º à Comissão Europeia na sequência da publicação do *Green Paper*.

incluindo os recolhidos por *apps* ou equipamentos, desde que relativos a doenças, patologias, história clínica e tratamentos. Aqui se incluem, p. ex., as *apps* e equipamentos que medem a glicémia ou a tensão arterial (mesmo que usadas em casa, fora de um contexto médico-profissional), ou uma *app* onde o utilizador registe a toma regular de um medicamento, na medida em que essa toma indique um problema de saúde ou patologia[11]. Depois, apoiado na experiência dos Estados-Membros, o Grupo de Trabalho ensaiou uma *extensão da definição* ao *mesmo tipo* de dados recolhidos *noutros contextos*, (*v.g.*, dados sobre alergias ou problemas de saúde revelados a uma companhia aérea ou a uma escola; a informação sobre o QI de uma pessoa ou o facto de usar óculos ou lentes de contacto, etc.) [12].

Note-se que esta posição já estava em harmonia com o (à data, ainda futuro) RGPD, cujo Considerando 35 inclui explicitamente, entre os dados pessoais relativos à saúde, as "informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal [...] e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte".

Excluídos deste universo ficariam, na perspectiva do Grupo de Trabalho, aqueles dados recolhidos pelos equipamentos e aplicações de bem-estar (*lifestyle apps and devices*) a partir dos quais nenhuma conclusão sobre o estado de saúde do sujeito pode ser razoavelmente extraída — pense-se no número de passos relativos a uma única caminhada, ou os passos dados durante alguns dias apenas. Estes *raw data* ou dados em

[11] Cfr. *Draft Code of Conduct on privacy for mobile health applications*, p. 2

[12] Ver p. 2 do citado Anexo *Health data in apps and devices*.

bruto não reclamam a protecção suplementar de que curamos — pelos menos se não forem armazenados pelo criador da *app* e usados para criar um perfil relativo à condição física do utilizador, ou se não forem combinados com outra informação.

Esta última ressalva leva-nos à chamada *zona cinzenta*: dados em bruto que, *quando processados e/ou combinados entre si*, permitem retirar *conclusões* sobre o estado de saúde físico ou psíquico do sujeito. Recorde-se, a título preliminar, que são cada vez mais populares as aplicações e equipamentos de "quantificação do indivíduo" (*quantified self*), as quais permitem ao utilizador registar todo o tipo de informação sobre aspectos da sua personalidade, estados de espírito, funções corporais, padrões de comportamento e, claro, sobre a sua localização. Ora, estes dados, que em si ou isoladamente não mereceriam a protecção adicional, *podem converter-se em dados de saúde por via do processamento*, seja *combinando-os entre si* (num exemplo simples: o peso e a altura relacionados fornecem o índice de massa corporal, o qual, combinado com o número de passos diários fornece um perfil que permite classificar a pessoa como sedentária ou activa, e avaliar certos riscos em termos de saúde), seja *pela sua continuidade temporal* — se um único registo do peso de um sujeito (ou do sono, ou da dieta, ou até de outros parâmetros mais relevantes, como tensão arterial ou ritmo cardíaco) não permite fazer inferências sobre o estado de saúde actual ou futuro desse sujeito, o prolongamento desses registos no tempo (sobretudo se combinado com a idade e o sexo) pode ser utilizado para determinar aspectos significativos da saúde do indivíduo (riscos ligados à obesidade, doença indiciada por excessiva ou rápida perda de peso, hipertensão, arritmia, etc.).

Repare-se que o que está em causa, para efeitos de tutela jurídica, é a *possibilidade de retirar conclusões* sobre o estado de saúde, independentemente do acerto dessas conclusões. Por outro lado, é indubitável que há um *elemento de escala* envolvido na apreciação: pode dizer-se que uma aplicação que registe durante meses ou anos padrões de sono, exercício, peso, dieta, pulsação e outros parâmetros vitais está a processar dados de saúde.

4. A tutela específica dos dados de saúde

A importância prática destas considerações e da classificação que a partir delas se leva a cabo reside na circunstância de *os dados relativos à saúde serem alvo de um regime especial, bastante mais restritivo* do que aquele a que estão submetidos os vulgares dados pessoais.

O ponto de partida será, naturalmente, a *interdição* do art. 9.º1, que estabelece ser "*proibido* o tratamento de dados pessoais [...]relativos à saúde". Não se trata, todavia, de uma proibição absoluta, e a derrogação mais frequentemente utilizada neste domínio será certamente a do *consentimento explícito*, contemplada na al. a) do n.º 2 da mesma norma.

Alerte-se, todavia, que, o *simples facto* de a aplicação proceder ao tratamento dos dados pessoais recolhidos (*independentemente* de serem relativos à saúde) faz com que seja necessário o *consentimento* para efeitos de licitude, nos termos do art. 6.º, 1, a). Por outro lado, se os dados recolhidos no equipamento *não forem transmitidos nem acedidos externamente*, sendo apenas processados no próprio aparelho pelo utilizador, então estaremos *fora do âmbito de aplicação* do RGPD,

na medida em que tal consubstancia um tratamento de dados pessoais "efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas" (art. 2.º2, b).

Numa breve *síntese da disciplina especial* a que estão submetidos os dados de saúde no quadro do RGPD, sublinho os seguintes aspectos:

- A necessidade de ter em conta a natureza especial dos dados para apurar a *compatibilidade* da finalidade *ulterior* com a finalidade *para a qual foram inicialmente recolhidos* (6.º4, c);
- nas *informações adicionais* a fornecer ao titular dos dados pelo responsável pelo tratamento que não os haja recolhido junto desse titular, inclui-se a da existência do direito de retirar o consentimento em qualquer altura (art. 14.º, 2 d);
- uma salvaguarda especial em termos de *decisões automatizadas* e *definição de perfis*, as quais não podem ter por base dados de saúde excepto se houver consentimento ou interesse público importante e, mesmo nesses casos, terão de ser aplicadas medidas adequadas para salvaguardar os direitos, liberdades e legítimos interesses do respectivo titular (22.º4);
- uma *contra-excepção* à excepção de designar por escrito representante na União Europeia (art. 27.º2, a);
- uma *contra-excepção* à inaplicabilidade a PMEs das obrigações de registo de actividade de tratamento (art. 30.º 5)[13];

[13] E recorde-se que, segundo o *Green Paper*, o Mercado das aplicações móveis na área da saúde "is dominated by individuals or small companies, with 30% of mobile app developer companies are individuals and 34.3% are small companies (defined as having 2-9 employees)"

- *obrigatoriedade* de avaliação de impacto para operações de tratamento em grande escala (art. 35.º3 b);
- *obrigatoriedade* de designação de encarregado da proteção de dados para operações de tratamento em grande escala (art. 37.º1, c).

Além desta moldura normativa estabelecida pelo RGPD, é importante ter em atenção o que decorre da lei nacional que a virá a complementar. A Proposta de Lei n.º 120/XIII, actualmente em discussão[14], contém alguns preceitos relevantes no que toca aos dados de saúde, como seja a previsão de que "os dados relativos à saúde podem ser organizados em *bases de dados ou registos centralizados assentes em plataformas únicas*, quando tratados para efeitos das finalidades legalmente previstas, mas tais bases e plataformas devem preencher os requisitos de segurança e de inviolabilidade previstos no RGPD" (art. 30.º) ou, no que toca aos crimes de utilização de dados de forma incompatível com a finalidade da recolha, acesso indevido desvio de dados, o *agravamento das penas para o dobro* dos seus limites quando estejam em causa dados pessoais de uma das

[14] E que visa assegurar "a execução do RGPD na ordem jurídica interna" (já que o RGPD "apresenta um conjunto significativo de normas que requerem ou permitem a intervenção do legislador nacional"), bem como adoptar "as soluções mais adequadas para a proteção dos direitos dos titulares de dados pessoais no contexto da competitividade das empresas portuguesas no quadro da União Europeia". A Proposta encontrava-se, à data da conclusão deste breve estudo, em análise na Comissão Parlamentar de Assuntos Constitucionais, Direitos, Liberdades e Garantias.

categorias do art. 9.º RGPD - onde se incluem os dados relativos à saúde (arts. 46.º2, 47.º2 e 48.º2).

5. Potenciais vulnerabilidades nas apps de saúde no confronto com os comandos do RGPD

Contra o pano de fundo não só desta tutela especial, mas da própria protecção geral de dados do RGPD, podemos identificar (potenciais ou efectivas) vulnerabilidades apresentadas pelas aplicações móveis na área da saúde e bem-estar, justificando algumas cautelas[15].

No que respeita ao *consentimento do titular dos dados* para o respectivo tratamento não se olvide que deverá ser *explícito* (art. art. 9.º, 1 a), ou seja, a sua prestação tem de implicar uma acção positiva e unívoca por parte do utilizador — não bastando, por exemplo, a falta de reacção à declaração da intenção de processar os dados. O consentimento para proceder ao tratamento dos dados para as finalidades específicas indicadas pela aplicação deve ser prestado *antes* de o titular instalar a aplicação ou *no momento* em que a instala; para maximizar o esclarecimento, pode o consentimento ser *modular e contextualizado*, ou seja, prestado à medida que se vai avançando na utilização da *app*, mas sempre antes do tratamento dos dados em causa.

A *retirada do consentimento* (cfr. art. 7.º3) deve operar através de mecanismos acessíveis e fáceis de compreender (*v.g.*,

[15] Recolho algumas notas que me parecem essenciais abordadas pelo *Draft Code of Conduct on privacy for mobile health applications*.

apagando os dados pessoais — no aparelho ou remotamente — ou simplesmente desinstalando a aplicação). Em qualquer caso, implicará o apagamento dos dados do utilizador de *todos os sistemas* controlados pelo responsável pelo tratamento.

No que respeita aos *princípios* que norteiam o tratamento de dados pessoais, são pertinentes diversos alertas.

Desde logo, no que toca à chamada *limitação das finalidades* (prevista no art. 5.º1, b), sublinhe-se que as ditas finalidades têm de ser *prévia e claramente definidas* e deverão possuir uma *ligação relevante* com as funcionalidades da aplicação, não sendo permito o tratamento de dados para finalidades incompatíveis com as comunicadas ao e autorizadas pelo utilizador (por ex., as *apps* que monitorizam o nível de glicémia de pacientes diabéticos não podem vender essa informação às empresas que comercializam a medicação correspondente[16]). Para exibição de *anúncios específicos*, que impliquem a partilha de dados com terceiros ou a criação de perfis, tem de haver um consentimento explícito prévio, um veradeiro *opting-in* do utilizador[17].

O respeito pela *minimização dos dados* (art. 5.º1 c) implica não coligir ou processar mais dados do que os estritamente ne-

[16] A menos, claro, que obtenham consentimento explícito para esse uso.

[17] Já se os anúncios forem genéricos, *i.e.*, não implicarem a partilha de dados pessoais, pode bastar um *direito de opting-out*. Questão interessante é a de saber se a própria utilização da aplicação pode ficar condicionada à exibição de anúncios. Na versão inicial do *Draft Code of Conduct* sugeria-se que sim, mas o Grupo de Trabalho do art. 29.º, na Carta de 10 abril 2017, veio sublinhar que isso seria susceptível de conflituar com o art. 7.º4 do RGPD pelo menos no que toca ao *behavioural advertising*, uma vez que o consentimento para a utilização de dados com vista à exibição de anúncios não é um elemento necessário à prestação do serviço ou execução do contrato

cessários para finalidades da aplicação (num exemplo simples: se para o correcto funcionamento da aplicação basta indicar a idade ou, até, um intervalo de idades, não se deve recolher e armazenar também a data de nascimento).

Já a *limitação da conservação* (art. 5.º, 1 e) requer que os dados sejam apagados quando deixarem de ser relevantes para as funcionalidades da aplicação[18].

Quanto à *protecção de dados desde a concepção* (art. 25.º1), implicará a adopção de medidas de segurança para evitar a perda ou destruição de dados, bem como o acesso ou a revelação não autorizados. Alem da pseudonimização de dados, pode implicar a criação de mecanismos de autorização de acesso à *app*, que detectem e evitem o acesso não autorizado, ou, mesmo, a encriptação (quer para os dados armazenados no aparelho, ou remotamente na *cloud*, quer para os dados em trânsito entre o aparelho e o servidor).

A *protecção de dados por defeito* (art. 25.º2) conduzirá a *opções de base* que impliquem uma menor invasão da privacidade, ainda que o utilizador a quem é dada a escolha não exprima a sua preferência quanto ao tipo de tratamento dos seus dados — por exemplo, se a aplicação permite que os utilizadores partilhem os seus dados numa rede social, esta opção deve estar, por defeito, desligada.

Para assegurar o *direito de acesso do titular dos* dados (art. 15.º), as informações que o RGPD exige que lhe sejam dispo-

[18] O que levanta algumas questões interessantes, como a de saber se, caso a aplicação não seja utilizada durante um certo período de tempo, se deve considerar que os dados "perecem" e terão de ser apagados, ainda que o utilizador não tome qualquer iniciativa nesse sentido.

nibilizadas devem estar acessíveis para consulta em qualquer momento após a instalação da aplicação.

Também no domínio das aplicações móveis na área da saúde os *códigos de conduta* e os *procedimentos de certificação* estimulados pelo RGPD terão um papel a desempenhar. Existe uma Proposta de Código de Conduta em discussão, que já foi analisada pelo agora extinto Grupo de Trabalho do art. 29.º e sujeita a algumas críticas e sugestões, aguardando-se para breve uma nova versão[19].

[19] O document, já várias vezes citado, intitulado *Draft Code of Conduct on privacy for mobile health applications*. A última apreciação do Grupo de Trabalho a este documento está contida na Carta de 11 de Abril de 2018 e identifica, ainda, algumas fragilidades, aconselhando a inclusão de um maior número de exemplos e de indicações de boas práticas.

Recorde-se que o RGPD pretende estimular a adopção de códigos de conduta com vista a facilitar a aplicação efetiva das suas normas tendo em conta as características específicas do tratamento efetuado em determinados setores e as necessidades particulares das micro, pequenas e médias empresas (cfr. Considerando 98 e arts. 40.º e 41.º), bem como estimular a adopção de procedimentos de certificação e selos e marcas de proteção de dados, que permitam aos titulares avaliar rapidamente o nível de proteção proporcionado pelos produtos e serviços em causa, reforçando a transparência e o cumprimento do regulamento (previstos e regulados nos arts. 42.º e 43.º).

Esta intenção do legislador é patente em determinadas consequências de regime associadas ao cumprimento de códigos e certificações aprovados, em particular no domínio do ónus da prova, como por exemplo as previstas no art. 23.º3 (a sua adopção/observância pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento), no art. 32.º, 3 (o cumprimento de códigos de conduta pode ser utilizado como elemento para demonstrar a observância da obrigação de assegurar um nível de segurança adequado ao risco) ou no art. 35.º8 (o cumprimento de códigos de conduta é um elemento a ter na devida conta no âmbito da avaliação de impacto).

6. Algumas questões pertinentes: a utilização posterior dos dados para finalidades diferentes das especificadas e a portabilidade dos dados

Segundo o *princípio da limitação das finalidades*, os dados pessoais são "recolhidos para finalidades determinadas, explícitas e legítimas" e não podem "ser tratados posteriormente de uma forma incompatível com essas finalidades" (art. 5.º, b). Pergunta-se, então: além do processamento dos dados para as finalidades ligadas ao *funcionamento da aplicação* (que terão sido consentidas), para que *outros propósitos* pode o responsável pelo tratamento utilizar os dados recolhidos?

Dir-se-á: para todos as outras finalidades em relação às quais tenha obtido o *consentimento* do titular (as quais passam a ser "finalidades especificadas" nos termos do 6.º, 1, a)[20].

Na ausência de consentimento, todavia, os dados ainda poderão ser utilizados para *fins que sejam considerados compatíveis* com as finalidades para que foram recolhidos, compatibilidade apurada com base nos critérios do art. 6.º4. Acresce, com especial pertinência para os dados de saúde, que, mesmo sem consentimento, os dados poderão vir a ser usados *para fins de investigação científica* (em sentido lato, abrangendo, por exemplo, o desenvolvimento tecnológico e a demonstração, a investigação fundamental, a investigação aplicada e a investigação financiada pelo sector privado — cfr. o Considerando 159) ou *estatísticos*[21]. Em ambos os casos, o tratamento *não é considerado incompatível* com as finalidades iniciais (art. 5.º, 1 b; reiterado pelo 9.º2, j) para os dados pessoais relativos à saúde com mais algumas salvaguardas), *desde* que seja feito em conformidade com as *cautelas* prescritas pelo art. 89.º1.

Daqui se conclui que utilização dos dados para (outras) finalidades ulteriores bastante comuns nesta área da saúde e bem-estar — pense-se na sua *comercialização* junto de anunciantes, de empresas que realizam estudos de mercado, de companhias de seguros, ou até de entidades patronais — *só será tipicamente possível obtendo o prévio consentimento* do titular, pois nenhuma das outras excepções consagradas terá aplicação[22]. E, ainda assim, há que ter em atenção o que decorre do art. 21.º2: quando os dados pessoais forem tratados para efeitos de comercialização directa, o titular tem o *direito de se opor a qualquer momento*, oposição que inclui a definição de

[20] Nomeadamente: "em todo o caso, deverá ser garantida a aplicação dos princípios enunciados pelo presente regulamento e, em particular, a obrigação de informar o titular dos dados sobre essas outras finalidades e sobre os seus direitos, incluindo o direito de se opor" e "deverá ser proibido proceder [...] ao tratamento posterior de dados pessoais se a operação não for compatível com alguma obrigação legal, profissional ou outra obrigação vinculativa de confidencialidade".

[21] O tratamento dos dados obtidos via *mHealth* poderá trazer contributos significativos em áreas como a epidemiologia, o desenvolvimento de mecanismos de detecção e prevenção de doenças variadas ou a redução das fases de teste para certos medicamentos (p. 7, Anexo *Health data in apps and devices*). Ver também as referências expressas no Considerando 157.

Resta acrescentar que está sobretudo aqui em causa a mais-valia ligada ao tratamento de grandes blocos de dados (os chamados *big data*): a "capacidade de analisar diversos conjuntos não-estruturados de dados provenientes de variadas fontes", estabelecendo ligações entre eles para extrair informação potencialmente valiosa de uma forma automatizada e eficiente em termos de custos (*Green Paper* p. 9).

[22] *Draft Code of Conduct on privacy for mobile health applications*, p. 8.

perfis relacionada com a comercialização[23]; se o titular vier a exercer esse direito, os dados pessoais deixarão de ser tratados para esse fim.

Claro que a questão se porá em termos diferentes se o responsável pelo tratamento levar a cabo uma *anonimização irreversível dos dados*, de tal forma que se torne impossível voltar a estabelecer a sua ligação com os indivíduos a que respeitam (*i.e.*, impossível proceder à respectiva re-identificação). A partir daí, os dados já poderão ser licitamente processados, re-utilizados para qualquer finalidade ou até comercializados *sem estarem sujeitos aos comandos do RGPD*, que só pretende proteger informações relativas a pessoas identificadas ou identificáveis[24]. Todavia, esta alternativa pode não ser viável. Desde logo, porque a anonimização *não é um procedimento simples*[25] — não se confunde com a mera pseudonimização [26] — e parece particularmente difícil de alcançar no âmbito de

[23] Ver também o Considerando 70.

[24] Considerando 26: "Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas".

[25] Cfr. a "Opinion 05/2014 on Anonymisation Techniques", adoptada pelo Grupo de Trabalho do art. 29.º em 10 de Abril de 2014, 0829/14/EN WP216.

[26] E, como se lê no Considerando 26 "Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. 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

dados relativos à saúde[27]. Mas também porque os dados totalmente anonimizados podem *perder boa parte do interesse,* quer para efeitos de comercialização, quer mesmo de investigação científica.

Finalmente, com o objectivo de r*eforçar o controlo do titular sobre os seus próprios dados*, o RGPD atribui-lhe no art. 20.º não só o *direito de receber* os dados pessoais que tenha fornecido num formato estruturado, de uso corrente e de leitura automática (portanto, pode guardá-los e arquivá-los para uso pessoal como bem lhe aprouver[28]) como, ainda, 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": é a chamada *portabilidade dos dados*.

Os únicos requisitos para a constituição destes direitos — a saber, que o tratamento seja realizado por meios automatizados e

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".

[27] Ou "very challenging", como se adverte na p. 11 do *Draft Code of Conduct on privacy for mobile health applications*.

[28] Cfr. as *Guidelines on the right to data portability*, revistas e adoptadas a 5 de Abril de 2017 pelo Grupo de Trabalho do art. 29.º, p. 5: "For example, a data subject might be interested in retrieving his current playlist (or a history of listened tracks) from a music streaming service, to find out how many times he listened to specific tracks, or to check which music he wants to purchase or listen to on another platform. Similarly, he may also want to retrieve his contact list from his webmail application, for example, to build a wedding list, or get information about purchases using different loyalty cards, or to assess his or her carbon footprint".

que tenha por base o consentimento ou um contrato — estão *geralmente verificados* no domínio das aplicações móveis de saúde.

Este direito à portabilidade dos dados será também (reflexamente) bastante importante para fomentar uma *saudável concorrência entre empresas* e *assegurar a livre escolha do consumidor*, na medida em que elimina o constrangimento dos *switching costs* relacionados com a perda do volume de informação que o titular já disponibilizou à aplicação que agora quer abandonar. E é bastante facilitado, em termos práticos, pela específica previsão de um direito a que os dados pessoais sejam *transmitidos diretamente entre os responsáveis* pelo tratamento, desde que tal seja tecnicamente possível (art. 20.º3).

A portabilidade dos dados traz para primeiro plano a questão conexa da *interoperabilidade*, daí que o regime que acabo de descrever seja complementado pelo propósito de encorajar os responsáveis pelo tratamento a desenvolver formatos interoperáveis que permitam a portabilidade[29]. No domínio da saúde móvel, a interoperabilidade pode ser complexa (dependendo do tipo de dados) e a falta de *standards* vinculativos é apontada como um factor de entrave à inovação e às economias de escala, particularmente problemática para as PMEs e pessoas singulares que constituem os principais protagonistas deste mercado[30].

[29] Cfr. Considerando 68 e *Guidelines on the right to data portability*, p. 18.

[30] *Green Paper*, p. 14-15

O REGULAMENTO DE PROTECÇÃO DE DADOS PESSOAIS (2016/679) NO CONTEXTO DOS DESAFIOS DA ACTIVIDADE SEGURADORA
— O CASO PARTICULAR DOS SEGUROS DE SAÚDE

Filipe Miguel Cruz de Albuquerque Matos

I . Uma primeira aproximação ao problema

Com a entrada em vigor na Ordem Jurídica Portuguesa do Regulamento 2016/679 27 de abril de 2016, muitos são os desafios colocados pelas exigências estabelecidas neste diploma comunitário em matéria de tratamento de dados pessoais, suscitando-se uma multiplicidade de questões a propósito da necessária e desejável livre circulação de tais dados. Tais desafios fazem-se sentir de um modo particular no âmbito da actividade das seguradoras, uma vez que a actuação das mesmas tem na base um contrato comummente qualificado de *Uberrima Fides*[1].

[1] Acerca da qualificação do contrato de seguro como um contrato de Uberrima Fides (" Utmost Good Faith") , cfr, por todos, o nosso estudo, *Uma Outra Abordagem em Torno das Declarações Inexactas e Reticentes no Âmbito do Contrato de Seguro.* "Os art.os 24.º a 26.º do Decreto Lei n.º72/2008", de 16 de abril, *in Estudos em Homenagem ao Prof. Doutor Jorge de Figueiredo Dias*, Vol. IV, Coimbra, 2010, pg. 617, Martins, Ines Oliveira, O Seguro do Vida enquanto

Razão pela qual, desde sempre a avaliação do risco a segurar pelas companhias de seguro ficou dependente das informações, ou, dos dados que lhe são transmitidos pela contraparte do contrato quanto ao quid a segurar.

Não admira assim que no universo dos seguros se viva intensamente a dialéctica consubstanciada, na protecção, por um lado, das pessoas relativamente ao tratamento dos dados pessoais, que é perspectivado, tanto pelo Direito Internacional[2], quanto pelo Direito Interno, como um direito fundamental[3],

tipo Contratual Legal, Coimbra, 2010, pgs. 55-56, POÇAS, LUIS, *O Dever de Declaração Inicial do Risco no Contrato de Seguro, Coimbra,* 2013, pg. 36 e ss. , Buttaro, Luca, " Assicurazione (contratto di)", *in Enciclopedia Del Diritto,* Vol. III, 1958, pg.483. Em sentido diverso, Margarida Lima Rego considera que em face do regime resultante dos art.os 227.º n.º1 e 762.º n.º2 do Código Civil não há razão justificativa para qualificar o contrato de seguro como um contrato de Uberrima Fides. A autora entende, a este propósito, que a exigência genérica constante do art.º 762.º n.º2, não se afirma com maior intensidade no contrato de seguro que nos demais contratos, cfr, Rego, Margarida Lima, *Contrato de Seguro e Terceiros, Estudo de Direito Civil*, Coimbra, 2010, pgs. 441-442 (especialmente nota 1170).

[2] Cfr, a este propósito, os arts. .º 8.º n.º1 da Carta dos Direitos Fundamentais da União Europeia, e o 16.º, n.º1 do Tratado sobre o Funcionamento da União Europeia (TFUE).

[3] Importa salientar que no panorama Europeu, a Constituição Portuguesa de 76 se revelou pioneira em matéria de protecção de dados pessoais, procedendo ao tratamento desta matéria de um modo indirecto no contexto dos Direitos, Liberdades e Garantias no art.º 35.º. Apesar de não se ter registado um reconhecimento expresso de um direito à protecção de dados pessoais, este preceito coloca em relevo os perigos decorrentes para os direitos fundamentais da utilização das tecnologias informáticas, apesar de na redacção originária da constituição, o legislador se reportar aos registos mecanográficos. Como a este propósito sugestivamente esclarece Sousa Pinheiro, o art.º 35.º da Constituição de 76 foi" o primeiro caso de constitucionalização expressa da relação Informática/Direitos Fundamentais", cfr, PINHEIRO, A. SOUSA, *Privacy e Protecção de Dados Pessoais, A Construção Dogmática do Direito à Identidade Informacional*, Lisboa, 2015, pgs.665-666.

e na tutela por outro, do direito das seguradoras acederem a um conjunto de informações tidas por necessárias ou relevantes para poderem, de forma esclarecida e sã, decidirem sobre a celebração dos contratos de seguro.

Uma tal colisão de direitos, sentida de modo particularmente significativo no mundo dos seguro, constitui expressão paradigmática de uma realidade conflitual bem característica das sociedades de informação, onde se multiplicam as situações onde o ataque à privacy[4] e aos dados pessoais é de-

[4] Apesar de alguma discussão em torno da origem do direito à reserva da vida privada, havendo quem a localize numa decisão judicial Francesa do séc. XIV, certo é que o marco histórico de referência deste direito de personalidade se traduz no estudo do Jurista Norte-Americano Samuel Warren e Louis Brandeis, intitulado The right to privacy, The Implicit Made Explicit, e publicado em 1890 na Harvard Law Review. Desde então, os tribunais Norte Americanos têm sido chamados a pronunciar-se sobre questões desta índole. A admissibilidade deste direito foi-se também afirmando no âmbito dos ordenamentos continentais, e muito se tem discutido na doutrina e jurisprudência sobre a delimitação do respectivo âmbito, doutrina e jurisprudência que entre nós encontra um importante arrimo no art.º 80.º n.º2 do Código Civil. No contexto do Direito Norte Americano, Direito pátrio da tutela da reserva da vida privada, tem-se assistido a uma tendência para alargar desmensuradamente o âmbito normativo deste direito, nele se incluindo uma panóplia de faculdades entre as quais se destaca o direito a abortar e o direito à eutanásia. Como, a este propósito justamente sublinha Rita Amaral Cabral "Tem-se, contudo, observado que a "colonização" das liberdades individuais pelo direito à privacidade tende a esvaziar este último e a privá-lo de utilidade na salvaguarda dos interesses que inicialmente construíram o seu objecto.", cfr, Cabral, Rita Amaral, "O Direito à intimidade da Vida Privada (Breve reflexão acerca do art.80.º do Código Civil)",*in Estudos em memória do Professor Doutor Paulo Cunha*, Lisboa, 1989, pg.391. Ainda a pro-

sencadeado pela necessidade do Estado ou entidades privadas, em nome da prossecução do interesse público, da segurança colectiva, da transparência administrativa, ou de outros interesses legítimos acederem a um conjunto de informações dos administrados ou dos cidadãos.

Num mundo profundamente dominado pela racionalidade tecnológico-informática, as situações de conflito acabadas de mencionar multiplicam-se, com uma intensidade exponencial, bastando, a este propósito, tomar em consideração o papel de relevo assumido nas sociedades modernas pela videovigilância, pelas redes sociais e pela radiofrequência.

Em face de todas estas considerações, não admira que a questão da protecção dos dados pessoais se encontre hoje inscrita na agenda dos ordenamentos jurídicos civilizados, e tenha sido objecto de uma atenção especial pelo direito comunitário que recentemente se debruçou sobre uma tal matéria no regulamento 2016/679 , sendo que já há mais de duas décadas atrás a União Europeia tinha disciplinado este universo através da Directiva 95/46/CE do Parlamento e do Conselho, de 24 de Outubro, revelando-se particularmente sensível aos ecos sentidos nas sociedades ocidentais a partir de finais da década de 60 do século passado, que apelavam para a necessidade de uma protecção adequada dos dados pessoais.

Encontrando-se subjacente à disciplina jurídico-positiva da protecção de dados pessoais um conflito entre prerrogativas públicas que justificam o conhecimento de informações, ou de dados pessoais dos cidadãos, por um lado, e o direito destes à privacidade e à tutela de outros bens fundamentais de personalidade, como a Honra e o Bom Nome, a imporem, por outro, uma limitação no acesso aos dados pelos poderes públicos, importa então encontrar o ponto óptimo do equilíbrio, de modo a que qualquer regulamentação sobre esta matéria consiga uma optimização dos direitos em confronto, apesar das necessárias compressões recíprocas a que os mesmos tendam a ser submetidos.

No fundo, este discurso encontra-se profundamente inspirado pelas exigências regulativas da concordância prática, que apesar ser um princípio com um forte desenvolvimento dogmático no universo publícistico[5], não deixa, no entanto, de assumir uma forte influência na densificação dos critérios orientadores dos conflitos mencionados no n.º1 do art.º 335.º do Código Civil. De resto, podemos qualificar este princípio jurídico fundamental como um princípio em forma de norma[6], uma vez que as directrizes fundamentais que o densificam encontram respaldo na lei, prescrevendo-se no art.º 335.º n.º1, a propósito do conflito entre direitos iguais ou da mesma espécie "... que os titulares dos direitos devam ceder na medida do

pósito da inclusão do direito a abortar na Privacy Norte-Americana, cfr, Pinto, Paulo Mota, "A Protecção da Vida Privada e a Constituição", *in B.F.D.*, Coimbra, 2000, pg.160. Sobre a necessidade de proceder a uma mais rigorosa delimitação do âmbito da Privacy Norte-Americana, cfr, Wacks, Raymond, *The Protection of Privacy*, London, 1980, pg.21 e ss.

[5] Para maiores desenvolvimentos em torno do Princípio da Concordância Prática, cfr, Canotilho, J. Gomes, *Direito Constitucional e Teoria da Constituição,*7.ªa ed. , Coimbra,2003,pgs.1282-1283, Andrade, M. Costa, *Liberdade de Imprensa e Inviolabilidade Pessoal- uma Perspectiva Jurídico-Criminal,* Coimbra, 1996, pg. 284 e ss. Quanto ao tratamento civilístico da matéria, cfr, Leitão, L. Menezes*, Direito das Obrigações,*I, 14.ª ed. , Coimbra, 2017, pg.292, Sousa, R. Capelo De, *O Direito Geral de Personalidade,* Coimbra,1995,pg. 548.

[6] Cfr, neste sentido, Bronze, F. Pinto, *Lições de Introdução do Direito*, 2.ª Ed., Coimbra, 2006, pg. 639.

necessário para que todos produzam igualmente o seu efeito, sem maior detrimento para qualquer das partes".

Transpondo-se estas considerações para o universo específico da protecção dos dados pessoais, dir-se-á que a tutela dos direitos de personalidade aqui implicados não pode chegar ao ponto de paralisar certas actividades socialmente lícitas e úteis, sendo certo que sob o pretexto de se desenvolverem um tal tipo de actuações não é possível aos titulares dos respectivos órgãos atingir, de modo significativo, um núcleo de direitos essenciais dos visados pelas mesmas, como é o caso dos direitos de personalidade.

De resto, esta dificuldade de conciliação ou articulação entre valores ou interesses antagónicos, quando esteja em causa a prossecução de interesses sociais ou colectivos prosseguidos por determinadas entidades sempre esteve presente ao longo da história, mesmo antes do surgimento do Estado-Nação.

Com efeito, a necessidade de proceder ao recenseamento das populações, bem como a de definir o cadastro das propriedades, para efeitos militares e de cobrança de rendas, fez sempre surgir conflitos entre o Rei, os Senhores Feudais e a Igreja, a quem, por um lado, eram atribuídos poderes para a realização de tais actos e os súbditos e as populações, que por outro, tentavam furtar-se ao cumprimento dos encargos que por aqueles lhe eram impostos, sobretudo quando os consideravam abusivos.

De resto, a agudização de conflitos desta natureza estiveram na origem de momentos revolucionários que ficaram célebres por determinarem mudanças significativas na organização política e económica das sociedades, bem como das estruturas jurídicas correspectivas, escusando-nos, porém, neste momento de nos debruçarmos sobre tais períodos históricos e alterações jurídicas neles envolvidos, por tal extravasar manifestamente os propósitos da nossa exposição[7].

Importa apenas evidenciar na lógica de preocupações que dominam este estudo, que as inúmeras situações de intromissão em dados pessoais dos cidadãos levadas a cabo por entes públicos, ou por outros particulares têm colocado significativos desafios ao Direito, desafios esses essencialmente colocados no âmbito da temática dos Direitos Fundamentais ou dos Direitos de Personalidade, consoante o tratamento da matéria seja visto numa óptica jusconstitucionalística ou juscivilística.

Nesta sede , não podemos ignorar que a emergência de categorias dogmáticas, como o Direito à Identidade Informacional, ou o Direito à Autodeterminação Informacional, correspondem a respostas do mundo do Direito a solicitações advindas do contexto social (feitas sentir de modo cada vez mais intenso), de proteger os dados respeitantes às pessoas, ou seja, de garantir a tutela de aspectos tidos por absolutamente essenciais para a afirmação da personalidade humana.

Teremos assim ocasião de nos pronunciar sobre uma tal categoria – Direito à Autodeterminação Informacional- , que foi já entre nós objecto de uma dissertação de doutoramento[8], e que é perspectivada como um direito que abrange um conjunto de posições jurídicas diversas, entre as quais se incluem a " (i) natureza garantística relativamente à identidade pessoal;

[7] Refira-se, a título puramente exemplificativo, a alteração introduzida no nosso ordenamento jurídico civil consubstanciada na revogação do instituto da Enfiteuse.

[8] Referimo-nos, à obra de Alexandre Sousa Pinheiro:" Privacy e Protecção de Dados Pessoais: A Construção Dogmática do Direito à Identidade Informacional", entretanto já citada neste trabalho.

(ii) contribui para a criação de manifestações de exercício ao direito ao livre desenvolvimento de personalidade; (iii) exprime as necessidades de intervenção do poder público no sentido de garantir as condições técnicas para o exercício de uma relação segura e isenta nas áreas das "comunicações electrónicas", (iv) integra o património do direito à protecção de dados pessoais; e (v) integra as posições jurídicas relacionadas com a "protecção da confiança" do individuo nos sistemas convencionais, de modo que possa explorar os recursos da sociedade da informação[9].

O destaque atribuído a este Direito à Autodeterminação Informacional resulta da circunstância de lhe ser conferida pela doutrina e até mesmo por alguns diplomas legislativos uma posição nevrálgica no âmbito da problemática da protecção de dados pessoais, importando proceder mais adiante a uma apreciação crítica acerca de uma tal relevância, juízo esse que implica uma visão de conjunto acerca da arquitectura técnico-jurídica do nosso ordenamento jurídico em matéria de tutela da personalidade.

Independentemente da questão de saber se a protecção dos direitos de personalidade dos titulares de dados pessoais será melhor alcançada através da autonomização do mencionado direito à autodeterminação informacional, ou se uma tal tutela se consegue atingir de modo satisfatório através dos expedientes gerais e tradicionais de tutela da personalidade, (questão essa sobre a qual teremos ocasião de mais tarde nos pronunciar), importa neste momento inicial caracterizar e explicitar uma ideia já atrás difusamente mencionada: os riscos de invasão e ataque aos direitos de personalidade dos titulares dos dados pessoais não têm apenas como fonte a actuação dos

[9] Cfr, Pinheiro, Alexandre S., *Privacy e* ..., ob cit, pgs.818 e 819.

poderes públicos, mas resultam igualmente da intervenção dos particulares.

Ora, a propósito dos múltiplos ataques dirigidos pelos particulares que exigem uma protecção dos titulares dos dados pessoais atingidos contam-se aqueles que são perpetrados através da utilização das novas tecnologias informáticas, revelando-se assim o universo informático um campo propício para a emergência de tais situações ilícitas[10].

Do ponto de vista do fenómeno mais tradicional e usual de ataques causados neste contexto dos dados pessoais pelos poderes públicos, cumpre fazer uma particular menção, atenta a actualidade e a gravidade dos conflitos suscitados, ao flagelo do terrorismo que se tem estendido nos últimos tempos no mundo ocidental. Fundando-se a legitimidade dos poderes públicos neste contexto em ponderosas razões de segurança pública, cumpre equacionar devidamente, qual o âmbito e espectro de dados pessoais dos cidadãos que será lícito às entidades públicas aceder.

Ora, são precisamente estas múltiplas situações, de contornos variados, advindas do universo das relações paritárias típicas do Direito Privado ou do domínio das relações de supra

[10] A propósito das potencialidades ofensivas da utilização das tecnologias informáticas aos direitos de personalidade dos titulares dos dados pessoais, cfr, por todos, Barbosa, Mafalda Miranda, *Protecção de Dados e Direitos de Personalidade: Uma Relação de Interioridade Constitutiva. Os Benefícios da Protecção e a Responsabilidade Civil*, in Estudos de Direito do consumidor, n.º 12, 2017, pg. 76 ss., Lopes, J. Seabra, "A Protecção da Privacidade e dos Dados Pessoais da Sociedade de Informação", *in Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa*, Lisboa,2002,pg.779 e ss. .

infra- ordenação, bem características do universo do Direito Público[11], que vão constituir o espectro da nossa análise.

II. A questão dos Dados Sensíveis e a Protecção de Privacidade

Apesar da referência ao direito à autodeterminação informacional parecer retirar relevo à privacidade como fundamento para a protecção a dispensar aos titulares dos dados pessoais, certo é que não se pode abordar adequadamente este universo temático se não se colocar precisamente no centro da discussão o direito à privacidade.

Importa, na verdade, ter bem presente que o acesso aos dados pessoais considerar-se-á ilícito na medida que o conhecimento de tais informações contenda com aspectos vitais ou nucleares da personalidade dos visados, em termos tais que o aludido conhecimento daquelas por terceiros deva qualificar-se como uma agressão ou intromissão. Em causa está precisamente uma agressão ou intromissão na privacidade dos titulares dos dados, porquanto estes respeitam a aspectos mais ou menos recônditos da personalidade, que os seus titulares pretendem manter resguardados da indiscrição ou conhecimento de terceiros.

[11] Cfr, a este propósito a análise descritiva do Direito enquanto ordem levada a cabo por Castanheira Neves, no âmbito da qual o autor identifica três linhas estruturantes da ordem jurídica, Vide, Neves, A. Castanheira, *O Direito (O Problema do Direito). O Sentido do Direito, Lições ao 1.º ano do Curso Jurídico, Lições Policopiadas,* pg. 7-10.

Torna-se assim absolutamente necessário chamar à colação uma categoria chave no âmbito da tutela dos dados pessoais: a categoria dos *dados sensíveis*.

Poderíamos começar por proceder a uma enumeração casuística dos dados susceptíveis de serem qualificados como sensíveis, e a partir daí discutir acerca da natureza sensível dos mesmos, para posteriormente alcançar uma noção acerca de uma tal categoria.

Sem pretender cair numa atitude conceitualista, explicitarei, desde já, uma característica ou atributo essencial que perpassa nos múltiplos exemplos susceptíveis de serem avançados neste âmbito: tais dados reportam-se a aspectos essenciais à afirmação da personalidade humana, e os seus titulares não se encontram, de todo em todo, interessados em que os mesmos sejam conhecidos de terceiros. Atenta a delicadeza dos aspectos coenvolvidos nesses dados, os seus titulares não apenas desejam afastá-los do conhecimento de um público anónimo, mais ou menos generalizado, como ainda temem que entidades, cujas funções suscitam um necessário acesso aos dados possam utilizá-los para finalidades estranhas aos motivos justificativos do conhecimento. Isto porque, se os titulares dos dados tivessem a possibilidade de optar pela divulgação ou não divulgação dos dados, a escolha recairia naturalmente no segundo termo do binómio.

Em rigor, todos estes aspectos acabados de evidenciar encontram-se incluídos no âmbito normativo do direito à reserva de intimidade da Vida Privada. Basta ter em conta o modo como o Tribunal Constitucional se pronunciou no Acórdão n.º128/92[12]

[12] Cfr, Acórdão n.º128/92, publicado no Diário da República, I série-A, de 9 de setembro de 1993. Este trecho do Acórdão citado em texto, foi, de resto,

acerca do conteúdo a associar a este direito, para nos apercebermos do acerto das conclusões acabadas de assinalar: " no âmbito desse espaço próprio inviolável engloba-se a vida pessoal, a vida familiar, a relação com outras esferas de privacidade (v.g. a amizade), o lugar próprio da vida pessoal e familiar (o lar ou domicilio) e , bem assim, os meios de expressão e de comunicação privados (a correspondência, o telefone, as conversas orais,etc)".

Todas estas dimensões protegidas pelo direito à reserva da vida privada serão melhor explicitadas na noção avançada por Paulo Mota Pinto sobre uma tal realidade[13] "Trata-se, em nossa opinião, do interesse em impedir ou controlar a tomada de conhecimento, a divulgação ou, simplesmente, a circulação de informação sobre a pessoa, isto é, sobre factos, comunicações ou situações relativo (ou próximos) ao indivíduo, e que possivelmente ele considere como íntimos, confidenciais ou reservados. "Trata-se do interesse na autodeterminação informativa, entendida como controlo sobre informação relativa à pessoa".

Ao integrar no conteúdo do direito à reserva da vida privada, o interesse na autodeterminação informativa, o autor, na senda da mesma linha de orientação dominante da civilística Portuguesa, entrelaça a questão do tratamento dos dados pessoais com a tutela do direito à privacidade[14].

reproduzido por um posterior Acórdão do mesmo Tribunal- Acórdão n.º 355/97.

[13] Cfr, Pinto, Mota Paulo, *A Protecção da Vida Privada e a Constituição*, in Boletim da Faculdade de Direito, Vol.LXXVI, Coimbra, 2000, pg.164.

[14] Cfr, neste sentido, Sousa, R. Capelo, *O Direito Geral...,* ob. cit., pg.318 e ss., Cordeiro, A. Menezes, *Tratado de Direito Civil Português,* I, Parte Geral, tomo III, Coimbra,2004, pg.90..

Não podemos, na verdade, deixar de assinalar, que um amplo leque de manifestações de quanto pode ser qualificado como dado sensível, respeita a aspectos significativos da personalidade humana, cuja garantia é assegurada através do direito à privacidade.

Antes de procedermos à análise da disciplina reservada pelo regulamento comunitário aos dados sensíveis, matéria tratada, de modo especial, no art.º 9.º n.º1 deste diploma, importa nesta sede dedicar alguma atenção à jurisprudência Constitucional Portuguesa, que no Acórdão n.º355/97, considerou o seguinte: " Os dados de saúde integram a categoria de dados relativos à vida privada, tais como as informações referentes à origem étnica, à vida familiar, à vida sexual, condenações em processo criminal, situação patrimonial e financeira[15]".

Bem vistas as coisas, também este conjunto diverso de dados sensíveis relativos à vida das pessoas foi considerado, no plano constitucionalístico, como parte integrante do direito à intimidade da vida privada.

Cumpre ainda salientar que relativamente à matéria que constitui o alvo das nossas preocupações – os seguros de saúde -, os dados de saúde foram considerados sensíveis. Um tal enquadramento relativamente aos dados de saúde mantém-se, de resto, bem actual, uma vez que o regulamento comunitário de protecção de dados no seu art.º 9.º, n.º1, lhes atribui o mesmo qualificativo.

Teremos ocasião de nos debruçar mais adiante sobre as implicações e dificuldades suscitadas pela opção feita por este regulamento comunitário quanto à classificação dos dados de

[15] Cfr, in http://www.tribunalconstitucional.pt/tc/19970355.html> (25.11.2011).

saúde, importando por agora problematizar a questão anteriormente já implícita ao longo da exposição: Fará sentido autonomizar um direito à autodeterminação informacional para proceder a um adequado tratamento da matéria da protecção dos dados, ou tal não se revelará necessário, porquanto a tutela dos particulares nesta sede se logra alcançar através do direito à privacidade?

Apesar do estudo da matéria da protecção dos dados pessoais gravitar em torno da tutela da privacidade[16], certo é que uma tal abordagem não deve ser confinada a este direito de personalidade, porquanto no universo em análise pontificam também imperiosas exigências de protecção da identidade pessoal, da Honra, do Bom Nome e do Crédito...

Ora, bem vistas as coisas, importa verdadeiramente averiguar qual a concreta manifestação da personalidade atingida quando uma entidade pública ou privada contenda com a esfera jurídica do titular dos dados pessoais.

Com isto queremos dizer que a protecção da multiplicidade de bens pessoais que são susceptíveis de ser afectados com o tratamento de dados pessoais, poderá ser alcançada através de um direito de conteúdo particularmente elástico, como é o Direito Geral de Personalidade, não se tornando propriamente necessário transpor para o nosso ordenamento jurídico uma categoria dogmática de inspiração germânica — O Direito à Autodeterminação Informacional.

[16] Cfr, a este propósito, Barbosa, Mafalda Miranda, *Protecção de Dados e Direitos*..., ob cit, pg.104 e ss., : " ...os autores não deixam como não devem deixar de fazer reconduzir para o cerne da protecção de dados a privacidade".

Com efeito, a este direito à Autodeterminação Informacional, apesar de se configurar como um "direito-garantia, uma guarda-avançada de certas posições jurídicas activas[17] ", não lhe pode, porém, ser atribuída uma maior amplitude que ao Direito Geral de Personalidade[18].

Como todos sabemos, certas dimensões absolutamente nucleares da pessoa humana, mesmo quando não sejam objecto de uma expressa referência legislativa, não deixam de merecer tutela jurídico-positiva, uma vez que tais formas de manifestação da personalidade humana, encontram guarida no direito geral de personalidade previsto no art.º 70.º. Exemplo paradigmático de quanto estamos a mencionar, com particular relevância neste universo da protecção dos dados, diz respeito ao direito à honra, cuja violação se revela particularmente frequente.

Assim, e para feitos da convocação do instituto de responsabilidade civil, importa averiguar qual o concreto direito de personalidade, ou posição jurídica atingidos por quem procede ao tratamento de dados, sendo que uma tal pesquisa pode fazer-se claramente no âmbito do nosso Direito Geral de Per-

[17] Cfr, Barbosa, Mafalda Miranda, *Protecção de Dados e Direitos*..., ob cit, pg.107.

[18] Não podemos neste contexto esquecer as críticas dirigidas por um certo sector doutrinal à enorme amplitude do âmbito do Direito Geral de Personalidade, considerando-o como uma espécie de abstração inútil, cfr, a este propósito, Ascensão, J. Oliveira, *Direito Civil, Teoria Geral*, Vol. I, Coimbra,2000, pg. 86 e ss., Festas, David de Oliveira, *O Direito à Reserva da Intimidade da Vida Privada do Trabalhador no Código do Trabalho,* in Revista da Ordem dos Advogados, 64, 2004, pg. 396, Do Conteúdo Patrimonial do Direito à Imagem. *Contributo para um Estudo do Seu Aproveitamento Consentido e Inter Vivos,* Coimbra, 2009, pg. 81 (especialmente nota 238).

sonalidade, porquanto o mesmo deve ser perspectivado como um Rahmenrecht[19].

Interessa então, identificar o concreto direito violado[20] com o tratamento dos dados pessoais para poder afirmar a existência de responsabilidade civil do responsável por tal tarefa , e assim sendo , a genérica invocação da violação do propalado direito à autodeterminação informacional corre o risco de se tornar insuficiente para um tal efeito, atenta a indeterminação do conteúdo de um tal direito.

Em face de todas estas considerações, a emergência de um direito à autodeterminação informacional acaba por implicar a criação de um outro direito de conteúdo particularmente elástico e amplo, sem que o mesmo venha garantir a tutela de realidades[21] já cobertas pelo Direito Geral de Personalidade, consagrado no art.º 70.º. Num ordenamento jurídico como o nosso, em que a tutela da Personalidade se pode qualificar de generosa e percursora[22], não nos parece haver razões justificativas de outra ordem, que não sejam as de índole conceptual, a reclamar a emergência de um direito a Autodeterminação Informacional.

[19] Cfr, a este propósito, o nosso estudo, *Responsabilidade Civil por...*, ob. cit., pg. 28 (especialmente nota 27) e pg.154 (especialmente nota 231).

[20] Cfr, neste sentido, Barbosa, Mafalda Miranda, *Protecção de Dados e Direitos...*, ob cit, pg.108. Em texto reportámo-nos tão somente à violação de direitos absolutos, sendo que para o surgimento de responsabilidade civil extracontratual, pode estar em causa também a violação de uma norma legal destinada a proteger interesses alheios (art.º 483.º. n.º1).

[21] Na verdade, como a doutrina tem vindo a sustentar que o Direito Geral de Personalidade deve ser concebido como "objecto da intervenção", cumpre a este propósito ter também em conta os critérios subjacentes e necessários à delimitação da autodeterminação informacional, cfr, Gronau, Kerstin, *Das Persönlichkeitsrecht von Personen der Zeitgeschite und die Medienfreiheit*, Baden-Baden,2002, pg.64 e ss.

[22] Cfr, o nosso estudo, "Tutela da Personalidade e Responsabilidade Civil*", in R.L.J*, Ano 147 (n.º4006), pgs. 10 e ss.

De um modo particular, relativamente à protecção dos dados sensíveis, pensamos que a generalidade das situações de violação de direitos de personalidade perpetradas com o tratamento dos dados pessoais se reportam basicamente ao direito à reserva da intimidade da vida privada.

Regressando agora à delicada questão dos dados sensíveis, e debruçando-nos sobre os dados relativos à saúde, cumpre fazer menção aos testes genéticos, matéria sobre a qual, quer do ponto de vista do direito positivo interno, quer a nível da moderna regulamentação comunitária de dos dados pessoais, não se suscitam quaisquer dificuldades. Na verdade, tanto a disciplina fixada no art.º 177.º, n.º2 do Decreto Lei n.º 72/2008, quanto o regime constante no art.º 9.º n.º1 do regulamento (EU) 2016/679, proíbem ostensivamente o tratamento de dados genéticos.

Com efeito, o n.º3 do art.º 12.º da Lei n.º 12/2005, de 26 de janeiro, veda às seguradoras a utilização de informações genéticas para poderem recusar a celebração de seguros de vida e de saúde, ou procederem ao agravamento do prémio, sendo que uma tal limitação não parece superada em face da actual regulamentação em vigor, porquanto o regulamento 2016/679, relativo ao tratamento de dados pessoais, vem excluir liminarmente a licitude de qualquer operação de tratamento desse tipo de dados. Subjacente a este regime tão restritivo parecem estar então, entre outras razões, o direito das pessoas a não terem conhecimento do seu estado de saúde, com o principal objectivo de não lhe serem causadas perturbações de ordem emocional.

Fundado nesta ordem de considerações, o direito à ignorância acerca do estado de saúde e, por conseguinte, das patologias que os resultados dos testes genéticos são susceptíveis de detectar, acaba por contender de modo significativo com a actividade das seguradoras. Na verdade, o regime consagrado nos arts.º 24.º a 26.º do Decreto Lei n.º 72/2008[23], dedicado ao velhíssimo dever do tomador do seguro ou do segurado declarar ao segurador todas as circunstâncias por eles conhecidas[24], e tidas por relevantes para a avaliação do risco — (a comummente conhecida declaração inicial do risco), não encontra nas disciplinas jurídicas particularmente restritivas atrás invocadas a propósito dos testes genéticos um aliado para garantir a sua efectivação.

Em face de todas estas dificuldades suscitadas, questiona-se até que ponto não se revelaria mais adequado um regime, que não pondo em causa o aludido direito à ignorância acerca do estado de saúde, não contendesse com o exercício das incontornáveis prerrogativas das seguradoras subjacentes ao art.º 24.º do Decreto lei n.º 72/2008.

Perguntar-se-á então até que ponto não seria exigível impor ao proponente do contrato de seguro o dever de informar

[23] Correspondente ao regime outrora fixado no art.º 429.º do Código Comercial.

[24] Cfr, a este propósito, Gomes, Julio, "O Dever de Informação do (candidato a) do tomador do seguro na fase pré — contratual, à luz do Decreto Lei n.º 72/2008 de 16 de abril ", *in Estudos em Homenagem ao Professor Doutor Carlos Ferreira de Almeida*, Vol. II, Coimbra, 2011, pg. 405 ss. O Autor considera que a solução que confina o dever de esclarecimento às circunstâncias conhecidas do segurador é a mais razoável: Não se trata de impor ao tomador do seguro ou ao segurado um ónus de averiguação ou de investigação, convertendo-os no "segurador do segurador", mas apenas de consagrar o dever de declarar com exactidão aquilo que se sabe, o que se conhece (ob.loc.ant.cit., pg.406).

a seguradora que tais testes genéticos foram realizados e os resultados realmente existem, conquanto não tenha acedido ao conhecimento desses dados. Ora, revelando-se exigível a adopção deste tipo de conduta, a não revelação dessas informações às seguradoras, traduzir-se-ia numa atitude culposa do tomador no âmbito do *iter negotti* do contrato de seguro, onde o art.º 24.º da lei do contrato de seguro assume uma importância capital.

Para além disso, a proibição das seguradoras terem acesso aos testes genéticos não deixa de merecer sérios reparos na doutrina, invocando-se, a este propósito, que não faz sentido afirmar limitações tão significativas, uma vez que se está a ignorar a importância assumida pelo dever de sigilo médio.

Ora, assim sendo, o proponente do contrato de seguro, em lugar de transmitir os resultados de tais testes a um qualquer agente das seguradoras, poderia realmente optar por fazê-lo apenas aos médicos das mesmas.

Não podemos, na verdade, ignorar os resultados úteis decorrentes da admissibilidade de um concurso entre os métodos tradicionais de diagnóstico e as mais modernas técnicas genéticas, sobretudo quando estas últimas sejam susceptíveis de detectar com um enorme grau de fidedignidade a probabilidade de superveniência de determinadas patologias ou doenças.

Importa, no entanto, explicitar, sem margem para dúvidas, que tais considerações apenas podem ser afirmadas no plano do Direito a constituir, atentas as profundas limitações impostas pelo direito vigente à solicitação ou utilização pelas seguradoras de informação genética de qualquer tipo. Cumpre ainda sublinhar a propósito dos atrás mencionados dados sensíveis, dados esses que impõem particulares limitações à actividade de recolha e tratamento de dados pessoais, seja pelas segura-

doras, seja por qualquer outra entidade responsável pela realização de tais tarefas, que o regulamento 2016/679, no art.º 9.º n.º1 procedeu a uma enumeração de categorias especiais de dados pessoais, os quais se identificam verdadeiramente com os ditos dados sensíveis.

Poder-se-á questionar se a enumeração constante no art.º 9.º n.º1[25] do regulamento geral de protecção de dados reveste carácter taxativo, ou se ao invés, não devemos ter subjacente uma orientação cada vez mais consolidada na doutrina, de acordo com a qual, não existem "dados pessoais "inofensivos", devendo acentuar-se não a natureza dos dados isoladamente considerados, mas o seu lugar no "contexto de um tratamento"[26] ".

Nesta sede, o legislador comunitário quis deixar claro que as categorias de dados pessoais mencionados no artigo em análise, devem considerar-se, à partida, como dados pessoais especialmente sensíveis, sendo que não podemos ignorar todas as demais limitações ao tratamento de dados pessoais constantes do regulamento 2016/679, cuja observância se revela necessária para garantir a licitude deste tipo de actividade.

[25] No art.º 9.º n.º1 do regulamento 2016/679, no âmbito das categorias especiais de dados pessoais, que podemos fazer coincidir com aqueloutra de dados sensíveis, são incluídos os dados que " relevam a *origem racial* ou étnica, as opiniões políticas, as *convicções religiosas* ou *filosóficas*, ou a *filiação sindical*, bem como o tratamento de *dados genéticos e biométricos*, para identificar uma pessoa de forma inequívoca, dados relativos à saúde, ou dados relativos à *vida sexual* ou *orientação sexual* de uma pessoa.".

[26] Cfr, a este propósito, Alexandre S., *Privacy* ..., ob cit, pgs. 486-487 (o autor confere um particular destaque a uma certa linha de orientação da doutrina germânica para a qual, em última análise, a categoria dogmática dos dados sensíveis deve ser considerada desajustada).

No contexto de tais limitações, cumpre fazer uma especial menção aos princípios relativos ao tratamento de dados pessoais.

Assim sendo, procedendo-se ao tratamento de dados pessoais aparentemente inócuos ou inofensivos, tais como a idade, a residência, o estado civil, a naturalidade, bem como de informações relativas aos ascendentes reportadas igualmente aos elementos acabados de mencionar,..., poderá suceder que o modo ou o contexto no âmbito do qual aquele tratamento tenha lugar, determine uma automática convulação de dados pessoais à priori, inofensivos, em dados pessoais susceptíveis de lhes serem atribuídos o epíteto de sensíveis.

Não podemos ignorar, nesta sede, que a descontextualização[27] das informações divulgadas pode constituir um factor decisivo para determinar a falta de veracidade das mesmas, quando é certo que tais informações isoladamente consideradas correspondiam à realidade factual.

Ora, como resulta, com toda a clareza, da alínea d) do n.º 1 art.º 5.º do regulamento geral de Protecção de Dados, a exactidão dos dados pessoais constitui um pressuposto ou requisito necessário para garantir a licitude do respectivo tratamento.

Uma tal conclusão em torno da tipicidade/atipicidade dos dados pessoais elencados no art.º 9.º , n.º1 do regulamento 2016/679, não decorre senão da circunstância de termos levado a cabo uma interpretação teleológica do regime neste preceito plasmado, tendo em conta, desde logo, a importância desempenhada no âmbito da actividade interpretativa de outros arri-

[27] Cfr, a este propósito, o nosso estudo, *Responsabilidade Civil por Ofensa*..., ob. cit., pg.452 e ss.

mos ou apoios sistemáticos, mormente a disciplina contida no art.º 5.º deste diploma normativo.

III. Os Princípios Reguladores do Tratamento dos dados pessoais

Tendo em conta a delicadeza da matéria regulada, desde logo, pela circunstância de estar em causa um conflito entre a prossecução de valores comunitários fundamentais (segurança, saúde, prossecução de finalidades administrativas relevantes...), por um lado, e a tutela de direitos de personalidade, que não deixa de revestir uma igual relevância pública[28], por outro, o regulamento 2016/679 dedicou o seu art.º 5.º à enunciação de um conjunto de princípios fundamentais a observar em matéria de tratamento de dados pessoais.

Importa, a este propósito, sublinhar que não se trata de uma opção legislativa original, tendo antes o regulamento geral de protecção de dados aproveitado amplamente da experiência normativa nesta sede adquirida ao longo dos tempos, não podendo neste contexto, ignorar-se a relevância assumida no mundo Europeu Ocidental pelo grande marco legislativo consubstanciado no *Datenschutz*, diploma germânico de referência surgido nos anos 70 do século passado.

Sem pretender proceder a uma análise exaustiva do percurso trilhado no âmbito da produção normativa em matéria da protecção de dados, sempre se fará referência à importante

[28] Cfr, a este propósito, o nosso estudo, "Tutela da Personalidade ...",ob. cit., pg.18.

directiva 95/46/CE, bem como aqueloutra relativa à retenção e armazenamento de dados de tráfego em comunicações electrónicas[29], e a nível do Direito Interno, uma menção especial é também devida à lei especialmente destinada a disciplinar esta matéria de protecção de dados pessoais- a lei n.º 67/98, de 26 de outubro[30].

Antes de proceder a uma análise mais cuidada e desenvolvida em torno destes princípios estruturantes, constantes do art.º 5.º do regulamento 2016/679, cumpre levar a cabo uma breve enumeração dos mesmos:

— Princípio da Licitude, Lealdade e Transparência — (art.º 5.º, n.º1 al.) a);

— Princípio da Especialidade — Limitação do tratamento dos dados para as finalidades determinadas, explícitas e legítimas que presidiram à respectiva escolha — (art.º 5.º, n.º1 al.)b);

— Princípio da Proporcionalidade (com os respectivos corolários da necessidade, adequação e proporcionalidade em sentido estrito) – (art.º 5.º, n.º1 al.)c);

— Princípio da Veracidade — (art.º 5.º, n.º1 al.)d);

[29] Cfr, Directiva n.º 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março.

[30] Na verdade, a nossa lei de protecção de dados pessoais- lei n.º67/98 de 26 de outubro, procedeu à transposição para a ordem jurídica Portuguesa da Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Ora, esta directiva versava precisamente sobre a matéria sobre a qual incide agora a disciplina do regulamento 2016/679, ou seja, sobre a protecção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

— Princípio da Integridade e Confidencialidade – (art.º 5 .º, n.º1 al.)e e f);

Não se torna assim difícil concluir que este conjunto de princípios constitui precisamente o pano de fundo no âmbito do qual se hão — de resolver[31] os conflitos de valores e interesses latentes na matéria do tratamento dos dados pessoais.

[31] Importa, de resto, sublinhar que este conjunto de princípios fundamentais, não difere substancialmente daqueloutro elencado pela lei n.º 67/98, no art.º 5.º. Na verdade, também a alínea a) do n.º1 deste preceito legal faz expressa menção ao princípio da licitude de tratamento dos dados, não obstante não constar aqui, à semelhança de quanto ocorre no art.º 5.º, n.º1 al.) a) do regulamento, uma referência ao princípio da transparência, omissão essa também extensível à lealdade. Porém, relativamente a esta última omissão, a mesma deve ser considerada mais aparente do que real, porquanto neste preceito da nossa lei dos dados pessoais impõe-se o respeito pelo Princípio da Boa-Fé, o qual em matéria de exigências de lealdade, correcção e honestidade da conduta dos respectivos destinatários manifesta uma maior riqueza axiológica que a simples menção à lealdade constante do Regulamento Comunitário. Para além disso, o por nós designado princípio da especialidade consubstanciado na exigibilidade da recolha e tratamento dos dados pessoais ser basicamente orientado pela prossecução de determinadas finalidades explícitas e legítimas, trata-se de uma regra comum contida no art.º 5.º, n.º1 al.) b) dos dois diplomas normativos em conflito. De igual modo, o conteúdo da al.) c do Regulamento Comunitário e da nossa lei de protecção de dados pessoais reporta-se basicamente à enunciação do princípio da proporcionalidade. O mesmo se diga quanto ao princípio da veracidade contigo na al.) d) do art.º 5.º dos dois diplomas. Relativamente ao princípio da integridade e confidencialidade, cujas ideias força encontram expressa menção na al.) f) do art.º 5.º, n.º1 do Regulamento Geral de Protecção de Dados, cumpre referir que uma tal dimensão não apareceu referida expressamente na al.) e) do n.º1 do art.º 5.º da lei n.º 67/98, onde apenas consta uma referência às exigências temporárias de conservação dos dados (tendo em conta as finalidades a que os mesmos se destinem), com uma formulação mais restrita, mas bastante próxima da al.) e) do art.º 5.º, n.º1 do Regulamento 2016/679. No fundo, apenas não encontramos na lei n.º 67/98, um

Não admira que o primeiro dos princípios enunciados na al.) a) do art.º 5.º, n.º1 do Regulamento 2016/679 seja precisamente o da licitude do tratamento dos dados. Coenvolvendo a actividade de recolha e tratamento de dados pessoais a realização de diligências susceptíveis de contenderem com os direitos de personalidade dos respectivos titulares, não constitui motivo de estupefação a exigibilidade feita neste preceito à licitude do tratamento como condição substancial e decisiva para o desenvolvimento de qualquer procedimento nesta área.

A densificação do conteúdo deste princípio fundamental implica uma necessária remissão para o art.º 6.º do Regulamento Geral de Protecção de Dados, onde o consentimento do titular assume um particular destaque, apesar de no diploma comunitário que actualmente regula a matéria o consentimento surja colocado no mesmo plano de outras razões justificativas para se proceder ao tratamento de dados pessoais, razões essas enunciadas nas alíneas b) a f) do número um deste mesmo preceito.

Uma análise comparativa com o modo como esta questão era regulada na lei n.º 67/98, permite numa primeira análise

artigo com uma formulação idêntica à al.) f) do n.º1 do art.º 5.º, do Regulamento Geral de Dados Pessoais. Cumpre a este propósito sublinhar, que a lei nacional de protecção de dados limitou-se a transpor o regime constante dos art.os 5.º e 6.º da directiva 95/46, sendo que a enunciação dos princípios é efectuada, neste último artigo, enquanto no art.º 5.º se procede apenas à indicação de que é no Cap. II da Directiva que se encontram reguladas as condições de licitude de tratamento dos dados. No fundo, não podemos deixar de evidenciar que desde o primeiro diploma normativo comunitário dedicado à protecção de dados pessoais se registou a preocupação pelo mesmo tipo de questões, conquanto se tenha registado ao longo do tempo uma clara tendência para o alargamento do âmbito normativo dos diplomas subsequentes, destacando aqui, de modo particular, o regulamento n.º2016/679.

concluir que o consentimento deixou de ser considerado como a principal razão justificativa[32] de um lícito tratamento dos dados pessoais.

Porém, não podemos deixar de referir o papel preponderante do consentimento, reservando-lhe o legislador comunitário um lugar de destaque no art.º 7.º, ao definir as condições aplicáveis ao consentimento, revelando-se, a este propósito, as exigências de Lealdade e Transparência mais evidentes, quando a recolha e tratamento dos dados sejam nele baseados.

Na verdade, o tratamento dos dados pessoais fundado no consentimento implica, por regra, uma estrutura dialógica muito mais evidente que quando a mesma actividade encontra o seu fundamento na "execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados" al.) b) do n.º1 do art.º 6.º do Regulamento n.º 2016/679. Apesar dos dados estarem a ser recolhidos no âmbito de uma relação contratual pré-contratual, que se funda, por conseguinte numa estrutura dialógica, não está, no entanto, em causa nesta hipótese única e simplesmente um diálogo dirigido à recolha de dados, razão pela qual uma tal questão pode afigurar-se para o titular dos dados como um problema secundário ou marginal.

Razão pela qual, o cumprimento das exigências de lealdade e transparência no âmbito das hipóteses previstas na al.) b) do n.º1 do art.º 6.º do Regulamento Geral de Protecção de Dados pode implicar um reforço[33] por parte da entidade responsável

[32] Cfr, a este propósito, Barbosa, Mafalda Miranda, Protecção de Dados..., ob. cit., pg.91.

[33] No fundo, a entidade responsável pelo tratamento dos dados deve chamar a atenção da contraparte, de modo claro e incisivo, para a circunstância

pela recolha dos dados dos deveres de informar e esclarecer de modo claro, explícito e perceptível o objectivo, o sentido e os fins da actividade que se encontram a desenvolver, representando estes deveres os corolários da Lealdade e Transparência.

Na verdade, projectam-se neste universo específico da protecção de dados ideias radicadas na categoria dogmática da ordem pública de protecção[34], cujo objectivo nuclear se traduz na defesa de quem é socialmente fraco e vulnerável. Por regra, quando se convoca uma tal categoria estamos a pensar nas relações de consumo, tendo-se como principal preocupação proteger o consumidor, que é precisamente a parte mais fraca.

Neste universo de protecção de dados, não estamos, de modo algum, a sugerir uma tutela circunscrita ao consumidor, sendo que a ratio da ordem pública de protecção se afirma igualmente, de modo indelével, em relação a outros destinatários da entidade responsável pelo tratamento dos dados, pois não obstante poderem estar em causa pessoas singulares dotadas de um particular poder económico e social, no âmbito deste contexto específico, revelam-se naturalmente menos bem preparadas quando confrontadas com o profissional que lhe solicita as informações.

Todas estas considerações permitem-nos concluir que a análise dos princípios fundamentais em matéria de tratamento dos dados pessoais não pode ser levada a cabo de um modo atomístico, baseada numa interpretação meramente literal e sistemática do art.º 5.º do Regulamento 2016/679.

do contrato a concluir, implicar na sua execução o acesso e tratamento dos respectivos dados pessoais.

[34] Cfr, a este propósito, Silva, J. Calvão, *Sinal e Contrato Promessa,* 14.ª Ed, Coimbra, 2017,pg.64.

Ora, continuando esta leitura articulada das várias regras enunciadas neste preceito, torna-se fundamental destacar a profunda interligação entre a licitude do tratamento dos dados, e as exigências da proporcionalidade[35], no âmbito das quais decidimos integrar a disciplina normativa contida na alínea b) do n.º 1 do art.º 5.º do regulamento comunitário em análise, disciplina essa centrada na adstrição da actividade de recolha e tratamento a determinadas finalidades legítimas e explicitamente transmitidas as titulares dos dados.

Ao fazer-se depender a licitude da recolha e tratamento dos dados pessoais das finalidades que foram indicadas ao titular dos mesmos, acabam por se definir balizas que constituem importantes limites ao desenvolvimento da actividade dos responsáveis pelo tratamento dos dados pessoais. No rol de tais limitações, cumpre mencionar, de modo particular, a proibição de utilização de cláusulas vagas e genéricas de consentimento para utilização de dados, bem como a proscrição dos desvios às finalidades a que se encontra adstrito o consentimento, por parte dos responsáveis pelo tratamento, situações essas particularmente potenciadas pelos tratamentos multifuncionais.

Ao proscrever-se a legitimidade da recolha de dados pessoais baseada na utilização de cláusulas vagas ou genéricas, tais como o consentimento manifestado para permitir *alcançar as finalidades específicas previstas na lei para um determinado sector de actividade*, pretende-se, no fundo, que os titulares dos dados possam prever ou contar com toda a segurança que os dados transmitidos venham a ser utilizados para as finalidades específicas ou explícitas previamente anunciadas pela entidade responsável pelo respectivo tratamento.

[35] A propósito desta profunda conexão entre a licitude do tratamento dos dados e o conhecimento dos fins a que se destina a recolha, cfr, Pinheiro, Alexandre Sousa, *Privacy e Protecção*..., ob cit, pg.806

Em causa está a exigência de manifestação pelo titular dos dados de um consentimento específico, razão pela qual a indicação das finalidades determinadas ou específicas pela entidade responsável pelo tratamento dos dados deve ser efectivada de modo particularmente explícito e densificado. Apenas concebendo desta forma a vertente do princípio da proporcionalidade consubstanciada na necessidade[36] do esclarecimento dos fins da recolha de dados se torna possível detectar a existência de situações de desvio de utilização dos mesmos (zweckänderung), por parte de quem procede ao respectivo tratamento.

Tais exigências aparecem, de resto, claramente formuladas na al.) b) do art.º 5.º do Regulamento n.º 2016/679, ao referir que os dados pessoais são: " Recolhidos para finalidades determinadas, explícitas e legítimas...", sancionando-se, igualmente de modo explícito, o tratamento dos dados de forma incompatível com a anunciada ao respectivo titular: "... não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades...".

Regressando à fórmula atrás mencionada – *"alcançar as finalidades específicas previstas na lei para um determinado*

[36] Acerca da necessidade enquanto dimensão fundamental do princípio da proporcionalidade, cfr, o nosso estudo, *Responsabilidade Civil por Ofensa*..., ob. cit., pgs.443-444, Adrian, Reinhold Heidorn Thomas, *Der Bankbetrieb (Lehrbuch und aufgaben)*, 15.ª Ed., Wiesbaden, 2000, pg.106-107 (o autor reporta-se ao requisito da necessidade no âmbito da actividade bancária, a propósito das importantes tarefas aí desenvolvidas de recolha, divulgação e transmissão de informações.).

sector de actividade", poder-se-á questionar verdadeiramente se afinal não se regista um ajustamento da mesma às exigências normativas indicadas na al.) b) do art.º 5.º do Regulamento Geral de Protecção de Dados, uma vez que apesar de tudo, se verifica aí uma formulação dos fins: alcançar as finalidades específicas previstas na lei para determinado sector de actividade.

Na verdade, a fórmula referida procede a uma dupla limitação – quanto às finalidades indicadas e quanto ao domínio de actividade a que as mesmas se reportam.

Para além disso, faz-se uma expressa remissão para a lei onde tais limitações se encontram consignadas, podendo, a este propósito, convocar-se com particular acuidade uma regra jurídica fundamental, que não condescende com a ignorância dos ditames legais: *a ignorância ou má interpretação da lei não escusa*[37]. Todavia, uma resposta adequada à questão atrás colocada, implica antes demais que se leve em linha de conta o quadro de finalidades do sector de actividade a que se reporta a recolha de dados.

Ora, pode bem suceder que ao sector de actividades em questão se encontrem associadas uma multiplicidade de funções, situação essa susceptível de ocasionar tratamentos multifuncionais. Com efeito, se entendermos que, de modo explícito e claro[38], se transmitiram aos titulares dos dados todas as finalidades específicas de um determinado sector de actividade,

[37] Uma tal máxima resulta expressis verbis do art.º 6.º do Código Civil.

[38] Ao referirmos estes pressupostos ou requisitos para a transmissão das informações pela entidade responsável pelo tratamento de dados, estamos a reportar-nos as exigências do princípio da Lealdade (melhor dizendo, da Boa-Fé) e da Transparência constantes da al.) a) do n.º1 do art.º 5.º do Regulamento n.º 2016/679.

então poder-se-á concluir que o consentimento daqueles não foi vago ou genérico.

Porém, não nos parece correcto invocar que o perigo da prestação de um consentimento vago e genérico fica afastado, pela circunstância do responsável pelo tratamento dos dados ter feito uma referência às finalidades legais associadas ao exercício de um determinado sector de actividade.

Não podemos ignorar que subjacente à necessidade de alcançar um consentimento informado e esclarecido por parte de quem vai emitir uma declaração (no domínio em análise — o titular dos dados), anda associado um objectivo fundamental traduzido na tutela de quem é considerado como mais desprotegido ou vulnerável[39]. No fundo, não nos parece excessivo convocar nesta sede as exigências regulativas da Ordem Pública da Protecção, e assim sendo a regra fundamental do nosso código civil expressa no seu art.º 6.º deve ser contemporizada com exigências fundamentais de informação a cargo de quem procede ao tratamento dos dados, de modo a suprimir o défice

[39] Não podemos esquecer, como resulta expressis verbis do considerando 1 do Regulamento Geral de Protecção de Dados que: "A protecção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental". Ainda a este propósito, cumpre sublinhar que o regulamento n.º 2016/679 "não abrange o tratamento de dados pessoais relativos a pessoas colectivas, em especial a empresas estabelecidas enquanto pessoas colectivas..." (considerando n.º14 desse regulamento). Ora, esta exclusão da protecção concedida pelo regulamento às pessoas colectivas, aponta claramente no sentido de o legislador comunitário ter considerado dispensável concedê-la a um tal tipo de pessoas, uma vez que relativamente a estas não se pode, à priori, afirmar a respectiva vulnerabilidade. Importa nesta sede não perder de vista a proclamação, de acordo com a qual "o tratamento dos dados pessoais deverá ser concedido para servir as pessoas".

-informativo que, em princípio, se regista na esfera jurídica do titular dos dados.

Desta feita, impõe-se um encargo sobre o responsável do tratamento dos dados, de modo a garantir um efectivo conhecimento da realidade jurídica pelos respectivos titulares, pois apenas deste modo o consentimento por eles prestado se pode considerar lícito.

Trata-se, de resto, de um cenário idêntico ao verificado em vários outros domínios da sociedade de consumo, entre os quais se destaca a necessidade do consentimento informado do paciente para intervenções cirúrgicas, bem como a protecção dispensada a quem nos mais variados sectores assuma a posição de aderente no âmbito da contratação baseada no modelo das cláusulas contratuais gerais[40].

Em face deste arrozado de considerações em torno da proibição do consentimento do titular dos dados se basear em cláusulas vagas e genéricas, ficou bem clara a profunda conexão existente entre este impedimento e aqueloutro respeitante à inadmissibilidade de tratamentos multifuncionais de dados.

Para além disso, resultou também bem claro que a conclusão acerca da natureza vaga e genérica do consentimento se encontra particularmente dependente do leque mais ou menos extenso de finalidades ligadas aos vários sectores de actividade a que se reportam as operações de tratamento de dados. Desta feita, o consentimento que pode ser qualificado como vago e genérico para um determinado sector de actividade, pode não o ser quanto a um outro domínio distinto.

[40] Em relação ao universo dos seguros, cumpre mencionar a proliferação na respectiva legislação de deveres de informação, assistindo-se, na senda do regime instituído pelo Decreto Lei n.º 446/85, a uma distinção cada vez mais frequente, entre deveres de informação e deveres de esclarecimento (art.º 5.º e art.º 6.º deste diploma legal). Exemplo paradigmático da concretização de uma tal distinção encontra-se plasmado na disciplina contida no art.º 18.º (dever de informação) e no art.º 22.º (dever de esclarecimento) do Decreto Lei n.º 72/2008.

Cumpre, porém, sublinhar que esta vertente do princípio da proporcionalidade consubstanciada na adstrição da recolha de dados a uma finalidade específica, não se afirma em termos absolutos, podendo admitir-se a utilização daqueles para outros fins, quando em causa estiverem ponderosas razões de interesse público.

Como expressis verbis decorre do art.º 5.º, n.º1, al.) b) do Regulamento Geral de Protecção de Dados "o tratamento posterior para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o art.º 89.º, n.º1 ("limitação das finalidades")".

Apesar de não ser incompatível com as finalidades iniciais, para as quais se encontrava adstrito o tratamento dos dados, a respectiva utilização para o desenvolvimento de actividades de investigação científica ou histórica, bem como para operações de índole estatística, certo é que o art.º 89.º, onde se regula precisamente esta matéria, estabelece particulares restrições quanto à admissibilidade da utilização dos dados para finalidades diversas.

Não obstante, o desvio do tratamento dos dados face às finalidades iniciais seja determinado para acautelar a prossecução de relevantes interesses públicos, a verdade é que uma tal derrogação à regra estabelecida no regulamento n.º2016/679 encontra-se dependente da adopção de garantias adequadas para os direitos e liberdades do titular dos dados, a saber: o respeito pela minimização dos dados. O legislador comunitário no art.º 89.º, n.º1 indica, de resto, medidas tidas por idóneas para acau-

telar o desiderato mencionado, referindo-se nomeadamente à possibilidade de recorrer à pseudonimização, ou ainda à possibilidade de realizar novas operações de tratamentos de dados que não permitam a identificação dos respectivos titulares.

Bem vistas as coisas, encontra-se neste preceito consagrado o princípio da subsidiariedade, porquanto a utilização plena e integral dos dados fornecidos para um tratamento inicial apenas ocorrerá se não for possível alcançar através daqueles dois tipos de operações mencionadas as finalidades de investigação científica ou histórica, ou os objectivos estatísticos desejados.

Para além do corolário do princípio da proporcionalidade, consubstanciado na necessidade da actividade de tratamento de dados respeitar as finalidades com base nas quais foi obtido o consentimento dos seus titulares, constante da al.) b) do n.º1 do art.º5.º do regulamento n.º2016/679, na al.) c) do mesmo diploma encontram-se previstas as demais vertentes implicadas neste princípio jurídico fundamental: a *adequação* e a *pertinência*, referindo-se o legislador comunitário também à *necessidade*. De acordo com o nosso entendimento, esta referência à necessidade revela-se redundante uma vez que um tal corolário do princípio reitor da proporcionalidade já consta do preceito anterior.

Assim sendo, podemos afirmar que o princípio da proporcionalidade em matéria de tratamento dos dados pessoais se encontra espraiado por dois preceitos desta regra do art.º 5.º do regulamento 2016/679: as alíneas b) e c) do seu número 1.

Tendo em conta as ditas exigências da necessidade, adequação e pertinência, ideia esta que podemos reconduzir ao corolário de proporcionalidade em sentido estrito[41], o legislador comunitário sugestivamente consubstanciou estas vertentes regulativas na regra da minimização dos dados.

[41] A propósito da proporcionalidade em sentido estrito, basicamente consubstanciada na ideia de pertinência, cfr, o nosso estudo, *Responsabilidade Civil por Ofensa*..., ob. cit., pg.447. Porém, tal como tivemos oportunidade de aí referir... "não devemos levar a cabo uma análise seccionada do princípio da Proporcionalidade, de acordo com o qual os juízos de adequação, necessidade e proporcionalidade em sentido estrito seriam concebidos como categorias autónomas e estanques. Com efeito, subjacente à apreciação da adequação e da necessidade, encontra-se já uma certa ponderação em torno da relevância dos bens jurídicos conflituantes".

Cumpre agora fazer menção a um outro princípio fundamental em matéria de tratamento de dados: o princípio da veracidade, princípio esse constante da al.) d) do art.º 5.º, n.º1 do regulamento 2016/679, concretizado nas notas da *exactidão* e da *actualidade*.

Torna-se, com efeito, importante a referência explícita à actualidade a propósito do princípio da veracidade, uma vez que a falta de actualização das informações pode determinar uma deturpação da verdade, tornando inexactos os dados.

Igualmente significativos se manifestam os poderes conferidos aos titulares dos dados de exigir que os mesmos sejam apagados e rectificados, poderes esses cuja efectivação deve ser garantida com prontidão: "sejam apagados ou retificados sem demora"[42] [43] [44].

[42] Esta matéria encontra-se actualmente regulada nos art.os 16.º e 17.º do Regulamento 2016/679, surgindo o direito ao apagamento dos dados previsto neste último preceito, fundando-se, por seu turno, um tal direito num alegado direito ao esquecimento.

[43] Cfr, a este propósito, Pinheiro, Alexandre S., Privacy e ..., ob. cit., pgs.653-654 (o autor reportava-se a estas faculdades integradas no âmbito de um direito mais amplo dos titulares dos dados – o direito à oposição a propósito da disciplina fixada na Directiva n.º 95/46).

[44] A propósito do direito ao apagamento dos dados previsto no art.º 17.º do Regulamento 2016/679, Morais de Carvalho equaciona o problema de saber

Com efeito, a exigibilidade de celeridade nos procedimentos de correcção dos dados pessoais constitui uma condição sine quo non para uma eficaz reposição da verdade pessoal dos titulares dos dados, uma vez que a perpetuação das inexactidões relativas aos titulares dos dados pode ser de molde a causar-lhes prejuízos significativos.

Desta feita, a imposição da exigência de brevidade temporal nos procedimentos de correcção dos dados constitui uma garantia de segurança, contribuindo para conferir credibilidade aos sistemas de tratamento daqueles.

Importa agora fazer menção a um outro princípio fundamental, para cuja caracterização se revelam também decisivas considerações de segurança e fiabilidade – o princípio da integridade dos dados — , que surge apenas explicitado na al.) f) do n.º 1 do art.º 5.º do regulamento 2016/679, a propósito da forma ou do modo de proceder ao tratamento dos dados, mas que em rigor surge também disciplinado na al.) e) a propósito da problemática da respectiva conservação.

Desta feita, pensamos que o princípio da integridade do tratamento dos dados se encontra disciplinado em ambas as disposições mencionadas do art.º 5.º n.º1 do Regulamento Geral

quais as consequências decorrentes do contraente que forneceu os dados retirar o seu consentimento. O autor problematiza "se o apagamento dos dados tem consequências no que respeite ao período anterior a esse apagamento, nomeadamente se o titular dos dados tem de compensar a contraparte". Cfr, Carvalho, Jorge Morais, *Manual de Direito do Consumo*, 4.ª Ed., 2017, pg. 40. Relativamente a esta questão, pensamos que a resposta deve ser negativa, uma vez que o titular dos dados ao exigir o apagamento não está a adoptar um comportamento ilícito. Uma breve análise dos motivos enunciados nas várias alíneas do número um do art.º 17.º, permite-nos, na verdade, concluir que o direito ao apagamento dos dados tem na base um comportamento lícito do respectivo titular.

de Protecção dos Dados – as alíneas e) e f), sendo que na alínea e), a questão é regulada a propósito da conservação dos dados, enquanto na alínea f) o problema é disciplinado sob a óptica específica do tratamento dos dados pessoais.

IV. O regulamento dos dados pessoais e os seguros de saúde

O contrato de seguro como contrato de Uberrima Fides: A necessidade de as seguradoras acederem à informação

Qualquer abordagem em torno do contrato de seguro, conquanto muito breve e superficial, permite identificar como nota caracterizadora desta modalidade contratual, a sua submissão às exigências regulativas do princípio da Boa-fé, consubstanciada na ideia que, quer as seguradoras, quer os proponentes do contrato de seguro têm o dever de orientar as respectivas condutas, seja na fase pré-contratual, seja no período do cumprimento do acordo, com os ditames de um correcto proceder[45]. Uma tal nota caracterizadora surge na doutrina,

[45] Com toda a propriedade, podemos convocar nesta sede as exigências inerentes ao *Iura Praecepta* romano Honeste Vivere, que, no essencial correspondem às directrizes fundamentais que se associam à Boa-Fé enquanto regra de conduta, ou seja, enquanto Princípio que impõe aos contraentes um comportamento honesto, correcto e leal.

bem como na jurisprudência explicitada pela identificação do contrato de seguro como um contrato de Uberrima Fides[46].

Uma tal qualificação Dogmático-Jurisprudencial exprime, de um modo claro, a realidade vivenciada no âmbito da formação e da execução dos contratos de seguro, onde a transmissão de informações acerca do objecto (a que respeita o risco a segurar) se revela absolutamente essencial. Ora, sob este aspecto, cumpre sublinhar que o proponente do seguro é realmente quem dispõe de um conhecimento mais aprofundado acerca dos dados ou elementos relevantes do risco, cuja cobertura pretende ver garantida com a celebração do contrato de seguro.

Configurando-se a seguradora como a parte económica-técnica e socialmente mais forte na relação contratual, a verdade é que, paradoxalmente, do ponto de vista das informações tidas por relevantes para a avaliação do risco, a mesma se encontra particularmente dependente do acervo informativo que lhe seja transmitido pelo proponente do seguro[47].

Razão pela qual no âmbito do direito dos seguros, classicamente os deveres de informação recaiam sobre os proponentes, sendo exemplo paradigmático de uma tal realidade o comummente designado dever de declaração inicial do risco, regulado no velho código de Veiga Beirão no art.º 429.º.

Apesar das múltiplas possibilidades abertas às seguradoras pelas modernas técnicas estatísticas e informáticas em matéria de conhecimento dos riscos a segurar[48], certo é que o aludido dever de declaração inicial do risco ainda hoje se mantém disciplinado nos art.os 24.º a 26.º do Decreto Lei n.º 72/2008, com uma manifesta actualidade.

Porém, a evolução registada no direito dos seguros em virtude das solicitações e exigências reivindicadas por um tráfico jurídico de massas, bem característico da moderna sociedade de consumo, determinou a imposição de deveres de informação a cargo, desta feita, das seguradoras. Uma leitura dos art.os 18.º e seguintes do Decreto Lei n.º72/2008- confronta-nos com uma vasta panóplia de exigências informativas, ditadas pelo objectivo de corrigir o desnivelamento técnico-social entre as seguradoras, enquanto parte economicamente mais forte e os tomadores de seguros e segurados, comummente designados por parte mais fraca.

Mais ainda: assiste-se a uma distinção legislativa entre os deveres de informação (art.º 18.º a 21.º) e os deveres de esclarecimento (art. .º22.º), distinção essa particularmente difícil, tornando-se tarefa bem complexa a de afirmar quando é que acaba o dever de informação e começa o dever de esclarecimento[49].

[46] Cfr, a este propósito, as referências bibliográficas constantes na nota 1 deste trabalho.

[47] Cfr, Rego, Margarida Lima, *Contrato de Seguro*..., ob. cit., pg.103 e ss.

[48] Cfr, neste sentido, Gomes, Júlio, O Dever de Informação do (Candidato) ..., ob. cit., pg.394.

[49] Uma tal distinção assume no âmbito da lei do Contrato de Seguro uma particular relevância prática, uma vez que o seu art.º 23.º, prevê para as hipóteses de violação dos deveres de informação a resolução do Contrato de Seguro, sendo que uma tal sanção não surge associada à violação dos deveres de esclarecimento. Na verdade, quando estiver em causa a violação de esclarecimento, o tomador do seguro apenas terá direito a uma indemnização. Porém, quando a celebração do Contrato de Seguro obedeça ao modelo das cláusulas contratuais gerais, as dificuldades distintivas mencionadas acabam por esbater-se em face do disposto no n.º 2 do art.º 11.º do Decreto Lei n.º 446/85.

Como critério tendencial para a distinção, poder-se-á destacar a exigência no âmbito dos deveres de esclarecimento de uma preocupação por parte de quem informa em acautelar e valorizar os interesses e a posição da contraparte[50].

Uma tal distinção legislativa suscita algumas perplexidades, uma vez que a esta *summa divisio* com contornos nebulosos, se associam consequências jurídicas diversas, pois como resulta do disposto no art.º 23.º da Lei dos Seguros, quando estiver em causa a violação dos deveres de informação poderá haver lugar à resolução do contrato, para além da responsabilidade civil, instituto este que é o único susceptível de ser convocado a propósito dos deveres de esclarecimento.

O legislador dos seguros, particularmente movido pelas mais recentes e louváveis preocupações consumeristas acabou por, em face da prolixidade informativa que é exigível às seguradoras, fomentar nesta sede um *ambiente de opacidade*, ambiente esse que acaba por desencorajar os proponentes consumidores em aceder às informações que lhe são dirigidas[51].

Em rigor, os objectivos de proteger a parte contratualmente mais fraca, acabam por não ser alcançados através desta cascata ou espiral de deveres, onde se assiste inclusivamente à emergência de deveres de informação de segundo grau[52], cuja

[50] Cfr, a este propósito, Monteiro, J. Sinde, *Responsabilidade por Conselhos, Recomendações*, 1989, pg. 359 (especialmente nota 65).

[51] Cfr, a este propósito, Poças, Luis, *O dever de Declaração*..., ob. cit., pg. 201.

[52] Neste contexto, importa referir como exemplos paradigmáticos os art.os 27.º n.º2 do Decreto Lei n.º 291/2007 e art.º 24.º n.º4 da Lei do Contrato de Seguro. A propósito das múltiplas dificuldades suscitadas pelo dever de informação de segundo grau consagrado no art.º 24.º n.º4 do regime comum do Contrato de Seguro, cfr, o nosso estudo, *Uma outra Abordagem em torno das Declarações Inexactas e Reticentes no âmbito do Contrato de Seguro*. "Os art.os 24.º a 26.º do Decreto Lei n.º 72/2008", de 16 de abril, *in Estudos em Homenagem ao Prof. Doutor Jorge de Figueiredo Dias*, Vol. IV, Coimbra, 2010, pg. 620-622.

efectividade prática suscita dificuldades de monta. A prática da actividade seguradora acaba efectivamente por demonstrar que afinal os pedagógicos e inovadores propósitos legislativos acabam por ela e por nela ser infirmados.

Esboçada em termos muito vagos e genéricos a evolução registada no âmbito do contrato de seguro a propósito dos circuitos informativos de que este necessariamente se alimenta, cumpre debruçarmo-nos agora sobre os problemas específicos suscitados pela aplicabilidade do regime constante no Regulamento da Protecção de Dados Pessoais (Regulamento 2016/679). Dito por outras palavras; é este o momento adequado para reflectir sobre as principais dificuldades ou obstáculos suscitados pelo regulamento de protecção de dados à actividade das seguradoras para acederem à informação tida por indispensável para a avaliação do risco.

Formulada a questão nestes termos, torna-se fácil concluir que afinal o polo relevante em matéria de fluxos ou circuitos informativos a propósito do regime de protecção de dados pessoais é aquele respeitante à declaração inicial do risco, ou seja, o atinente aos dados ou informações que cabe ao proponente do seguro transmitir à seguradora.

Importa ainda especificar um pouco mais o campo da nossa análise, o qual tem precisamente em vista um sector particular da actividade seguradora, onde a obtenção de dados pessoais do proponente do seguro assume uma particular acuidade: o universo dos seguros de saúde.

A assunção, por via contratual, do risco pelas seguradoras encontra-se dependente da obtenção de informações qualificadas pela nossa jurisprudência constitucional[53] como dados sensíveis, orientação essa que podendo revelar-se discutível, não suscitou, porém, dificuldades ao legislador comunitário, pois no art.º 9.º n.º1 do regulamento n.º2016/679 os dados relativos à saúde foram qualificados expressis verbis como uma categoria especial de dados pessoais[54].

Com efeito, a propósito do tratamento das categorias de dados pessoais qualificadas de especiais, o regulamento comunitário prescreve a respectiva proibição como regra geral (art.º 9.º n.º1). Apenas se revela possível proceder ao tratamento dos dados pessoais de natureza especial "se o titular dos dados tiver dado o seu consentimento explícito "...para uma ou mais finalidades específicas..." (art.º 9.º, n.º2, al.) a) do regulamento n.º2016/679).

Em face desta disposição, resulta claro que as seguradoras apenas podem proceder ao tratamento de dados pessoais sensíveis quando obtiverem o consentimento dos respectivos titulares e apenas se lhe tiverem sido indicadas de modo detalhado as finalidades específicas que presidiram à respectiva recolha.

De resto, neste contexto tem sido advogado um entendimento restritivo acerca do consentimento enquanto fundamento jurídico válido para o tratamento de dados pessoais,

[53] Cfr, a este propósito, o já anteriormente citado Acórdão do Tribunal Constitucional n.º355/97.

[54] Na verdade, o art.º 9.º do Regulamento de dados pessoais tem como epígrafe "Tratamento de categorias especiais de dados pessoais", e no elenco desses dados, o legislador comunitário indica expressamente "os dados relativos" à saúde.

considerando-se livre aquele consentimento manifestado "para diferentes operações de tratamento de dados pessoais..."[55], quando o mesmo for dado separadamente em relação a cada uma das respectivas operações. Seguindo-se um tal entendimento, então não basta que o titular dos dados pessoais seja parte de um contrato de seguro para o qual tenha manifestado o seu consentimento de forma livre e esclarecida, exigindo-se algo mais para o tratamento de certos dados necessários à execução da relação contratual, e esse quid traduzir-se-á numa explicita manifestação de vontade relativa a uma tal operação específica de recolha de dados.

Apenas quando o tratamento dos dados se revele necessário para o "cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular ou titular dos dados em matéria de legislação laboral, de segurança social e de protecção social..."[56] se revelará possível efectuar a recolha de tais elementos sem o seu consentimento explícito.

Em abono deste entendimento restritivo poderá invocar-se o art.º 6.º, n.º1, al.) b) do regulamento de protecção de dados pessoais ao admitir a "licitude do tratamento"[57] quando uma tal actividade de captação e conservação de dados se revele necessária para a execução do contrato. Uma tal posição, numa primeira aproximação da matéria, considerar-se-á ainda reforçada pelo confronto levado a cabo com o art.º 9.º, n.º1, do

[55] Considerando art.º 43.º do Regulamento n.º2016/679.

[56] Cfr, art.º 9.º, n.º2, al.) b) do Regulamento n.º2016/679.

[57] "Licitude de tratamento" é precisamente a epígrafe do art.º 6.º, onde no seu número 1, al.) b) se admite a recolha de dados para "a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados".

regulamento, onde expressis verbis se encontra vertida a regra da proibição do tratamento de dados pessoais, tidos por especiais, como é o caso dos dados de saúde, e assim sendo, mesmo quando a recolha de tais elementos se traduza como necessária para a execução, sem o consentimento expresso do titular dos dados, não será permitido o respectivo tratamento.

Importa, porém, sublinhar que este entendimento restritivo quanto às condições de admissibilidade do tratamento de dados pessoais sensíveis, se funda numa leitura demasiadamente limitativa do considerando n.º43 do Regulamento n.º2016/679. Com efeito, poder-se-á legitimamente admitir que o consentimento prestado pelo proponente dos seguros para a celebração de um contrato de seguro de saúde, que representa, em si mesma, uma situação específica, constitua fundamento jurídico suficiente para o tratamento dos dados pessoais do proponente em relação às questões específicas atinentes ao(s) risco(s) conexionado(s) com esse universo particular.

Não podemos, na verdade, ignorar que a exigibilidade constante do considerando n.º43 do Regulamento n.º2016/679, de manifestação pelo titular dos dados de um consentimento específico e seccionado para várias operações tem como pressuposto a existência de "um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública[58]".

Bem vistas as coisas, neste particular contexto dos contratos de seguro de saúde, não se regista entre o responsável pelo tratamento de dados e o respectivo titular o manifesto desequilíbrio a que se reporta o considerando em análise, para além da entidade responsável não ser uma autoridade pública.

Como já atrás tivemos ocasião de sublinhar quanto ao acervo informativo considerado relevante para as seguradoras avaliarem o risco a segurar, estas não se encontram numa posição de supremacia susceptível de pôr em causa um consentimento livre por parte do titular dos dados. Antes pelo contrário, neste contexto, a entidade responsável pelo tratamento encontra-se numa posição deficitária, dependendo amplamente das informações que lhe venham a ser transmitidas pelos titulares dos dados, para, desta forma, o consentimento por si prestado no âmbito do contrato de seguro a celebrar possa ser considerado como esclarecido.

Não nos parece assim inadmissível que quando o tomador do seguro ou o segurado concluam um contrato de seguro de saúde, se considere manifestado de forma livre e esclarecida o seu consentimento quanto aos dados relevantes para a boa execução do evento contratual, podendo assim tais dados ser tratados e conservados pelas seguradoras. Desde logo, porque a entidade responsável pelo tratamento dos dados se encontra particularmente condicionada pela observância de um conjunto de exigências regulativas constantes no art.º 5.º do Regulamento n.º2016/679, que, na verdade, oferecem garantias ao tomador do seguro ou ao segurado para não temerem uma invasão inadmissível das suas esferas jurídico-pessoais.

Nem se diga, de resto, que a ausência de um consentimento separado, escalpelizado ou particular, detalhado para a recolha de dados a propósito de cada operação particular realizada no âmbito da execução do contrato é susceptível de pôr em causa o cumprimento do princípio de adstrição da utilização dos dados para as finalidades que presidiram à respectiva recolha.

[58] Cfr, considerando n.º43 do Regulamento n.º2016/679.

Com efeito, toda a vasta panóplia de informações (art.º 18.º e ss do Decreto Lei 72/2008), que impende sobre a seguradora transmitir na fase de formação do contrato, permite, com toda a certeza, a definição de um quadro suficientemente preciso de exigências e de regras, no âmbito das quais a execução da relação contratual terá lugar.

Razão pela qual, atento todo o quadro actual vigente de "Prolixidade informativa", não é de recear o perigo de haver surpresas por parte dos titulares dos dados quanto à necessidade de proceder ao tratamento de categorias diversificadas dos mesmos ou à respectiva conservação[59].

Não aceitar este posicionamento, e sufragar, ao invés, um entendimento mais restritivo que exige um tratamento dos dados profundamente dominado pelas regras do *detalhe, do consentimento sectorial ou segmentado,* e de uma *especialização qualificada,* implica a emergência de obstáculos significativos à actividade das seguradoras, os quais não podem admitir-se no âmbito da execução de contratos caracterizados pelas notas da aleatoriedade e da Uberrima Fides.

[59] Para além das múltiplas exigências constantes nos art.os 5.º, 6.º e 7.º do Regulamento 2016/679 para a obtenção do consentimento, as quais apenas se revelam compreensíveis no âmbito da categoria dogmática de um Consentimento Informado, importa ainda colocar em destaque que recai sobre o responsável pelo tratamento dos dados o ónus de provar que "... o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.". Desta feita, tendo o contrato sido celebrado com prévio esclarecimento da contraparte pela entidade responsável pelo tratamento de dados das finalidade específicas da recolha no âmbito da relação contratual em causa, então não constituirá surpresa para os titulares dos dados a realização de operações parciais de captação de dados que se revelem necessárias durante a pendência do contrato, sem ser, contudo necessário o consentimento fragmentado para tais específicos actos contratuais.

V. Os dados relativos à saúde como dados sensíveis – Seguros de saúde e tratamento de dados

A simples localização sistemática dos seguros de saúde no âmbito dos seguros de pessoas (art.º 175.º e ss. do Decreto Lei n.º 72/2008) é de molde a não suscitar dúvidas quanto ao relevo assumido pela recolha e tratamento de dados pessoais dos tomadores e segurados, tanto no período da formação do contrato, quanto na fase da respectiva execução.

Abrangendo-se nas apólices dos seguros de saúde, quer as situações clássicas de alteração involuntária do estado de saúde (o comummente designado seguro de doença), quer as despesas médicas resultantes de tratamento e outras realidades (partos...)[60], torna-se absolutamente essencial para a actividade das seguradoras o acesso a um acervo de elementos informativos relativos à esfera pessoal dos proponentes (idade, estrutura física e perfil psicológico das pessoas, hobbies, hábitos de consumo de determinados bens como álcool, estupefacientes..., vida sexual dos tomadores...).

Como já tivemos ocasião de sublinhar ao longo do trabalho, este tipo de dados integra-se numa categoria especial de dados de dados pessoais: os dados sensíveis.

Recordando ainda quanto já ficou anteriormente exposto, a qualificação deste tipo de dados como dados sensíveis não se consubstancia numa inócua e indiferente tarefa dogmática, porquanto o legislador comunitário faz-lhe associar importantes

[60] Cfr, a este propósito, Brito, J. Alves, anotação ao art.º 213.º da Lei do Contrato de Seguro, *in Lei do Contrato de Seguro anotada...,* ob. cit.,pg.577.

consequências de regime jurídico, como claramente decorre de uma simples leitura do art.º 9.º n.º 1 do Regulamento n.º 2016/679.

A exigibilidade de um consentimento explícito (art.º 9.º n.º2, al.) a) do Regulamento de dados pessoais), do titular dos dados como condição para derrogar a regra da proibição do tratamento dos dados relativos à saúde, pode representar, sem margem para dúvidas, um forte obstáculo para as seguradoras acederem a um conjunto de informações tidas por absolutamente essenciais para as seguradoras procederem à avaliação e monitorização do risco[61].

Tais dificuldades revelam-se, de resto, acrescidas pelo entendimento restritivo que tem sido dominante quanto ao tipo de consentimento explícito, mencionado no art.º 9.º, n.º2, al.) b), baseado numa certa interpretação do considerando n.º43 do Regulamento Geral de Protecção de Dados, perspectivando-se esse consentimento como um consentimento específico, segmentado, ou seja, *como um consentimento particularmente qualificado e informado.*

Mencionadas sumariamente as dificuldades suscitadas pelo regime jurídico plasmado no Regulamento de Protecção de Dados Pessoais à celebração dos seguros de saúde, importa, neste momento, evidenciar algumas específicas realidades coenvolvidas neste tipo de contratos, onde intensamente se vivencia um conflito entre a legitimidade de recolha e tratamento de informação pelas seguradoras e a tutela dos direitos de personalidade[62] dos titulares dos dados.

Nesta sede, não podemos deixar de fazer menção à admissibilidade de cobertura de doenças pré-existentes, tal como expressamente resulta do art.º 216, n.º1 do Decreto Lei n.º72/2008.

Revelando-se possível as apólices de seguros de saúde abrangerem doenças pré-existentes, então as seguradoras para poderem avaliar devidamente o risco a segurar têm de aceder a um conjunto de informações que lhes permitam ajuizar acerca da pré-disposição constitucional dos proponentes. Importa, porém, ter em conta que este mesmo preceito da lei dos seguros prevê a possibilidade da exclusão genérica ou especificada das doenças pré-existentes, revelando a prática seguradora que no âmbito dos seguros de saúde são mais frequentes as cláusulas de exclusão genéricas, ao invés de quanto sucede no universo dos seguros de vida, onde é mais usual o recurso às exclusões especificadas deste tipo de patologias[63].

Uma tal diferença tendencial resulta fundamentalmente da circunstância da contratação no contexto dos seguros de saúde recorrer, por regra, aos procedimentos característicos do tráfico jurídico de massas[64].

Estando em causa exclusões específicas de doenças pré-existentes no âmbito dos seguros de saúde, o que, de resto, corresponde, como vimos, a situações menos vulgares, então

[61] A exigibilidade de consentimento explícito dos proponentes manifesta-se, desde logo, quanto à realização de exames médicos, tidos por necessários para a seguradora celebrar o contrato de Seguro. Não admira assim que o art.º 178.º da Lei do Contrato de Seguro tenha definido um regime específico atinente à informação sobre exames médicos, impondo às seguradoras o dever de esclarecer os candidatos à celebração do contrato de seguro acerca de um conjunto de elementos respeitantes aos ditos exames médicos.

[62] Cfr, neste sentido, Vicente, Pedro Rubio, *El Deber Precontratual de Declaración del Riesgo en el Contrato de Seguro*, Madrid,2003, pg. 148 e ss.

[63] Cfr, a este propósito, Poças, Luis, *O dever de Declaração...*, ob. cit., pgs.733-734

[64] Cfr, neste sentido, Poças, Luis, *O Dever de Declaração...,* ob. cit., pgs.733.

assume uma particular relevância as informações transmitidas pelo proponente às seguradoras através da declaração inicial do risco. Porém, quando das apólices constarem exclusões genéricas de patologias pré-existentes, tende a destacar-se a irrelevância da declaração inicial do risco[65], porquanto se a pessoa segura estiver afectada por uma tal doença, a cobertura do seguro será automaticamente excluída, uma vez verificadas as respectivas manifestações ou sintomatologias.

Parece-nos demasiadamente simples chegar a uma tal conclusão, uma vez que a circunstância de as seguradoras não cobrirem pura e simplesmente encargos inerentes aos tratamentos de tais doenças, não afasta, de modo algum o relevo que necessariamente se tem de atribuir ao acesso pelas seguradoras a dados que possam, de algum modo, indiciar a existência de tais patologias excludentes.

Assim sendo, o proponente do seguro tem o dever na declaração inicial do risco de transmitir à seguradora os dados neste contexto relevantes, e que por si sejam conhecidos[66].

Na verdade, para o efeito automático do afastamento da cobertura pela seguradora ocorrer, em virtude da existência das mencionadas cláusulas genéricas de exoneração, torna-se muito importante a eficaz e fluida circulação de informação transmitida às seguradoras.

[65] Cfr, a este propósito, Poças, Luis, O Dever de Declaração..., ob. cit., pgs. 734.

[66] Como a este propósito, justamente sublinha Luis Poças "... ao permitir uma aferição mais rigorosa do risco (aproximando o risco estimado do real), o domínio dessa informação pode revolucionar a actividade seguradora, possibilitando uma melhor segmentação do risco e beneficiando, dessa forma, o segurado consumidor e a própria mutualidade segura". Cfr, Poças, Luis, O Dever de Declaração..., ob. cit., pg.743.

Em face das declarações emitidas pelos proponentes de seguro, que de algum modo indiciem a existência das doenças pré-existentes, as seguradoras podem ter um interesse legítimo na recolha de dados clínicos, qualificados pelo regulamento de protecção de dados pessoais, como sensíveis.[67]

Em tais hipóteses, o que verdadeiramente se questiona é se faz sentido exigir como condição de admissibilidade para a recolha de tais dados, o consentimento explícito, específico e segmentado dos tomadores ou seguradores.

Com efeito, se a resposta a esta questão for positiva, como parece resultar do regime do Regulamento n.º2016/679, as seguradoras podem acabar por proceder a uma avaliação insuficiente e pouco esclarecida do risco.

Dir-se-á que uma vez ocorridas tais hipóteses, nunca a seguradora ficará desprotegida uma vez que sempre poderá proceder à anulação do contrato de seguro, ou à sua modificação,

[67] A formulação legal contida no art.º 24.º do actual regime do Contrato de Seguro, faz inculcar a ideia que o legislador elegeu o conhecimento efectivo e não apenas a mera cognoscibilidade como pressuposto para aplicação do preceito. Uma interpretação da leitura deste preceito legal não permite chegar a uma outra conclusão. Nesse sentido se pronunciam vários autores na doutrina nacional, cfr, Gomes, Júlio," O Dever de Informação do (candidato/a),..., ob. cit., pg.405.Porém, na doutrina, há quem advogue posição diversa atribuindo relevância às hipóteses de desconhecimento pelo proponente da factualidade com negligência grosseira, cfr, Oliveira, Arnaldo, *Anotação ao art.º 24.º da Lei do Contrato de Seguro,(Pedro Romano Martinez e Outros)*, Coimbra, 2016, 3.ª Ed., pg.138. Também Luís Poças, ancorando-se no sentido de Boa-Fé subjectiva sufragado por Menezes Cordeiro (Boa-Fé ética), defende que " O sentido literal inerente ao "conhecimento" comporta, portanto, a omissão culposa de ciência, pelo que a mera interpretação declarativa lata dá já suporte ao entendimento "subscrito", cfr, Poças, Luis, O Dever de Declaração..., ob. cit. Pg. 342.

nos termo previstos, respectivamente, nos art.os 25.º e 26.º do Decreto Lei n.º72/2008.

Para além das dificuldades ou contingências que um qualquer regime sancionatório pode suscitar, dificuldades essas a que o regime estabelecido na lei dos seguros quanto à declaração inicial do risco não se encontra também imune, certo é que verdadeiramente desejável será o ordenamento jurídico dispor de expedientes ou mecanismos aptos para garantir o efectivo acesso às informações pelas seguradoras, evitando, assim, na medida do possível, o recurso aos ditos mecanismos sancionatórios.

Uma boa disciplina jurídica em torno de qualquer matéria ou assunto não pode centrar-se no momento sancionatório, devendo antes permitir conseguir que os critérios de justiça que se lhe encontram subjacentes se tornem efectivamente operantes.

Ora, o regime plasmado nos arts.os 24.º a 26.º do Decreto Lei n.º72/2008, não se encontra à margem destas observações genéricas, que conquanto genéricas, não deixam de ser importantes considerações axiológicas[68].

Razão pela qual, no âmbito de um contrato como o de seguro, onde o conhecimento de dados pessoais dos tomadores pelas seguradoras se revela fundamental, tanto na fase de formação do contrato, quanto durante a respectiva execução, a aplicação do regime do Regulamento de Protecção de Dados deverá ser mediada por uma legislação interna no âmbito do

[68] Como tivemos ocasião de sublinhar, todo e qualquer regime jurídico -positivo convoca um momento de validade, revelando-se essencial a apreensão dos princípios jurídicos fundamentais em que se sustentam as soluções legais para compreender a respectiva teleologia. Acerca da relevância do momento de Validade no âmbito das Fontes do Direito, cfr, Neves, A. Castanheira, *Digesta*, Volume 2.º. *Escritos acerca do Direito, do Pensamento Jurídico, da sua Metodologia e Outros*, Coimbra, 1995, pg. 58 e ss.

direito dos seguros que tornasse mais fácil o acesso às seguradoras de dados sensíveis, entre os quais se incluem, de modo paradigmático, os dados relativos à saúde.

Como, de resto, teremos ocasião de esclarecer adiante de um modo mais desenvolvido, uma tal solução encontra respaldo no art.º 9.º, n.º4 do Regulamento 2016/679.

VI. Seguros de saúde e tratamento de dados genéticos

Particularmente relevante no âmbito da celebração dos seguros de saúde, como já tivemos ocasião de sublinhar no capítulo II, se traduz a questão de saber se às seguradoras será permitida a solicitação ou a utilização de informação genética dos tomadores do seguro ou dos segurados.

Não é possível ignorar, a importância assumida pelas modernas técnicas genéticas a nível do diagnóstico das doenças, permitindo um tal tipo de testes alcançar um resultado muito fiável no tocante à detecção de algumas patologias, tal como sucede a propósito das doenças monogénicas (incuráveis), bem como em relação à identificação de meras predisposições para certas doenças cuja superveniência seja susceptível de se manifestar com um elevado grau de probabilidade.

Podemos assim reconhecer que ao lado das técnicas tradicionais de diagnóstico, a detecção de doenças encontra nas possibilidades que lhe são abertas pela realização de testes genéticos um importante aliado, acabando por se registar uma certa concorrência entre os dois universos[69] acabados de mencionar.

[69] O recurso à informação genética poder-se-á revelar um instrumento importante para as seguradoras poderem mais rigorosamente proceder à al-

Ora, assim sendo, a pergunta com que iniciámos este ponto da nossa exposição assume uma particular acuidade. Nesta sede, importa começar por referir que esta matéria surge regulada no nosso ordenamento jurídico na lei n.º12/2005, de 26 de janeiro, no seu art. .º12.º, lei essa para a qual o Regime Geral do Contrato de Seguro remete.

Uma simples leitura do art.º 12.º da lei n.º 12/2005 permite concluir, sem margem para dúvidas, que se proíbe, em abstracto e aprioristicamente às seguradoras a solicitação ou a utilização de informação genética de qualquer tipo (art.º 12.º, n.º3 da lei 92/2005).

Trata-se, na verdade, de uma proibição bastante severa[70], uma vez que a mesma se estende quer a potenciais tomadores, quer a actuais segurados e , ainda porque a proibição impede as seguradoras de recorrerem a dados genéticos, quer para recusarem a celebração de contratos, quer para procederem a um aumento ou agravamento do prémio. Mais ainda, a regra proibitiva constante do art.º 12.º da lei n.º 12/2005, não permite

mejada segmentação dos riscos. Porém, o risco de mortalidade ou de ocorrência de doenças desde sempre foi reflectido nos cálculos actuariais das seguradoras. Razão pela qual, não nos parece inteiramente correcto afirmar que as seguradoras revelam uma particular obsessão com o acesso à informação genética. Sobre esta questão, cfr, Oliveira, Guilherme, "Implicações Jurídicas do Conhecimento do Genoma", *Temas do Direito da Medicina,* Coimbra, 1999, pg. 144.

[70] Particularmente crítico de uma solução semelhante acolhida no Ordenamento Jurídico dos Seguros Belga se manifesta Marcel Fontaine, alertando para o enorme perigo de com este tipo de medida se admitirem práticas discriminatórias entre quem sofre doenças genéticas e quem padeça de outras patologias de diferente origem. Cfr, Fontaine, Marcel, *Droit des Assurances*, 3.ª Ed., Bruxelas, 2006, pg.171.

às seguradoras, nem imporem a realização de testes genéticos a potenciais ou actuais tomadores, nem aproveitarem os resultados dos testes genéticos já a estes entretanto realizados.

Estando em causa uma proibição com um âmbito objectivo e subjectivo tão amplo, poder-se-á concluir que, tal como atrás já mencionámos, se trata de uma proibição absoluta para as seguradoras recorrerem ou utilizarem resultados de testes genéticos. Subjacente a toda a problemática em análise, encontra-se o direito dos tomadores à ignorância ou a não terem conhecimento do seu estado de saúde[71], o qual deve ser visto como o reverso da medalha do direito ao conhecimento acerca do estado clínico, que a todos deve ser reconhecido, o qual, por seu turno, se encontra expressamente previsto na letra do n.º2 do art.º 3.º da lei n.º12/2005.

Na eventualidade de ser aceitável que as seguradoras acedam ao conhecimento dos resultados dos testes genéticos, este direito à ignorância acerca do estado de saúde pessoal levantaria particulares dificuldades no tocante ao cumprimento do dever de declaração inicial do risco previsto no art.º 24.º do Decreto Lei n.º72/2008.

Com efeito, um tal direito à ignorância dos resultados dos testes genéticos, fundado na exigência de tutela dos bens da personalidade de quem a estes se submete[72], por se enten-

[71] Acerca deste fundamento para a proibição de acesso aos resultados dos testes genéticos pelas seguradoras, cfr, Rego, Margarida Lima, *Contrato de Seguro...,* ob. cit., pg. 140 (nota 288).

[72] Com efeito, na base deste direito à ignorância quanto aos resultados dos testes genéticos está naturalmente o argumento, de acordo com o qual, a revelação de tais dados ao respectivo titular é de molde a causar-lhe enormes perturbações emocionais.

der que a revelação de tais dados lhes é susceptível de causar enormes perturbações emocionais, pode contender indelevelmente com o dever de transmitir as informações relevantes para a apreciação do risco a cargo dos tomadores de seguro ou dos segurados, caso lhes seja exigível revelar à seguradora a existência de tais testes.

Revelando-se incontestada a existência do direito a não ter conhecimento dos resultados dos exames de saúde realizados, certo é que as pessoas que pretendessem salvaguardar um tal direito e simultaneamente quisessem celebrar um contrato de seguro, acabariam por se encontrar envolvidas no âmbito de um modelo de admissibilidade de recurso aos testes genéticos, numa situação de conflito entre o exercício de um direito e o cumprimento de um dever.

Importaria então ponderar se o proponente à celebração do contrato de seguro se poderia escusar a cumprir o dever plasmado no art.º 24.º do Regime Geral do Contrato de Seguro, com fundamento na circunstancia de a não revelação das informações ser precisamente o resultado do exercício de um direito que lhe assiste: o direito ao não conhecimento do seu estado de saúde.

Estando em causa o exercício de um direito de personalidade, cujos efeitos são oponíveis até a terceiros, poder-se-á considerar que a invocação de um tal direito em face da seguradora constituirá uma causa legítima de escusa, pois caso contrário poder-se-ia sustentar, que no âmbito da celebração de um contrato de seguro, a seguradora incorreria na violação de um direito absoluto, emergindo então também questões de índole extracontratual.

Admitindo-se a procedência desta causa de exclusão de incumprimento do dever de declaração inicial do risco, já não se colocaria também a eventual questão da culpa do proponente pela ausência de transmissão das informações, porquanto um tal acto de transmissão não lhe era exigível.

Poder-se-á, no entanto, questionar acerca da possibilidade, no âmbito do modelo em análise, encontrar um ponto de equilíbrio entre o direito à ignorância quanto ao estado de saúde e a exclusão do dever de declaração inicial do risco, permitindo-se a quem simultaneamente é titular de um direito e sujeito de um dever, não ter acesso ao conhecimento dos resultados dos seguros genéticos, por um lado, mas exigindo-lhe, por outro, o dever de transmitir à seguradora que foram realizados testes genéticos.

Pensamos que no plano do direito a constituir, uma tal solução se nos afigura razoável, uma vez que permite uma certa conciliação entre o exercício dos poderes inerentes a um direito e o cumprimento das exigências coenvolvidas num dever.

Porém, a lei nacional que vigora em matéria de informação genética (lei n.º12/2005/) não abre espaço para a defesa de uma tal solução, e não se vislumbra, de resto que, do ponto de vista do direito constituído, o regime jurídico dedicado a esta matéria se venha a alterar tão cedo, porquanto o art.º 9.º n.º1 do Regulamento 2016/679 veio a incluir o tratamento dos dados genéticos no âmbito das categorias especiais de dados pessoais, as quais se encontram sujeitas, como já deixámos referido, a um regime particularmente severo e limitativo para as seguradoras.

Não podemos ainda ignorar que no âmbito desta proibição imposta às seguradoras de acederem aos resultados dos testes genéticos dos candidatos ao seguro se encontra a problemática questão da admissibilidade das práticas de segmentação do risco. No centro desta problemática encontram-se natural-

mente questões complexas, entre as quais resulta o perigo da proliferação de comportamentos discriminatórios pelas seguradoras, por um lado, e o risco de emergência de um fenómeno de agravada selecção adversa, susceptível de provocar um aumento global e genérico do montante dos prémios[73], por outro.

Na nossa perspectiva, o regime estabelecido, quer na lei n.º12/2005, quer no regulamento 2016/679, constitui, um particular obstáculo à efectivação dos direitos das seguradoras a acederem ao conhecimento de dados pessoais tidos como particularmente relevantes para a conclusão dos contratos de seguro, sobretudo quando estiverem em causa seguros de saúde.

De resto, este regime particularmente severo para as seguradoras não parece encontrar razão justificativa no receio destas comunidades de risco invadirem ilegitimamente a esfera de personalidade dos segurados.

Com efeito, se ao titular dos dados se reservasse o direito de transmitir as informações relevantes sobre a saúde aos médicos das seguradoras, a tutela dos seus direitos de personalidade encontraria um apoio significativo nos deveres de sigilo que recaiam sobre estes profissionais de saúde.

Ficaria incompleta esta exposição se não fizéssemos ainda menção, conquanto sumária, a uma questão idêntica de tutela dos direitos de personalidade dos proponentes de seguro (tomadores de seguro e segurados), no âmbito do cumprimento do dever de declaração inicial do risco: a questão de saber se o

[73] Para uma análise mais aprofundada desta problemática, cfr, REGO, MARGARIDA LIMA, *O Contrato de Seguro*..., ob. cit., pg. 106 e ss. (especialmente nota 208). Sobre a problemática da selecção adversa no contexto das assimetrias informativas, cfr, MARTINS, INÊS OLIVEIRA, *O Seguro de Vida*...ob. cit., pg. 189. e ss.

proponente do seguro tem o dever de revelar um conjunto de aspectos respeitantes à sua esfera de vida privada, mormente de certos hábitos como sejam o consumo de álcool, de estupefacientes, de tabaco, ou até de certas questões atinentes aos seus comportamentos sexuais.

Os problemas suscitados pelas hipóteses acabadas de mencionar são substancialmente idênticos aos já atrás referidos, a propósito da problemática de revelação dos resultados dos testes genéticos. Porém, não existe quanto a todas estas questões uma resolução expressa tão clara como a que se encontra a propósito da submissão e revelação dos resultados de testes genéticos.

Relativamente ao tratamento de dados respeitantes à vida sexual, mormente as informações atinentes à orientação sexual dos proponentes, o art.º 9.º n.º1 do Regulamento 2016/679, sujeita-o a um regime particularmente severo e restritivo, dificultando a legítima actividade das seguradoras de acederem a informação relevante.

Importa sublinhar, que o acesso a um tal tipo de informação pode assumir uma particular relevância não apenas para que as seguradoras decidam, de modo livre e esclarecido, sobre a celebração ou não celebração do contrato, como ainda, na eventualidade de optarem pela conclusão do contrato, poderem fazer valer as exigências do principio da proporcionalidade entre o prémio e o risco[74], exigências estas contempladas em várias disposições da lei dos seguros (art.ºs 15.º, 92.º, 93.º e 94.º).

[74] Para maiores desenvolvimentos em torno do princípio de equivalência entre o prémio e o risco, cfr, REGO, MAFALDA LIMA, *O Contrato de Seguro*..., ob. cit., pg.375 e ss.

Nesta sede, importa destacar o art.º 15.º do Decreto Lei n.º72/2008, que na redacção introduzida pela Lei n.º 174/2015, de 9 de setembro, veio claramente permitir às seguradoras mobilizar as técnicas de segmentação do risco, e com base nelas, adoptar práticas discriminatórias quando na base das mesmas existam razões objectivas e actuariais que justifiquem uma diferença de tratamento.

Razão pela qual, nem mesmo em nome do princípio da igualdade de tratamento, princípio constitucional (art.º13.º C.R.P), cujo âmbito se estende também às relações entre os particulares[75], as seguradoras estão impedidas de recusarem a celebração de contratos de seguro ou de agravarem o prémio a pagar nas situações de deficiência do proponente ou de risco agravado de saúde.

No tocante à vasta panóplia de informações atrás mencionadas que se encontram estritamente conexionadas com hábitos de vida quotidiana (consumo de álcool, estupefacientes, tabaco, ...), poder-se-á dizer que o factor de neutralização para a revelação de tais dados às seguradoras se traduz no direito à reserva da vida privada dos respectivos titulares.

Apesar de não se encontrar expressamente previsto no art.º 9.º n.º1 do Regulamento 2016/679, o tratamento de dados pessoais que respeitem à reserva da vida privada em termos amplos e genéricos, certo é que boa parte dos dados pessoais aí mencionados "...dados pessoais que revelam a origem racional, ou étnica, as opiniões políticas, as convicções religiosas ou

[75] A propósito da relevância dos princípios constitucionais e dos Direitos Fundamentais nas relações entre os particulares, cfr, o nosso estudo, Responsabilidade Civil..., ob. cit., pg. 43 e ss., Canaris, Claus-Wilhelm, "Grundrechte und Privatrecht", *in Archiv fir Civilistiche Praxis*, 1984, pg.202 e ss.

filosóficas, ou a filiação sindical...", bem como os já atrás mencionados "dados relativos à vida sexual ou orientação sexual de uma pessoa", são atinentes à esfera da reserva da vida privada dos seus titulares.

Particularmente relevante se manifesta neste contexto a questão paralela da legitimidade das entidades patronais sujeitarem os trabalhadores a testes destinados a identificar os respectivos hábitos de consumo, entre os quais se destaca o consumo de bebidas alcoólicas e estupefacientes. A tutela da reserva da intimidade da vida privada dos trabalhadores representa assim um obstáculo significativo à admissibilidade da recolha de tais dados, conquanto a mesma ocorra em termos limitados, tal como se passa com a realização de testes em termos aleatórios[76], ou alternativos, tidos à partida, como consentâneos com as mais elementares exigências da tutela dos direitos de personalidade dos trabalhadores.

Importa, no entanto, sublinhar, numa apreciação um pouco mais aprofundada, que a submissão dos trabalhadores à realização de tal tipo de testes pode não representar uma devassa no direito à reserva de vida privada daqueles, conquanto o trabalhador possa impor que os dados resultantes da realização dos testes sejam apenas revelados aos médicos das empresas, os quais se encontram sujeitos, por força de exigências legais diversas, ao sigilo profissional.

No fundo, o dever de sigilo profissional acabaria por acautelar os riscos da violação dos direitos de personalidade dos ti-

[76] O recurso ao modelo de realização de testes clínicos em termos aleatórios, bastante utilizado no universo desportivo visa precisamente evitar situações de discriminação ou de assédio moral, cfr, a este propósito, Pinheiro, Alexandre Sousa, *Privacy e Protecção*..., ob. cit, pg. 201-202

tulares dos dados, riscos esses que o regulamento de protecção de dados visa precisamente neutralizar.

Por seu turno, a transmissão pelo médico à entidade patronal do risco de manutenção de trabalhadores com os mencionados hábitos de consumo pode revelar-se uma informação particularmente importante para alcançar objectivos de prevenção e planificação de riscos profissionais.

Nesta sede, importa sublinhar que a Comissão Nacional de Protecção de Dados já se pronunciou sobre a licitude da realização de testes de controlo sobre o consumo de álcool e de drogas no meio laboral, tendo-se manifestado favoravelmente em relação a esta querela, sendo que a licitude da recolha de tais dados pela entidade patronal se encontrava dependente do consentimento dos trabalhadores[77].

Porém, não havendo consentimento expresso dos titulares dos dados para que se proceda à respectiva recolha e tratamento, torna-se difícil admitir que a entidade patronal possa sujeitar os trabalhadores à realização de tais testes. Na verdade, não podemos ignorar que uma tal situação é susceptível de configurar uma atitude penalmente censurável, podendo traduzir-se até na prática do crime de intervenções e tratamentos médico – cirúrgicos arbitrários (art.º 156.º do Código Penal).

Estas considerações expendidas a propósito do contexto laboral, revelam-se extensivas à prática seguradora, podendo no universo dos seguros de saúde, duvidar-se da legitimidade das companhias de seguro imporem aos proponentes a realização de testes médicos, referindo-se a título de exemplo a realização de exames para detectar a seropositividade.

[77] Estamos a reportar-nos à autorização n.º479/03, de 3 de junho, disponível em < http://cnpd.pt/bin/decisões/aut/10_479_2003.pdf>. Sobre esta decisão, já foram, de resto, tecidas apreciações pela doutrina nacional, cfr, Pinheiro, Alexandre Sousa, *Privacy e Protecção*..., ob. cit., pg.201-201.

Poder-se-á, no entanto, questionar se sobre o tomador do seguro ou sobre o segurado que tendo conhecimento de ser portador do Vírus da Sida, não se imporá a obrigação de informar a seguradora no âmbito da declaração inicial do risco (art.º 24.º do Decreto Lei 72/2008), de tal circunstância, circunstância essa, que, a todas as luzes, terá de ser considerada como relevante para a seguradora proceder a uma adequada avaliação do risco.

Cumpre, na verdade, ter em conta na resposta a esta questão, que a multiplicação de entraves ao acesso de dados tidos por relevantes para a apreciação do risco pode determinar um défice significativo de informação da seguradora, o qual é, por seu turno, susceptível de despoletar a ocorrência de situações de celebração de contratos de seguro, no âmbito dos quais o risco se revela inexistente (art.º 44.º do Decreto Lei n.º 72/ 2008).

Razão pela qual, pensamos, que a resposta à questão atrás colocada não pode deixar de ser positiva, sob pena de em nome de uma protecção particularmente intensa dos direitos de personalidade dos titulares dos dados se estar a colocar em causa o respeito pelas exigências fundamentais do Princípio da Boa-Fé, bem como até a fazer perigar a própria estrutura aleatória do contrato

VII. A Necessidade de uma Legislação Especial de Protecção de Dados para o Universo da Actividade Seguradora

Neste momento de balanço das considerações expendidas ao longo do trabalho, importa destacar que o regulamento de protecção de dados pessoais vem colocar alguns embaraços à

actividade seguradora, tornando particularmente difícil às seguradoras acederem à informação tida por adequada para decidirem de forma livre, sã e esclarecida acerca da contratação, bem como ainda de adequarem durante a vigência da relação contratual o prémio a pagar e o risco segurado ou garantido pelo contrato de seguro[78].

Tais dificuldades que se afirmam genericamente no âmbito da actividade seguradora, assumem particular acuidade, como tivemos ocasião de sublinhar, a propósito dos seguros de saúde, uma vez que o legislador comunitário qualificou os dados de saúde como dados sensíveis, e estabeleceu como regra a proibição do respectivo tratamento (art.º 9.º, n.º1 do Regulamento 2016/679).

Apenas quando houver consentimento expresso do titular dos dados permitindo o tratamento de dados, ou a sua recolha se revelar necessária para o exercício de direitos ou para o cumprimento de obrigações do titular dos dados ou da entidade responsável pelo seu tratamento no âmbito da legislação de segurança social, laboral ou da protecção social (art.º 9.º. n .º 2, al.) b) do Regulamento 2016/679), será admitido o tratamento e conservação pelas seguradoras dos dados relativos à saúde.

No tocante aos seguros cuja celebração se revele obrigatória, poder-se-á descortinar alguma função de protecção social[79] por eles desempenhada, e apesar dos seguros de saúde

[78] Uma tal faculdade de adequação do prémio a pagar ao risco segurado encontra um particular respaldo nos art.os 92.º a 94.º da Lei do Contrato de Seguro.

[79] Cfr, a este propósito, o Parecer n.º 20/2018 da Comissão Nacional de Protecção de Dados a propósito de proposta de lei n.º 120/XIII/3.º, que "Assegura a execução, na Ordem Jurídica Nacional, do Regulamento (EU) 2016/679, relativo à protecção das pessoas singulares no que diz respeito aos tratamentos de

não serem obrigatórios, certo é que não será descabido evidenciar aí uma forte dimensão social.

Esta interpretação em torno do alcance do âmbito da al.) b) do n.º2 do art.º 9.º parece-nos correcta, apesar de sempre se poderem suscitar dúvidas se são susceptíveis de se incluir nos dados objecto de tratamento em matéria de "legislação laboral, de segurança social e de protecção social[80], os dados de saúde qualificados no n.º1 do art.º 9.º do dito regulamento como dados especiais, ou seja, como dados sensíveis.

Com efeito, poder-se-á legitimamente questionar se a actividade das seguradoras quando celebram seguros de saúde preenche as finalidades de protecção social tidas em vista na legislação, do respectivo sector, ou seja, se com uma tal actuação se prosseguem estratégias sociais específicas (neste caso, no âmbito da saúde), eleitas pela colectividade como significativas para prosseguir objectivos relevantes da polis.

Neste contexto, parece-nos não haver razoes justificativas para circunscrever a prossecução de finalidades públicas à actividade das entidades estaduais, podendo tais objectivos serem legitimamente atingidos pela actuação de entidades privadas, sobretudo quando uma tal actuação seja objecto de uma particular tutela pública, tal como é o caso das seguradoras.

dados pessoais e à livre circulação desses dados". Como expressamente refere este órgão quando analisa a derrogação da al.) b) do n.º2 do art.º 9.º do Regulamento a propósito da protecção social: "Deste modo, apenas se poderá enquadrar aqui os seguros de saúde, na medida em que se possa considerá-los ainda como uma forma de protecção social, (pg. 37 V. do parecer da Comissão Nacional de Protecção de Dados).

[80] Cfr, art.º 9.º, n.º2 al.) b) do Regulamento (EU) 2016/679.

Não podemos, na verdade, ignorar que entre os arquétipos ou modelos no âmbito dos quais se desenvolve actualmente a actividade de administração pública, se conta precisamente o *exercício privado de funções públicas,* registando-se nesta sede uma clara fuga para o Direito Privado[81].

Idênticas observações se podem estender relativamente à derrogação estabelecida na al.) g) do art.º 9.º do Regulamento (UE) 2016/679 à proibição de tratamento das categorias especiais de dados pessoais elencadas no n.º1 deste preceito. Aí se prescreve que pode haver lugar ao tratamento de dados pessoais especiais quando tal se revelar "necessário por motivos de interesse público importante, com base no direito da união ou de um Estado-Membro, ..."[82].

Esta ressalva do regulamento consubstanciada na prossecução do interesse público pode assumir uma particular relevância no universo dos seguros de contratação obrigatória.

Como a este propósito já se pronunciou a Comissão Nacional de Protecção de Dados "Ora, se se consegue acompanhar que no âmbito dos seguros obrigatórios é já reconhecido o interesse público, já o mesmo não acontece relativamente aos restantes seguros, designadamente os seguros de vida"[83].

[81] Sobre o exercício de funções administrativas por entidades privadas, cfr, Gonçalves, Pedro, *Entidades Privadas com Poderes Públicos*, Coimbra, 2005, pg.1038 e ss., Moniz, Ana Raquel, *Os Direitos Fundamentais e a sua Circunstância*, Coimbra, 2017, pg.128. e ss.

[82] Cfr, art.º 9.º n.º2, al.) g) do Regulamento (EU) 2016/679.

[83] Cfr, pg. 37 V. do parecer n.º20/2018 da Comissão Nacional de Protecção de Dados (processo n.º 6275/2018).

Porém, também a este propósito, tal como relativamente à protecção social referida na al.) b) do art.º 9.º n.º2 do Regulamento 2016/679, se pode questionar se o interesse público prosseguido no âmbito da categoria de seguros em análise, corresponde ao interesse público específico ou qualificado a que o regulamento comunitário neste preceito se reporta.

Não podemos a este propósito ignorar que os seguros obrigatórios desempenham uma função manifestamente social, tutelando, por conseguinte, interesses públicos relevantes.

Basta pensar no seguro de responsabilidade civil automóvel, onde a tutela do interesse público assume uma particular relevância, condicionando indelevelmente o regime jurídico correspectivo, ao ponto de obrigar as seguradoras a intervir em situações onde a lógica contratual não justificava a respectiva actuação (ex: art.º 15.º, n.º3 do Decreto Lei n.º 291/2007)[84].

No fundo, a disciplina jurídica positiva reservada a tais seguros (no caso do Decreto Lei n.º 291/2007), exprime claramente a influência regulativa de exigências de justiça distributiva e não apenas a necessidade de acautelar os interesses dos particulares, cuja tutela tem fundamentalmente subjacente razões de justiça comutativa.

Razão pela qual, à semelhança de quando atrás defendemos quanto à prossecução de uma inequívoca função de protecção social nos seguros de saúde, também a propósito dos seguros obrigatórios se pode afirmar que há razões justificativas baseadas no interesse público dos respectivos regimes ju-

[84] A propósito da função social do seguro patente nas hipóteses de furo, cfr., o nosso estudo, O Contrato de Seguro Obrigatório de Responsabilidade Civil Automóvel, Coimbra, 2001, pg. 384 e ss.

rídicos positivos para aplicar o regime especial contido no art.º 9.º n.º2 al.) g) do Regulamento (EU) 2016/679.

Importa, no entanto, sublinhar que nem mesmo a defesa deste entendimento mais amplo permite às seguradoras beneficiarem do regime diferenciado e mais favorável previsto no n.º2 do art.º 9.º do Regulamento de Protecção de Dados Pessoais, em certos domínios, tal como sucede com seguros tão relevantes como são *os seguros de vida*.

Em face de todas as considerações anteriores, pensamos ser possível às seguradoras no âmbito da celebração de contratos de seguro de saúde, ou de contratos de seguro de celebração obrigatória, acederem a dados pessoais sensíveis sem necessidade de obterem consentimento expresso do titular dos dados, ao abrigo, respectivamente da al.) b) e g) do n.º2 do art.º 9.º do Regulamento 2016/679.

No entanto, a admissibilidade de acesso aos dados e ao respectivo tratamento pelas entidades responsáveis nos universos que acabámos de mencionar com os fundamentos aludidos, não se revela algo absolutamente adquirido ou pacífico, em função de alguns obstáculos que tivemos ocasião de sublinhar ao longo da exposição.

Porém, e relativamente aos seguros, cuja celebração não seja obrigatória, bem como quanto aos seguros não integrados no âmbito dos seguros de saúde, os preceitos atrás mencionados (art.º 9.º, n.º2, al.) b) e g) do Regulamento 2016/679) não permitem às seguradoras aceder a dados importantes e proceder ao respectivo tratamento sem se submeterem ao espartilho dos art.os 9.º, n.º1, e 9.º n.º2 al.) a) do Regulamento de Protecção de Dados.

Em tais contextos, os múltiplos obstáculos colocados às seguradoras para procederem à recolha e ao tratamento dos

dados poderão ser ladeados se ao abrigo do n.º4 do art.º 9.º, o Estado Português emanar legislação destinada a prever condições mais flexíveis e razoáveis, tal como sufraga a Comissão Nacional de Dados[85].

Um tal propósito, que oferece inevitavelmente maiores garantias às seguradoras de acederem a informações necessárias à formação da vontade das partes de um modo *são*, l*ivre* e *esclarecido,* deverá ser concretizada, através de legislação interna específica em matérias de seguro, o que entre nós significa, incluir a disciplina desta matéria na Lei do Contrato de Seguro.

Como a este propósito justamente sublinha a Comissão Nacional de Protecção de Dados no seu parecer n.º 20/2018, a propósito da proposta de lei n.º 120/XIII/3.º (gov)[86] "... é imperioso que a lei nacional preveja não apenas a possibilidade de efectuar ou efectivar o tratamento de dados de saúde, mas também o respectivo regime do mesmo, designadamente os limites a que necessariamente tem de estar sujeito e as medidas de segurança e de mitigação do impacto sobre os direitos dos titulares dos dados – o que, na perspectiva da CNPD, terá mais

[85] "..., a CNPD entende que para os seguros que não sejam obrigatórios ou de saúde, apenas o n.º4 do art.º 9.º poderá servir para legitimar os Estados-Membros a prever em lei novas condições de tratamento. A seguir-se qualquer dos caminhos aqui apontados, é imperioso que a lei nacional preveja não apenas a possibilidade de efectuar o tratamento de dados de saúde, mas também o respectivo regime do mesmo, designadamente, os limites a que necessariamente tem de estar sujeito e as medidas de segurança e de mitigação do impacto sobre os direitos dos titulares dos dados" – pgs. 37v. e 38 do Parecer n.º20/2018 da CNPD.

[86] Cfr, pg.38 do Parecer n.º 20/2018 da CNPT.

sentido ser concretizado na legislação que regula este sector de actividade."[87].

Um tal entendimento encontra, na verdade, respaldo no art.º 9.º, n.º4 do Regulamento (UE) 2016/679, ao permitir aos Estados-Membros "manter ou impor novas condições" no que respeite ao tratamento de dados relativos à saúde[88].

Nem se diga em defesa de uma perspectiva diferente, bem mais restrita, que o artigo do regulamento acabado de mencionar, apenas permite aos Estados, ou manter a disciplina nele fixada relativa aos dados de saúde, ou estabelecer regimes onde o acesso e o tratamento dos dados se revele mais rigoroso.

O legislador comunitário ao referir-se no art.º 9.º n.º4 do Regulamento sobre Protecção de Dados Pessoais à possibilidade conferida aos Estados-Membros de impor novas condições, não parece ter querido restringir o âmbito de aplicabilidade do preceito às hipóteses de agravamento pelos Estados-Membros do acesso e tratamento de dados pessoais respeitantes à saúde.

Com efeito, o regulamento ao admitir aos Estados-Membros estabelecer mais condições, quer abrir a possibilidade de estabelecer outras condições, ou seja, diferentes condições das previstas no regime nele estatuído, e essas condições diferenciadas a constar em legislações nacionais, podem revelar-se condições mais flexíveis ou favoráveis.

[87] Como já atrás tivemos oportunidade de sublinhar, com esta proposta de lei, o governo tinha em vista assegurar a execução na Ordem Jurídica Interna do Regulamento EU 2016/679, relativo à protecção das pessoas singulares no que toca ao tratamento de dados pessoais. Cfr, pg. 38 do Parecer n.º 20/2018 da CNPD.

[88] O Regulamento (EU) 2016/679, reporta-se para além dos dados atinentes à saúde, aos dados genéticos e aos dados biométricos.

Desta feita, a referência constante do art.º 9.º, n.º4, onde se confere aos Estados-Membros a alternativa de manter ou impor novas condições, deve entender-se, como a faculdade atribuída aos Estados-Membros ou de manterem o regime constante do regulamento ou de estabelecerem disciplinas jurídicas diferentes, em matéria de acesso e tratamento de certos tipos especiais de dados pessoais, entre os quais se incluem os dados de saúde.

A TUTELA ADMINISTRATIVA DE DADOS PESSOAIS EM MATÉRIA DE SEGUROS: EM ESPECIAL, A AUTORIDADE REGULADORA[*]

Ana Raquel Gonçalves Moniz

1. As preocupações com a aquisição, tratamento e partilha de dados representam uma das tendências de evolução do direito, associadas à explosão tecnológica, com repercussões em todas as áreas sociais, económicas e financeiras. Sob as vestes da mundialização das sociedades, assomam fenómenos tão distintos como a mobilidade e o comércio transnacionais, a regulação por meio de atores não-estaduais ligados em redes globais, o aumento do âmbito e da fluidez das redes societais decorrente da evolução dos meios de comunicação que potencia a ubiquidade[89], a transnacionalização das instituições polí-

[*] O presente texto corresponde à versão escrita da comunicação oral apresentada no Colóquio *Seguros, Seguradoras e o Novo Regulamento de Proteção de Dados*, a que apenas se adicionaram as notas de rodapé com as respetivas referências bibliográficas.

[89] Cf. também Delmas-Marty, *Le Relatif et l'Universel – Les Forces Imaginantes du Droit*, vol. I, Seuil, Paris, 2004, pp. 337 e ss.., e *Le Pluralisme Ordonné – Les Forces Imaginantes du Droit*, vol. II, Seuil, Paris, 2006, p. 21, enfatizando que a Internet, em virtude das suas características da imediaticidade e da neutralidade, anula a territorialidade e fragiliza os sistemas jurídicos nacionais, potenciando os conflitos de jurisdição.

ticas, a aproximação, miscigenação e assimilação de culturas[90], e a emergência de "violações espontâneas das fronteiras" realizadas pela poluição, pelo crime organizado, pelas epidemias, pelos riscos associados à tecnologia de ponta e pelo impacto da adoção de políticas nacionais que acabam por tocar cidadãos de outros Estados[91].

A Internet e as tecnologias de informação em geral, em virtude das suas características da imediaticidade e da neutralidade, tendem a anular a territorialidade e a fragilizar os sistemas jurídicos nacionais, potenciando os conflitos e contribuindo cada vez mais para a construção de um *Big Brother* – não necessariamente (e cada vez menos...) estadual, mas privado, sobretudo quando se considera serem as grandes corporações as detentoras do maior volume de dados pessoais.

A atividade seguradora não escapa, naturalmente, aos desafios colocados pelas tecnologias de informação, e a significativa quantidade de dados armazenados nos seus sistemas

[90] Walker, «Beyond Boundary Disputes and Basic Grids: Mapping the Global Disorder of Normative Orders», in: *International Journal of Constitutional Law*, n.os 3/4, vol. 6, julho/outubro 2008, p. 374; Bignami, «Individual Rights and Transnational Networks», in: Rose-Ackerman/Lindseth (eds.), *Comparative Administrative Law*, Cheltenham/Northampton, 2010, p. 633.

Ainda que, em muitos casos, esta aproximação ou integração de culturas ou perspetivas filosófico-sociológicas se revele mais aparente que real, pois que a construção de múltiplas identidades que a Internet permite (desde logo, através das redes sociais) pode contribuir para reforçar os estereótipos – refletindo sobre este problema no contexto da criação de identidades alternativas *on-line*, *v.* Rodotà, *La Vita e le Regole: Tra Diritto e Non Diritto*, Feltrinelli, Milano, 2006, pp. 77 e s..

[91] Habermas, «Crossing Globalization's Valley of Tears», in: *New Perspectives Quarterly*, n.º 4, vol. 17, outono 2000, p. 52.

coloca questões delicadas sob a ótica da preservação de identidades e da garantia da autonomia pessoal quanto à recolha, tratamento, destino e conservação das informações detidas pelas empresas da área dos seguros – sobretudo se pensarmos nas possibilidades que o cruzamento de tais informações pode oferecer quer para poderes públicos, quer para entidades privadas, com perigos para a tutela da intimidade da vida privada, para o princípio da igualdade (em virtude da suscetibilidade de gerar exclusões sociais) e para a liberdade.

Neste contexto, não surpreenderá que a proteção dos dados surja integrada no direito à autodeterminação informativa, concebido como direito fundamental, pela Constituição portuguesa (cf. artigo 35.º da CRP) – e, significativamente, com autonomia face à reserva da intimidade da vida privada[92], asso-

[92] A íntima relação entre a reserva da intimidade da vida privada e a autodeterminação informativa influencia, desde logo, o próprio conceito dos dados pessoais protegidos pelo artigo 35.º da CRP, os quais, em geral, se identificarão, no contexto jurídico-constitucional, com qualquer informação detida, independentemente do seu suporte, a respeito de uma pessoa singular identificada ou identificável (cf. também, mas apenas como arrimo interpretativo, o artigo 2.º, alínea *a)*, da *Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de carácter pessoal*, aprovada pela Resolução da Assembleia da República n.º 23/93 e ratificada pelo Decreto do Presidente da República n.º 21/93 (in: *Diário da República*, I Série-A, n.º 159, 09.07.1993)].

Estando em causa um direito com indefetíveis conexões com a personalidade humana e relacionado com o direito à privacidade, o âmbito subjetivo de proteção constitucional dos «dados pessoais» circunscreve-se, em regra, às pessoas singulares (cf. Gomes Canotilho/Vital Moreira, *Constituição da República Portuguesa Anotada*, 4.ª ed. vol. I, Coimbra Editora, Coimbra, 2007, p. 558, anotação XV ao artigo 35.º; em sentido próximo, quanto à titularidade do direito à intimidade da vida privada, Paulo Mota Pinto, «O Direito à Reserva Sobre a Intimidade da Vida Privada», in: *Boletim da Faculdade de Direito*, vol.

ciando a sua proteção à institucionalização de uma entidade administrativa independente. Ou ainda que a *Carta dos Direitos Fundamentais da União Europeia* contemple, *ex professo*, um direito à proteção dos dados pessoais, ficando o cumprimento das disposições nesta matéria sujeito à fiscalização de uma entidade administrativa independente (cf. artigo 8.º).

A autonomização de um direito à autodeterminação informativa ou à proteção dos dados pessoais surge plenamente

LXIX, 1993, p. 553; diversamente, Bacelar Gouveia, «Os Direitos Fundamentais à Protecção de Dados Pessoais Informatizados», in: *Revista da Ordem dos Advogados*, n.º 3, ano 51, dezembro 1991, p. 711). Mesmo quando assim se entenda, tal não significa, porém, uma ausência de proteção das pessoas coletivas nesta matéria que veem os dados a elas respeitantes tutelados por outros direitos fundamentais de que beneficiam.

Considera-se, pois, que qualquer registo e divulgação de dados pessoais não consentida pelo respetivo titular pode representar uma intromissão na sua vida, assimilada, por alguma doutrina, à própria invasão do domicílio (Barbosa de Melo/Cardoso da Costa/Vieira de Andrade, *Estudo e Projecto de Revisão da Constituição*, Coimbra Editora, Coimbra, 1981, p. 54).

Não podemos ignorar que, dentro do conceito de dados pessoais se encontram sobretudo abrangidos aqueles que respeitam à esfera *pessoalíssima* individualizados no n.º 3 do artigo 35.º (dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica), protegendo o respetivo titular contra o tratamento informático não autorizado ou não previsto por lei. A especial natureza destes dados levou ainda a que o legislador ordinário criminalizasse os comportamentos dirigidos a criar, manter ou utilizar ficheiro informatizado onde os mesmos constem (cf. artigo 193.º do Código Penal) – a acentuar que, para lá da posição jurídica subjetiva garantida ao cidadão, também existe uma obrigação constitucionalmente imposta de o Estado sancionar de forma especialmente exigente o mero registo daquelas informações pessoalíssimas e insindicáveis [nestes termos, Damião da Cunha, «Artigo 193.º – Anotação», in: Figueiredo Dias (dir.), *Comentário Conimbricense do Código Penal*, tomo I, Coimbra Editora, Coimbra, 1999, p. 194].

consonante com uma das perplexidades hoje emergentes da teoria dos direitos fundamentais e que produz um duplo resultado: por um lado, aumentam os direitos destinados a responder aos novos riscos; por outro lado, crescem as restrições a liberdades individuais em nome da tutela da segurança. Tudo isto no contexto de uma tensão, presente no espaço global, entre o empobrecimento e o enriquecimento dos direitos (a outra face da tensão entre restrição e extensão), que começam a (sobre)viver sob a égide da supremacia do mercado e da necessidade de segurança[93].

Assim, se, por um lado, foi a sucessão das "gerações" de direitos fundamentais que permitiu o surgimento do direito à autodeterminação informativa e do direito à proteção de dados pessoais, por outro lado, a guerra contra o terrorismo vem consentir na previsão de restrições (também) a estes direitos com o propósito de salvaguardar a segurança – pondo, assim, em causa a proteção dos dados, em especial, a garantia da sua confidencialidade. Esta compulsão pela busca da segurança ultrapassa também as fronteiras dos Estados (ou das organizações de Estados), começa a ser desenvolvida também por corporações privadas, e, numa era de "vigilância global", e parece reclamar também uma constitucionalização (normação constitucional) global das estruturas de comunicação[94], chamando a atenção, quanto ao ponto que nos interessa, para o problema do tratamento de dados transfronteiriços.

[93] Cf. também Rodotà, *Il Diritto di Avere Diritti*, Laterza, Roma/Bari, 2015, pp. 3 e s..

[94] Cf. Fischer-Lescano, «Struggles for a Global Internet Constitution: Protecting Global Communication Structures Against Surveillance Measures», in: *Global Constitutionalism*, n.º 2, vol. 5, julho 2016, pp. 145 e ss..

2. Todas estas preocupações se encontram subjacentes à emanação do *Regulamento Geral de Proteção de Dados* (RGPD)[95]. São vários os aspetos que, encontrando-se versados no Regulamento, se localizam no entrelaçamento com a atividade seguradora: eis o que acontece, por exemplo, com os problemas relacionados com a "definição de perfis"[96], ou com a natureza dos dados objeto de tratamento quando estão em causa seguros de pessoas (como sejam os dados relativos à saúde ou os dados genéticos, que consubstanciam, na terminologia do Regulamento, categorias especiais de dados).

Não se ignora, porém, que a proteção conferida por este diploma se encontra (assumidamente) funcionalizada à satisfação dos fins da construção europeia, tendo como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares, e nessa medida, visando gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno[97].

[95] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, in: *JOUE*, n.º L 119 04.05.2016, pp. 1 e ss., retificado no *JO*, L 127, de 23.05.2018, pp. 2 e ss..

[96] Nos termos do n.º 4 do artigo 4.º do RGDP, entende-se por definição de perfis "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações".

[97] Cf. §§ 2 e 7 do preâmbulo, respetivamente.

O facto de a proteção de dados pessoais ser agora efetuada por regulamento europeu (e não apenas, como sucedia anteriormente, através de uma diretiva) reveste-se de um propósito não despiciendo: assegurar um nível de proteção coerente, elevado e tendencialmente homogéneo dos direitos (fundamentais) em todos os Estados-membros, eliminando as divergências entre os ordenamentos estaduais, sem prejuízo da manutenção da autonomia em determinados aspetos[98] – aliás, é uma tal tensão dialética entre coerência e autonomia que vamos encontrar na configuração da autoridade nacional de controlo, relativamente à qual o Regulamento fixa um substrato de normas destinado a delinear o sentido da autoridade nacional de controlo, assim como as respetivas funções e poderes, atribuindo, deste quadro, alguma autonomia aos Estados-Membros.

3. Esta referência à autoridade de controlo (nacional) permite-nos já dar um passo em frente, direcionando a nossa atenção para a forma como o RGDP a trata normativamente, e verificar se a sua configuração corresponde às tradicionais entidades administrativas independentes de tutela de direitos fundamentais ou se, como nos parece, estamos diante de uma figura dotada de alguma originalidade.

3.1. Importa, desde já, acentuar que a circunstância de estarem em causa questões relacionadas com os direitos fundamentais não conduz a que as reflexões sobre a respetiva tutela se orientem necessariamente para a sua defesa através dos tribunais. Se estes se assumem como instâncias privilegiadas de

[98] Neste sentido aponta também o preâmbulo do diploma: cf., *v. g.*, § 10.

proteção dos direitos (também no âmbito da autodeterminação informativa), a verdade é que, cada vez mais, a Administração Pública (*rectius*, determinadas entidades administrativas) desempenha(m) um papel relevantíssimo como guardiã(s) da Constituição e dos direitos fundamentais. Na verdade, a subordinação constitucional da atividade administrativa (o princípio da constitucionalidade da Administração) atinge a respetiva sublimação quando se considera que a perceção da Constituição como *higher Law* leva, de alguma forma, ínsita a ideia de que cabe àquela definir os fundamentos axiológicos-jurídicos em que repousa, em termos mais próximos ou mais longínquos, a ação da Administração Pública. Eis-nos diante de uma ideia que se reveste de particular importância no contexto da promoção dos direitos fundamentais.

O «constitucionalismo administrativo»[99] constitui uma particular expressão do princípio da constitucionalidade da Administração, que, no seio da doutrina anglo-saxónica (em especial, norte-americana), defende o "acesso direto" à Constituição pela Administração, cometendo a esta última responsabilidades ativas no que tange à interpretação e implementação dos princípios e imperativos constitucionais[100]. Trata-se de uma conce-

[99] Sobre o constitucionalismo administrativo, *v.* também o nosso trabalho «O *Administrative Constitutionalism*: Resgatar a Constituição para a Administração Pública», in: *Estudos em Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho*, vol. IV, Studia Iuridica 106, Boletim da Faculdade de Direito/ Coimbra Editora, Coimbra, 2012, pp. 385 e ss., que recuperamos em parte.

[100] Lee («Race, Sex, and Rulemaking: Administrative Constitutionalism and the Workplace, 1960 to the Present», in: *Virginia Law Review*, vol. 96, 2010, pp. 801, 806 e s.) sugere justamente que o *punctum saliens* do *administrative constitutionalism não reside na afirmação da subordinação administrativa à Constituição, funcionando esta como limite (negativo) da* atuação da Administração, mas antes na autonomia da interpretação e da implementação administrativas da Constituição e no modo como estas duas tarefas se refletem na ideia do *government by Constitution*.

ção que, visando sublinhar o radical democrático e a legitimação do poder administrativo[101] e intercedendo sobre as questões atinentes ao papel (aos papéis) desempenhado(s) pela Administração[102], toca a dinâmica das *relações entre poderes* (poder constituinte e poderes constituídos, e, dentro destes, poder legislativo, poder judicial e poder administrativo), das *relações entre «fontes de direito»* (Constituição e lei) mobilizadas pela Administração e das *relações entre ramos jurídico-dogmáticos* (Direito Constitucional e Direito Administrativo, tomado este em sentido estrito, como *ordinary administrative law*)[103].

Do acesso à Constituição pressuposto por esta perspetiva decorrem refrações para o exercício da ação administrativa – entre as quais se destaca justamente a *defesa da Constituição e dos direitos fundamentais através de entidades administra-*

[101] Cf. Fisher/Harding, «The Precautionary Principle and Administrative Constitutionalism: The Development of Frameworks for Applying the Precautionary Principle», in: Fisher/Jones/Schomberg (eds.), *Implementing the Precautionary Principle: Perspectives and Prospectives*, Elgar, Cheltenham/ Northampton, 2006, p. 116. *V.* também Fisher, «Food Safety Crises as Crises in Administrative Constitutionalism», in: *Health Matrix – Journal of Law Medicine*, vol. 20, 2010, pp. 60 e s..

[102] Cf. Fisher, *Risk Regulation and Administrative Constitutionalism*, reimp., Hart Publishing, Oxford/Portland, 2010, p. 37.

[103] No contexto da reflexão sobre o sentido do *administrative constitutionalism*, Fisher (*Risk*..., cit., p. 26) refere-se ainda à "relação simbiótica entre o Direito Administrativo, a Administração Pública e os problemas que a Administração Pública coloca".

tivas independentes[104], conceito amplo (objeto de consagração constitucional no n.º 3 do artigo 267.º da CRP), onde cabem, a par, as entidades com funções de regulação económica e social (autoridades reguladoras) e as entidades vocacionadas para a defesa dos direitos dos cidadãos.

3.2. A importância da tutela de dados pessoais através de uma entidade administrativa independente não constitui propriamente uma inovação. Por um lado, o artigo 28.º da Diretiva 95/46/CE[105] já previa a obrigação, a impender sobre cada Estado-Membro, de estabelecer uma ou mais autoridades públicas responsáveis pela fiscalização da aplicação, no respetivo território, das disposições contantes daquele diploma, esclarecendo que tal(is) autoridade(s) exerceriam *com total independência* as funções que lhe seriam conferidas. O mesmo preceito conferia à autoridade de controlo competência relevantes de natureza consultiva, a que se encontravam ainda associados poderes de inquérito, poderes decisórios de intervenção, poderes de colaboração com as autoridades judiciais perante comportamentos ofensivos dos direitos consagrados pela Diretiva. Por outro lado, a revisão de 1997 veio determinar, no quadro do artigo 35.º,

[104] Que corresponde a um dos cinco domínios ilustrativos do sentido do "resgate" da Lei Fundamental para a Administração Pública, a que nos vimos reportando – cf., por último, o nosso trabalho *Os Direitos Fundamentais e a sua Circunstância: Crise e Vinculação Axiológica entre o Estado, a Comunidade e Sociedade Global, Imprensa da Universidade de Coimbra, Coimbra, 2017,*., pp. 129 e ss. (131 e ss.).

[105] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, in: *JO* L 281, 23.11.1995, pp. 31 e ss..

que a lei (de proteção de dados pessoais) deveria, *inter alia*, garantir a sua proteção, "*designadamente através de entidade administrativa independente*" (cf. artigo 35.º, n.º 2). Finalmente, e regressando ao âmbito europeu, também o n.º 3 do artigo 8.º da *Carta dos Direitos Fundamentais da União Europeia* salientava, como apontámos, que a fiscalização do cumprimento das disposições em matéria de proteção dos dados pessoais se encontraria cometida a uma autoridade independente.

Na sequência destes dispositivos, o legislador criou a (atual) *Comissão Nacional de Proteção de Dados*[106], concebida como autoridade de controlo para efeitos da Diretiva 95/46/CE, configurada como entidade administrativa independente, tendo por missão controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, e sendo dotada de competências de investigação e de inquérito, de autoridade, e de emissão de pareceres.

3.3. O reconhecimento do relevo da tutela administrativa dos dados pessoais volta a ser reconhecido pelo RGPD, que consagra a "autoridade de controlo" como entidade responsável pela fiscalização da aplicação deste diploma e pela sua aplicação coerente no respetivo Estado-Membro, com o propósito último de defender os direitos e liberdades fundamentais relativamente ao tratamento e de facilitar o tratamento desses dados na União (cf. artigo 51.º). A singularidade revestida pela sua conformação normativa torna-a num caso de estudo pela confluência de dimensões que a conformam como entidade vocacionada para a defesa dos direitos dos cidadãos, mas tam-

[106] Cf. artigos 21.º e seguintes da Lei n.º 67/98, de 26 de outubro (alterada pela Lei n.º 103/2015, de 24 de agosto), e Lei n.º 43/2004, de 18 de agosto.

bém que a aproximam de uma autoridade com funções reguladoras. Aliás, uma análise dos diversos dispositivos sobre esta matéria demonstra, com nitidez, que o Regulamento insufla um novo fôlego à atuação da autoridade (nacional) de controlo.

3.3.1. Não persistem dúvidas de que uma das notas características desta entidade se reconduz à independência – uma nota imediatamente concatenada com o imperativo da subordinação direta ao direito. O facto de a esta autoridade funcionar, em certo sentido, como «instância parajurisdicional»[107] demanda que esteja munida de garantias de imparcialidade e sujeita a um regime de incompatibilidades que as aproxima da disciplina jurídica dos tribunais. A independência surge, neste contexto, associada aos imperativos da objetividade, da exclusividade, da transparência, da isenção e da neutralidade[108].

Esta independência manifesta-se quer ao nível orgânico-estrutural, quer no plano funcional. Em termos orgânicos, a independência afeta essencialmente o modo de designação

[107] Qualificando, em atenção a certos poderes, as autoridades administrativas independentes como instâncias parajurisdicionais, *v.* Vital Moreira, *Administração Autónoma e Associações Públicas*, Almedina, Coimbra, 1997, p. 135, n. 171.

[108] Sobre estas dimensões, enquanto corolários do princípio da imparcialidade, cf. Maria Teresa Ribeiro, *O Princípio da Imparcialidade da Administração Pública*, Almedina, Coimbra, 1996, pp. 161 e ss..

Sobre a neutralidade como critério caracterizador das autoridades reguladoras independentes, cf. Vital Moreira/Fernanda Maçãs, *Autoridades Reguladoras Independentes – Estudo e Projecto de Lei-Quadro*, Coimbra Editora, Coimbra, 2003, pp. 29 e s.. *V.* ainda, sobre as várias dimensões desta neutralidade, Blanco de Morais, «As Autoridades Administrativas Independentes na Ordem Jurídica Portuguesa», in: *Revista da Ordem dos Advogados*, n.º 1, ano 61.º, janeiro 2001, pp. 118 e s..

dos titulares dos órgãos ou o regime jurídico dos respetivos mandatos: assim, *v. g.*, o RGPD estabelece o impedimento do exercício de qualquer atividade (pública ou privada), remunerada ou não, que seja incompatível com o desempenho das suas funções (artigo 52.º); por sua vez, a estabilidade constitui uma característica do mandato dos membros, que não poderá ser inferior a quatro anos [cf. artigo 54.º, n.º 1, alínea *d)*]; também a nomeação (mesmo que efetuada por um órgão de soberania) deve ser realizada através de um procedimento transparente (cf. artigo 53.º, n.º 1).

É, todavia, a vertente funcional da independência, que mais releva neste domínio, pois que a atividade desta entidade está isenta da subordinação a qualquer poder de direção ou orientação do Governo, não competindo, de igual modo, à Administração estadual o respetivo controlo ou fiscalização. A única exceção admitida a esse controlo respeita a matéria financeira e, mesmo assim, tal fiscalização não pode afetar a independência da autoridade, que disporá de orçamentos separados e públicos, podendo estar integrados no orçamento geral do Estado (cf. artigo 52.º, n.º 6).

Apesar (ou justamente por causa) da sua independência em face de quaisquer influências externas – incluindo do Governo (e, por conseguinte, das maiorias eleitorais) –, não solicitando, nem recebendo instruções de outrem (cf. artigo 52.º, n.º 2), esta autoridade não se encontra, como se afigurará evidente, imune ao controlo jurisdicional, sendo todas as suas ações e omissões suscetíveis de apreciação pelos tribunais, que têm competência para avaliar da respetiva juridicidade (cf. artigo 78.º).

3.3.2. A natureza das tarefas confiada a esta entidade apresenta um caráter acentuadamente polimórfico, com destaque para o desempenho de funções de normação (ou paranormativas), de resolução de litígios e de aplicação de sanções, numa clara miscigenação (mas não confusão) entre função legislativa, função administrativa e função judicial. Esta mesma ideia ressalta do artigo 58.º do RGPD que elenca quais os poderes da autoridade de controlo, categorizando-os em três grupos: poderes de investigação; poderes de correção e sanção; e poderes consultivos e de autorização. Repare-se que a esta autoridade se encontram conferidas competências normativas (e paranormativas) relevantíssimas (como sucede com a aprovação das regras vinculativas aplicáveis às empresas previstas no artigo 47.º), ou competências típicas de execução administrativa (como as autorizações administrativas de tratamento de dados), ou ainda competências parajurisdicionais (como se verifica, paradigmaticamente, quer com a aplicação das sanções administrativas, quer com as decisões das reclamações ou queixas apresentadas pelos titulares dos dados). Seguindo um figurino próximo do que encontramos em muitas entidades reguladoras, o Regulamento não prevê um elenco fechado de funções, optando pela inclusão de uma cláusula aberta que atribui à autoridade de controlo os poderes para "desempenhar quaisquer outras tarefas relacionadas com a proteção de dados pessoais" [cf. artigo 57.º, n.º 1, alínea *v)*], viabilizando ainda que os Estados-Membros lhes cometam competências para além das que se encontram expressamente previstas (cf. artigo 58.º, n.º 6).

3.3.3. O âmbito e o alcance das competências conferidas a esta entidade e, sobretudo, a forma genérica como se lhe encontram cometidos poderes para o desempenho de quaisquer tarefas relacionadas com a proteção de dados pessoais, revelam a amplitude da discricionariedade de que a autoridade de controlo goza – muito próximas do que se designa como "discricionariedade regulatória"[109], *hoc sensu*, beneficiando de uma liberdade de conformação e de prerrogativas de avaliação, em contextos de risco, caracterizados pela necessidade de realização de juízos técnicos ou de prognose[110].

Como se sabe, porém, uma decisão administrativa nunca é totalmente discricionária, na medida em que está sempre sujeita a vinculações jurídicas. Sem prejuízo de o alcance da atribuição legislativa de poderes discricionários variar em função das normas legais habilitantes da ação administrativa, bem como dos limites resultantes de outras prescrições legislativas que incidam sobre a matéria em causa[111], não se pode olvidar

[109] Sobre esta matéria, *v.* também as considerações que tecemos em «A Discricionariedade Administrativa: Reflexões a partir da Pluridimensionalidade da Função Administrativa», in: *O Direito*, n.º III, ano 144.º, 2012, pp. 641 e ss..

[110] *V.* Attendorn, «Das "Regulierungsermessen" – Ein Deutscher "Sonderweg" bei der Gerichtlichen Kontrolle TK-rechtlicher Regulierungsentscheidungen?», in: *Multimedia und Recht*, 2009, p. 238; Schmidt-Assmann, *Das Allgemeine Verwaltungsrecht als Ordnungsidee*, 2.ª ed., Springer, Berlin/Heidelberg, 2006, p. 141.

A amplitude desta discricionariedade regulatória e a deferência jurisdicional não deixam de se revelar preocupantes, podendo estar na base, segundo alguns, do aumento da corrupção e da economia paralela – assim, Johnson/Kaufmann/Zoido-Lobatón, «Regulatory Discretion and the Unofficial Economy», in: *The American Economic Review*, fasc. 2, vol. 88, maio 1998, pp. 387 e ss..

[111] Sachs («§ 40 Ermessen», in: Stelkens/Bonk/Sachs, *Verwaltungsverfahrensgesetz*, 9.ª ed., Beck, München, 2018, n.ºs de margem 74 e ss.) distingue precisamente entre os limites decorrentes da lei habilitante (*Grenzen aus*

que a subordinação a critérios jurídicos possui uma intensidade *mínima*: a exigida pelos princípios normativos. Eis o motivo pelo qual a submissão da atividade administrativa aos princípios assume uma relevância fundamental nos casos em que os poderes discricionários também se revestem de maior alcance.

Esta mesma ideia não passou despercebida ao RGPD. Com efeito, o exercício dos poderes da autoridade de controlo encontra-se, expressamente, submetido à observância de relevantes princípios. O Regulamento destaca, em especial:

a) O princípio da proporcionalidade e da razoabilidade das medidas adotadas;

b) O princípio do procedimento justo, demandando-se o respeito pelas garantias de audiência e contraditório, imparcialidade e decisão em prazo razoável;

c) O princípio da transparência, desde logo, no que respeita à exteriorização das medidas juridicamente vinculativas, onde avultam as exigências relativas à clareza e inequivocidade das mesmas, bem como à necessidade de incluir no respetivo texto a autoridade de controlo que as emitiu, a data da decisão, a fundamentação da medida e o direito de impugnação;

d) O princípio da cooperação (entre as autoridades de controlo dos diferentes Estados-Membros) e da racionalização, especialmente visível no âmbito do controlo das atividades de tratamento transfronteiriço ou que envolva cidadãos de mais do que um Estado-Membro

dem ermächtigenden Gesetz) e os limites emergentes de outras leis incidentes sobre a matéria (*Grenzen aus sonstigen Gesetzen*).

da União Europeia. A ideia de cooperação encontra-se traduzida num sistema de balcão único e na identificação de uma "autoridade de controlo principal" (a qual não impede que outras autoridades de controlo – as autoridades de controlo interessadas – intervenham nas questões: eis o que sucederá quando, por exemplo, pessoas residentes fora da jurisdição da autoridade principal sejam substancialmente afetadas por uma atividade de tratamento de dados). Quer dizer, e sem prejuízo da intervenção das autoridades de controlo interessadas (mas em conjugação com elas), cabe à autoridade de controlo principal a responsabilidade fundamental gerir a atividade de tratamento transfronteiriço de dados: assim, por exemplo, quando um titular de dados apresenta uma queixa relativa ao tratamento dos seus dados pessoais, a autoridade de controlo principal coordenará as eventuais investigações, com a participação de outras autoridades de controlo «interessadas».

O mesmo empenho com a cooperação volta a surgir no capítulo VII, precisamente com a epígrafe: cooperação e coerência (cf. artigos 60.º e seguintes). Além das questões associadas ao sistema de controlo do tratamento transfronteiriço, assoma agora com especial relevância o propósito de assegurar uma aplicação coerente do Regulamento, que se pretende garantir através da consagração de um dever de assistência mútua, da realização de operações conjuntas das autoridades de controlo, ou da criação do procedimento de controlo da coerência que envolve conjugadamente as autoridades de controlo dos Estados-membros e a própria Comissão

Europeia (e com impacto em aspetos tão determinantes como a determinação de cláusulas-tipo de proteção de dados, ou de aprovação de critérios de acreditação).

3.3.4. A análise das normas atinentes à autoridade de controlo, acompanhada da sua conjugação com o resto do diploma, desvelam certos traços do modelo regulatório (público e independente) que o legislador europeu pretende implementar no âmbito da proteção de dados pessoais, e que poderemos sintetizar em quatro pontos: preferência pela autorregulação, coordenação, regulação responsiva, e meta-regulação.

a) Por um lado, denota uma clara preferência pelas formas de *autorregulação*. É à luz desta ideia que se deverá interpretar a previsão de um "encarregado da proteção de dados" (cf. artigos 37.º e seguintes). Embora esta figura não constasse da anterior diretiva, já se havia desenvolvido alguma prática neste sentido. O RGPD vem prever a designação obrigatória de um encarregado de proteção de dados em três situações específicas: quando o tratamento seja efetuado por uma autoridade ou um organismo público; quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou quando as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações. Pelo

menos ao abrigo dos dois últimos critérios, poderemos incluir aqui as seguradoras, especialmente na parte em que celebram contratos de seguro de pessoas, que pressupõem, na maioria dos casos, o tratamento maciço de dados relativos à saúde.

A previsão de casos obrigatórios de designação de um encarregado de proteção de dados não impede a sua designação a título voluntário que é, aliás, encorajada pelos vários organismos europeus de reflexão sobre esta matéria.

O encarregado da proteção de dados assume um papel demiúrgico entre as autoridades de controlo, os titulares dos dados e as empresas e responsáveis pelo tratamento de dados. Neste sentido, o artigo 39.º do Regulamento comete-lhe funções que passam pela informação e aconselhamento do responsável pelo tratamento (ou o subcontratante) e dos trabalhadores que tratam os dados, pelo controlo de qualidade do tratamento de dados, tendo por referência o quadro jurídico aplicável e as políticas do responsável quanto à proteção de dados pessoais, pela intervenção no âmbito da avaliação de impacto, pela cooperação e articulação com a autoridade de controlo.

b) Por outro lado, a autoridade de controlo apresenta-se como uma entidade coadjuvante das empresas no que se refere à promoção de boas práticas no âmbito recolha e tratamento de dados pessoais, viabilizando,

em certo sentido, a *coordenação* entre regulação pública e os comportamentos dos regulados. Incluem-se neste horizonte as atuações da autoridade de controlo dirigidas a incentivar a elaboração de códigos de conduta destinados a contribuir para a aplicação do Regulamento (cf. artigo 40.º) ou a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados (cf. artigo 42.º)[112];

c) Além disso, a forma de exercício dos poderes mais gravosos surge como solução de *ultima ratio* para reação contra o incumprimento das obrigações impostas pelo Regulamento. Destarte, poder-se-á afirmar que a estratégia regulatória de proteção de dados se desenvolverá à luz das ideias da *responsive regulation*[113], em

[112] O procedimento de exame deverá ser utilizado para a adoção de atos de execução em matéria de cláusulas contratuais-tipo entre os responsáveis pelo tratamento e os subcontratantes e entre subcontratantes; códigos de conduta; normas técnicas e procedimentos de certificação; nível de proteção adequado conferido por um país terceiro, um território ou um setor específico nesse país terceiro ou uma organização internacional; cláusulas normalizadas de proteção; formatos e procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas aplicáveis às empresas; assistência mútua; e regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité.

[113] Cf o estudo clássico de Ayres/Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, Oxford/New York, 1992. Cf. também Braithwaite, *Restorative Justice and Responsive Regulation*, Oxford University Press, Oxford, 2002.

que a persuasão deverá atuar como estratégia de primeira linha, pelo que, somente se esta não funcionar, se recorrerá ao exercício de poderes sancionatórios[114]. Se se reconhece que devem ser atribuídos poderes fortes às agências, também se entende que estas devem usá-los moderadamente, privilegiando o recurso a instrumentos de *soft law* (como sucede, *v. g.*, com as advertências ao responsável pelo tratamento no sentido de que as operações são suscetíveis de violar o Regulamento, as quais podem ir subindo de tom, passando a repreensões em caso de efetiva violação do diploma).

A simples ameaça – que paira sobre os regulados – de que o regulador pode adotar decisões devastadoras (como a imposição temporária ou definitiva do tratamento de dados, ou mesmo a sua proibição, ou ainda a retirada da certificação emitida, ou também, de forma isolada ou em conjunto com as anteriores, a imposição de uma

Já em momentos anteriores, propendêramos para a defesa deste modelo: *v.* o nosso trabalho «A Crise e a Regulação: O Futuro da Regulação Administrativa», in: Pedro Gonçalves/Carla Amado Gomes/Helena Melo/Filipa Calvão (org.), *A Crise e o Direito Público*, ICJP | Faculdade de Direito da Universidade de Lisboa, Lisboa, 2013, pp. 108 e ss..

[114] Quer dizer, a intensidade e a utilização dos poderes reguladores variarão consoante os riscos que os regulados impliquem para o alcance das finalidades regulatórias, admitindo-se o recurso estratégias proativas (persuasivas) ou reativas (sancionatórias) em função daqueles riscos (cf. Baldwin/Black, «Really Responsive Regulation», in: *The Modern Law Review*, fasc. 1, vol. 71, 2008, p. 66). A questão agora consiste em saber quando persuadir ou quando punir – cf. já Braithwaite, *To Punish or Persuade*, State University of New York Press, Albany, 1985, pp. 75 e ss., e *Restorative Justice and Responsive Regulation*, Oxford University Press, Oxford/New York, 2002, p. 29; Ayres/Braithwaite, *Responsive Regulation*..., cit., pp. 21 e ss..

coima) funcionará como uma *benign big gun*[115] e poderá, com frequência, inibir a prática de infrações, favorecendo que os comportamentos das empresas se conformem com os objetivos da política regulatória, talqualmente os mesmos se lhes apresentam através de instrumentos de persuasão. Neste horizonte aproximamo-nos da ideia de *smarter regulation*, no sentido em que desvaloriza uma regulação do tipo *command-and-control* (pelo menos, em exclusivo) e mostra-se favorável à utilização de mecanismos informais de persuasão dos operadores económicos[116] – persuadindo-os a cumprir.

[115] Ayres/Braithwaite, *Responsive Regulation*..., cit., pp. 19 e ss., esp.te pp. 40 e ss..

[116] Esta conceção do sentido e do alcance dos poderes reguladores encontra acolhimento na perspetiva defendida por alguma doutrina, segundo a qual a missão de regular se encontra na confluência das duas tendências que caracterizam a própria evolução do Direito Administrativo em geral: por um lado, e à semelhança de uma *red light theory*, a atribuição de poderes sancionatórios às agências implica que a sua atuação assuma uma feição restritiva, orientada para a tutela da legalidade e para a eliminação/repressão dos comportamentos (não da Administração, mas agora) dos operadores económicos que contrariem o direito vigente e a satisfação dos objetivos de política regulatória que lhe estão subjacentes; por outro lado, o reconhecimento de que a primeira linha de ação das entidades reguladoras se reconduz à persuasão sobre os regulados significa que o propósito do exercício dos poderes reguladores consiste em implementar uma certa política regulatória, talqualmente surge pressuposto pela *green light theory*. Cf. Baldwin/Cave/Lodge, *Understanding Regulation*, Oxford University Press, Oxford, 2012, p. 3. Sobre as *red light, green light and amber light theories*, *v.* Harlow/Rawlings, *Law and Administration*, 3.ª ed., Cambridge University Press, Cambridge, 2009, pp. 1 e ss.; cf. também a síntese de Stott/Felix, *Principles of Administrative Law*, Cavendish, London, 1997, pp. 29 e ss..

d) O Regulamento aponta, por fim, para o estabelecimento de novos níveis regulatórios em matéria de proteção de dados. A *meta-regulação* pressupõe, pois, a criação de mecanismos destinados a regular o estabelecimento e a utilização dos instrumentos regulatórios[117]. Como se sabe, este regime passa pela criação (ou reforço dos poderes) de organismos que controlam a criação e a implementação das políticas regulatórias, pela definição de critérios para o exercício da atividade regulatória, e, articuladamente, pela introdução da ideia de éti-

[117] Entre outras, esta nota distingue a *meta-regulation* da *regulatory review* presidencial existente nos Estados Unidos desde o *Paperwork Reduction Act*, de 1980 (cf., em especial, § 3503, na redação de 1995), embora com antecedentes na Administração Nixon: na sequência de críticas quanto à qualidade da regulação e à emergência de um «quarto poder acéfalo» (na formulação da Comissão Brownlow), aquele ato legislativo criou, no interior do *Office of Managemente and Budget* (e, por conseguinte, integrado no gabinete do presidente), o *Office of Information and Regulatory Affairs* (OIRA) – um sistema que posteriores *Executive Orders* (sobretudo das eras Reagan, Clinton, Bush e Obama) vieram intensificar e aperfeiçoar. Embora se possa afirmar que, em ambos os casos está em causa a supervisão da atividade regulatória, a *regulatory review* constitui um mecanismo que, além de não ter (evidentemente, por força do princípio da separação de poderes) repercussões no plano legislativo (e, por conseguinte, se circunscrever à análise da atuação – sobretudo, normativa – dos reguladores), pretende estender os poderes de influência do Presidente sobre as agências reguladoras, contribuindo para a centralização presidencial, com particulares repercussões no que tange à coordenação e à unidade na execução ou implementação das políticas públicas. Os problemas emergem, como sublinha alguma doutrina, quando a intensidade do controlo presidencial é tão forte que compromete o próprio sistema de *checks and balances* (assim, Boggart, «Presidential Control Over Agencies: When Does Enough Become Too Much?», in: *Journal of Land, Resources & Environmental Law*, vol. 29, 2009, pp. 399 e ss., esp.te pp. 409 e ss.).

ca, enquanto condição da legitimidade da ação pública de regulação, que concebe as pessoas como parte de um procedimento mais transparente de delineação das medidas regulatórias e leva a ter em conta o impacto destas últimas nos interesses do cidadão. É com base nesta ideia que o Regulamento configura o Comité Europeu para a Proteção de Dados (artigos 68.º e seguintes). Ainda que a sua atividade assuma natureza predominantemente consultiva e seja exteriorizada, sobretudo, através de instrumentos de *soft law*, não deixa de se revelar interessante que aquela entidade assuma a importante função de controlar e assegurar a aplicação do Regulamento.

4. O novo regime jurídico da proteção de dados apresenta desafios determinantes para o reforço da importância da tutela administrativa dos direitos dos cidadãos. E tal sucede por se pautar pela necessidade de um equilíbrio dos poderes reguladores e na sua compreensão como poderes dirigidos, em último termo, à realização dos interesses públicos primários no quadro do Direito. Se este Regulamento impõe deveres importantes a cargo das empresas e pressupõe a existência de cidadãos cientes dos seus direitos, também não demite as administrações públicas dos Estados-membros de, através da autoridade de controlo, contribuir quer para a promoção de boas práticas, quer para o efetivo *enforcement* dos instrumentos de proteção de dados pessoais.

DATA CONTROLLERS E DATA PROCESSORS: DA RESPONSABILIDADE PELO TRATAMENTO DE DADOS À RESPONSABILIDADE CIVIL

Mafalda Miranda Barbosa

1. Introdução

A proteção de dados está na ordem do dia, não só pelos específicos problemas que em torno dela eclodem, fruto de ambientes cada vez mais complexos de recolha e partilha de informações[1], como pela necessidade de dar cumprimento ao Regulamento (UE) 2016/679, relativo à proteção de dados

[1] Cf. Jorge Miranda/Rui de Medeiros, *Constituição Portuguesa Anotada*, tomo I, Coimbra Editora, Coimbra, 2005, artigo 35.º, 379-380, referindo que "a necessidade de tutela do indivíduo relativamente ao uso da informática faz-se sentir cada vez com mais premência tendo em conta as possibilidades de recolha e de armazenamento de informação relativa aos cidadãos por parte de terceiros e dos próprios poderes públicos, e a facilidade e a velocidade de acesso e de cruzamento de todos esses dados".

Veja-se, igualmente, J. Seabra Lopes, "A proteção da privacidade e dos dados pessoais na sociedade de informação", *Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa*, UCP, 2002, 779 s.; Alexandre de Sousa Pinheiro, "A proteção de dados na proposta de regulamento comunitário apresentado pela Comissão Europeia: primeiras reflexões", *Direito e Política*, n.º1, 2012, 9 s.;

pessoais. Este foi pensado quer no sentido do reforço dos direitos dos titulares dos dados pessoais, quer no sentido da harmonização de um elevado nível de proteção em todo o espaço europeu, atenta a possibilidade e a velocidade de circulação dos dados pessoais entre diversos Estados.

Tal como já acontecia com a anterior legislação europeia na matéria, confrontamo-nos novamente com as noções de *data controller* (responsável pelo tratamento de dados) e *data processor* (subcontratante). Assumindo-se como peças centrais da regulamentação relativa aos dados pessoais, o responsável e o subcontratante oferecem-nos o desenho das relações que se estabelecem ou podem estabelecer entre aqueles que controlam ou executam uma operação de tratamento de dados, ao mesmo tempo que nos dotam de critérios de determinação do responsável em caso de violação do direito à proteção de dados pessoais. Lidamos, assim, com duas noções distintas de responsabilidade, a fazer rememorar, neste quadro, a lição de Honoré[2], que, apresentando uma taxonomia das diversas aceções de responsabilidade, fala, entre outras, da *role responsibility* e da *liability*.

Se o conceito de responsável pelo tratamento de dados nos remete para uma ideia de responsabilidade enquanto assunção de um especial encargo, a implicar especiais deveres, que visam a salvaguarda dos dados pessoais alheios; o referido responsável pelo tratamento de dados pode tornar-se responsável, no sentido da *liability*, em caso de violação de algum ou

Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*, AAFDL, Lisboa, 2015, 427.

[2] Cf., para uma adequada compreensão dos diversos sentidos com que pode ser assumido o termo responsabilidade, H.L.A. HART, *Punishment and Responsability, Essays in the Philosophy of Law*, Oxford University Press, 1968, 210 s. Apresentam-se, aí, quatro sentidos para o termo *responsability*. A *role -responsability,* indicando que, se uma pessoa está investida num determinado cargo, lugar, estatuto, papel, fica adstrita a especiais deveres, alguns dos quais se prendem com a promoção do bem-estar dos outros ou a prossecução dos objetivos de uma dada organização; a *causal-responsability*, em cuja aceção o responsável se vem a identificar com o causador de um ato, pelo que não só os humanos, mas também as coisas, os animais ou os fenómenos não humanos podem ser considerados responsáveis (cf. p. 214); a *liability responsability*, que, ao contrário do sentido prévio, implica já uma assunção acerca do mérito da conduta, afastando-se do mecanicismo característico da visão da responsabilidade/causalidade, a implicar a responsabilidade como o desencadear de um efeito na realidade, tanto mais que a pessoa pode ser responsabilizada, neste sentido, pelos atos praticados por terceiros; a *capacity responsability,* intrinsecamente ligada à anterior, na medida em que a responsabilização do agente implica a existência de determinadas faculdades mentais e psicológicas sem as quais ele não se autodetermina, pelo que, em última instância, denotamos já o apelo a um dado sentido de liberdade sem a qual a primeira não pode ser tematizada (cf. p. 226-227). Cf., ainda, sobre os vários sentidos do termo *responsibility,* H. L. A. HART, "Varieties of responsibility", *Law Quarterly Review*, 83, 1967, 346. No artigo citado, o autor apresenta a taxonomia referida. No que respeita, por exemplo, à *role responsibility*, salienta a dificuldade, por vezes sentida na apreciação do caso concreto, de determinação dos concretos deveres que oneram o sujeito em virtude da posição em que está investido. Acresce que inclui no conceito todas as obrigações que impendem sobre a pessoa como decorrência de um particular acordo firmado, entrando em considerações atinentes ao mundo contratual, tendo, não obstante, a cautela de, num esforço de compartimentação categorial, alertar que a assunção feita do termo responsabilidade não é confundível com aqueloutra de dever específico. A separá-los a consciência da complexidade e extensão da primeira, a implicar a conformação de uma *sphere of responsibility, requiring the exercise of discretion and care usually over a protracted period of time*. (cf. p. 347). Também, aí, claramente refere a interdependência entre os diversos sentidos da responsabilidade. Atendo-se ao direito já constituído, o autor considera que a *liability* está muitas vezes dependente da *causal responsibility* ou da *capacity responsibility.*

alguns desses deveres. Fazendo-nos situar a montante ou a jusante do processo de tratamento de dados, as duas responsabilidades com que assim lidamos — responsabilidade pelo tratamento de dados e responsabilidade civil pela violação de dados pessoais — não deixam de apresentar entre si uma linha de continuidade, já que é a responsabilidade pelo tratamento de dados que, ao desenhar uma esfera de controlo associada a especiais deveres de cuidado que têm de ser assumidos, nos permite, *a posteriori,* determinar quem é o civilmente responsável.

Não se estranha, por isso, que o grupo de trabalho do artigo 29.º sobre a proteção de dados[3], ainda por referência à Diretiva 95/46/CE, venha sustentar que o conceito de responsável pelo tratamento de dados é um conceito funcional, que visa atribuir responsabilidades àqueles que exercem uma influência de facto sobre os dados pessoais alheios. Numa outra formulação, lê-se no documento que todas as disposições que estabelecem condições para o tratamento lícito dos dados têm como destinatário o *controller*, sendo, por isso, ele o responsável pelos prejuízos sofridos devido ao tratamento ilícito dos dados, o que implica que a principal função do conceito seja a atribuição de responsabilidade[4].

[3] Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, Fevereiro de 2010, 13 s.

[4] Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 7 s.

De notar, desde já, que o novo Regulamento Geral de Proteção de Dados vem considerar que os subcontratantes podem também ser responsabilizados em determinadas circunstâncias.

Em termos gerais, a conexão que assim se estabelece não é perturbadora. Diríamos, pelo contrário, que ela resulta clara em qualquer esquema de imputação. Na verdade, do ponto de vista delitual, porque o homem se concebe como pessoa, a responsabilidade que possa avultar, pela lesão, em regra culposa, de um direito ou de um interesse protegido através de uma disposição legal de proteção de interesses alheios, resulta da convolação de uma primitiva esfera de responsabilidade *pelo outro* numa esfera de responsabilidade *perante o outro*, sendo os deveres do tráfego que integram a primeira o que nos oferece o embrião da imputação objetiva que se há-de estabelecer. Do ponto de vista contratual, embora com uma finalidade diversa e um fundamento axiológico também diferente, a compreensão de uma esfera de risco/responsabilidade — agora emergente da própria vinculação negocial — não nos fará andar muito longe destas ideias.

A novidade que o Regulamento Geral de Proteção de Dados nos oferece é a concretização, pelos deveres que estabelece e pela identificação dos obrigados por tais deveres, da referida *role responsibility*. Contudo, isto não nos resolve todos os problemas. De facto, não basta pensar numa esfera de responsabilidade a montante para que a imputação — e, portanto, a responsabilidade civil, a jusante — se possa afirmar, tanto mais que, neste âmbito, ela se define em abstrato pelo legislador. Assim, haveremos de analisar em que medida a lesão que ocorre se liga funcionalmente ao dever preterido, para o que teremos de confrontar a esfera de responsabilidade do *controller* com outras esferas de responsabilidade. É por isso que se torna particularmente importante — ou mesmo imprescindível — compreender as relações que se podem estabelecer entre o responsável pelo tratamento de dados e outros responsáveis pelo

tratamento de dados ou entre o responsável pelo tratamento de dados e os subcontratantes. Do mesmo modo que é essencial contemplar, a este nível, os eventuais comportamentos de terceiros que possam surgir.

Nas páginas que se seguem, procuraremos refletir um pouco sobre a responsabilidade civil do responsável pelo tratamento de dados, para o que haveremos de analisar o conceito de *contollers na sua relação com os processors*. Antes, porém, teceremos algumas considerações quer acerca do desenho genérico oferecido pelo Regulamento para a proteção de dados pessoais, quer acerca das possíveis modalidades de responsabilidade civil que podem, em abstrato, assimilar o âmbito de relevância das hipóteses suscetíveis de emergir em concreto.

2. A proteção de dados pessoais à luz do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril de 2016: traçado genérico

O Regulamento 2016/679, do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, não altera a intencionalidade da disciplina legal em vigor até então, mas reforça alguns dos direitos dos titulares dos dados e torna mais rigorosos alguns procedimentos. Além disso, parece alterar a relação de forças entre a recolha e tratamento de dados consentidos pelo titular e as outras finalidades de tratamento. Na verdade, enquanto ao nível da lei n.º67/98 a regra era a do tratamento de dados com base no consentimento do titular dos mesmos, embora houvesse a previsão de situações em que dele se podia prescindir, nos termos do Regulamento (EU) 2016/679, entre as condições

de licitude do tratamento de dados, o consentimento do titular surge na mesma posição que os restantes fundamentos.

Importa, por isso, acompanhar algumas (mas não todas) das alterações introduzidas à tutela dos dados pessoais pelo referido regulamento.

Desde logo, é o conceito de dados pessoais que parece sofrer uma ampliação. Se, nos termos da al. a) do artigo 3.º da Lei n.º 67/98, eram definidos como qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável, sendo considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social, o artigo 4.º/1 RGPD vem considerar dados pessoais toda a informação relativa a uma pessoa singular identificada ou identificável, sendo considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. Não obstante a diversa formulação, cremos que a ampliação da noção não é senão aparente. De facto, a falta de referência aos dados de localização ou identificadores por via eletrónica, bem como aos elementos da identidade genética não condena à sua exclusão do âmbito de relevância da lei n.º 67/98. Aliás, o TJUE, no acórdão de 19 de Outubro de 2016 (Proc. C-582/14), em atenção à Diretiva 95/46/CE, do Parlamento

Europeu e do Conselho, que a Lei n.º 67/98 vem transpor para o ordenamento jurídico interno (devendo, por isso, ser interpretada de acordo com o direito comunitário), considera que o endereço de protocolo internet dinâmico (IP) é um dado pessoal. De outro modo não poderia, aliás, deixar de ser, atenta a intencionalidade predicativa da disciplina, vertida não só na noção de dado pessoal, como nos princípios norteadores do tratamento de dados.

Estes estão, agora, especificados no artigo 5.º Regulamento. De certo modo, reproduzem o que já estava anteriormente consagrado. O tratamento de dados pessoais deve ser feito de forma lícita, transparente e de acordo com o princípio da boa-fé. Acrescenta-se, relativamente ao artigo 5.º/1 a) Lei n.º67/98, a transparência, sem que, contudo, isso signifique que ela estivesse ausente do regime legal. Além disso, os dados apenas podem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades. Quer isto dizer que o artigo 5.º/1 b) RGPD reproduz o conteúdo do artigo 5.º/1 b) Lei n.º 67/98, esclarecendo, contudo, que o tratamento posterior para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos não é considerado incompatível com as finalidades iniciais. Consagra-se, igualmente, o princípio da minimização de dados, isto é, estes devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados, em absoluta correspondência com o artigo 5.º/1 c) Lei n.º67/98; o princípio da exatidão (os dados pessoais devem ser exatos e atualizados sempre que necessário, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora), em sintonia com o artigo 5.º/1 d) Lei n.º67/98; o princípio da limitação da conservação (os dados pessoais devem ser conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados), que reproduz sensivelmente a solução consagrada no artigo 5.º/1 e) Lei n.º67/98, embora se esclareça, agora, que os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos; e o princípio da integridade e confidencialidade. Quanto a este último, ausente do elenco de condições a que devem obedecer os dados pessoais de acordo com a Lei n.º67/98, significa que os referidos dados devem ser tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas. Não obstante a referida omissão, importa considerar que ele já se extrairia de uma análise sistemática do regime legal em vigor em Portugal.

Tal como sob a vigência da Lei n.º 67/98, de acordo com o RGPD, o tratamento de dados pessoais só é lícito se existir consentimento do seu titular ou, em alternativa, se se verificar uma das seguintes situações: se o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; se o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; se o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; se o tratamento for necessário ao exercício de funções de

interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; se o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Apesar da similitude de formulações, há, como referido anteriormente, algumas diferenças a assinalar. Assim, e mesmo sem nos referirmos a condições de licitude não especificadas na Lei n.º67/98 e consagradas no Regulamento, deixa de se partir do princípio do consentimento para colocar em pé de igualdade as situações em que o tratamento de dados é feito com base nele ou com base nas outras circunstâncias ali especificadas. Há, também, a relevar as alterações ao nível do próprio consentimento, que passa a ter de obedecer, pelo menos aparentemente, a condições mais estritas de obtenção.

O consentimento tem de ser prestado livremente[5] e tem de ser esclarecido. Daí que o titular dos dados tenha direito à

[5] Cf. o artigo 7.º/4 Regulamento, nos termos do qual "o avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato".

A propósito do caráter livre do consentimento, importa considerar que o Regulamento estabelece regras atinentes ao consentimento por menores. Dispõe o artigo 8.º que "quando for aplicável o artigo 6.º/1 a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais

prestação de uma série de informações, por parte do responsável, que lhe permitam compreender a natureza e o alcance do ato, bem como lhe permitam, posteriormente, acompanhar o tratamento que deles seja feito. No mais, o consentimento tem de ser específico, isto é, orientado para as finalidades a que o responsável se propõe, nos termos dos artigos 12.º e seguintes do Regulamento. De notar, porém, que o direito à informação de que se cura tem um âmbito e uma intencionalidade mais vastas do que de mero instrumento de esclarecimento conducente à licitude do consentimento. Por um lado, ele continua a existir, quando o tratamento dos dados se baseie noutros fundamentos que não essa autorização do titular; por outro lado, ele revela-se essencial para que o titular dos dados pessoais possa acompanhar o tratamento que deles seja feito. Parece, aliás, ser esta a *ratio* do direito à informação a que se refere o artigo 15.º Regulamento e que surge associado ao direito de acesso do titular dos dados. Tal direito de acesso é subsequente à recolha dos dados.

De notar, ainda, que a concretização do direito à informação, tal como acontecia no âmbito da lei n.º67/98, vai ser diverso consoante os dados tenham sido recolhidos diretamente junto do seu titular ou não. É esta a solução que decorre dos artigos 13.º e 14.º RGPD.

O consentimento é livremente revogável a todo o tempo. O artigo 7.º/3 RGPD especifica que "o titular dos dados tem o di-

da criança". A esta solução já seria possível chegar com base nas regras próprias do ordenamento jurídico português. Para tanto seria, no entanto, necessário perscrutar a natureza do direito à proteção de dados.

Refira-se que os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos.

reito de retirar o seu consentimento a qualquer momento", embora a retirada do consentimento não comprometa a licitude do tratamento efetuado com base no consentimento previamente dado. Esta ideia é concretizada por via da consagração do direito ao esquecimento, embora a intencionalidade deste ultrapasse as hipóteses de mera revogação do consentimento. Nos termos do artigo 17.º RGPD, o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando tais dados deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento; quando o titular retire o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º/1 a) ou do artigo 9.º/2 a) e se não existir outro fundamento jurídico para o referido tratamento; quando o titular se oponha ao tratamento nos termos do artigo 21.º/1, e não existam interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular se oponha ao tratamento nos termos do artigo 21.º/2; quando os dados pessoais foram tratados ilicitamente; quando os dados pessoais tiverem de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito; quando os dados pessoais tiverem sido recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º/1. Este direito ao esquecimento apresenta determinados limites. Designadamente, ele não poderá ser exercido quando o tratamento se revele necessário ao exercício da liberdade de expressão e de informação; ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito; ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento; quando haja motivos de interesse público no domínio da saúde pública; quando estejam envolvidos arquivos de interesse público, fins de investigação científica ou histórica ou fins estatísticos, e o direito ao esquecimento tornasse impossível ou prejudicasse gravemente a obtenção dos objetivos desse tratamento; ou quando esteja em causa o exercício de um direito num processo judicial.

Para além do direito ao esquecimento, o titular dos dados tem também direito, nos termos do artigo 16.º, a obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito ou que os dados incompletos sejam completados; nos termos do artigo 18.º, a obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma hipóteses previstas no preceito (direito de limitação); nos termos do artigo 20.º, a receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e 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, desde que o tratamento se baseie no consentimento ou num contrato e desde que o tratamento seja realizado por meios automatizados (direito de portabilidade); nos termos do artigo 21.º, a opor-se, a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais feito de acordo com o artigo 6.º/1/ e) ou f), ou no artigo 6.º/4. Neste caso, o responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados.

O regulamento vem, igualmente, reforçar alguns dos deveres que recaem sobre os responsáveis (*controllers*) pelo tratamento dos dados, incrementando a segurança na matéria. Estes deveres são extensíveis aos subcontratantes (*processors*) e aplicam-se mesmo que estes sujeitos estejam sediados fora da União Europeia. Fundamental é que os dados incidam sobre titulares europeus.

O reforço da segurança passa, a este nível, *inter alia,* também, pela aplicação, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, de medidas técnicas e organizativas adequadas, como a pseudonimização, a garantir a eficácia dos princípios da proteção de dados, nos termos do artigo 25.º/1 RGPD. De acordo com o n.º2 do mesmo artigo 25.º "o responsável pelo tratamento aplica, ainda, as medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares". Outras medidas técnicas e organizativas estão previstas no artigo 32.º Regulamento.

Havendo mais do que um responsável pelo tratamento dos dados, ambos determinam, por acordo entre si e de modo transparente, as respetivas responsabilidades pelo cumprimento das obrigações a que estão vinculados, nomeadamente no que diz respeito aos deveres de informação. Cada responsável deve, ainda, conservar um registo de todas as atividades de tratamento sob a sua responsabilidade, o qual deverá conter as informações constantes do artigo 30.º RGPD.

O responsável pelo tratamento de dados pode proceder a esse tratamento internamente ou adjudica-lo a um subcontratante. Nos termos do artigo 28.º, apenas é possível recorrer a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos da proteção de dados contidos no Regulamento. Por seu turno, o subcontratante não pode transmitir os dados a outro subcontratante sem que o responsável pelo tratamento tenha dado por escrito autorização, genérica ou específica, para o efeito. Nos termos do artigo 28.º/3 RGPD, "o tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento".

Prevêem-se, igualmente, outras regras, quais sejam o estabelecimento de códigos de conduta, a realização de *privacy impact assessements*, a notificação obrigatória das autoridades em caso de violação de dados pessoais, a nomeação de um encarregado de proteção de dados. São também reguladas, nos artigos 44.º e seguintes, as transferências de dados para países terceiros.

3. A responsabilidade civil pela violação do direito aos dados pessoais

O regulamento europeu prevê, no artigo 82.º, que qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do referido regulamento tem direito a receber

uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. Acrescenta o n.º 2 do preceito que qualquer responsável pelo tratamento que nele esteja envolvido é responsável pelos danos causados por um tratamento que viole o presente regulamento, sendo o subcontratante responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações impostas pelo regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento. Esta responsabilidade pode ser afastada se o responsável pelo tratamento ou o subcontratante provar que não é responsável pelo evento que deu origem aos danos. Havendo mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, que sejam responsáveis por danos causados pelo tratamento, cada um é responsável pela totalidade dos danos, prevendo-se no n.º5 do artigo 82.º a possibilidade de exercício do direito de regresso em relação à parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com a regra estabelecida no n.º 2.

Torna-se, assim, inequívoco que o Regulamento 2016/679 consagra uma regra de solidariedade obrigacional entre os corresponsáveis, ao mesmo tempo que parece inverter o ónus da prova, a partir do momento em que se constata a violação das obrigações por ele impostas[6]. As soluções são de aplaudir, não

[6] A solução parecia já resultar da lei de proteção de dados nacional. O n.º2 do artigo 34.º prevê que "o responsável pelo tratamento pode ser parcial ou totalmente exonerado desta responsabilidade se provar que o facto que causou o dano não lhe é imputável". A formulação legal peca, contudo, por não perceber que, se o evento não for imputável ao sujeito, não é possível afirmar-se a responsabilidade, não fazendo sentido falar de uma responsabilidade parcial.

só pelo cunho protetivo do titular dos dados que apresentam, como porque parecem resultar do funcionamento das regras ressarcitórias, quando entendidas numa ótica personalista. De facto, a partir do momento em que um determinado sujeito lida com dados alheios, assume uma esfera de risco/responsabilidade, devendo adotar as medidas de cuidado — consagradas pelo legislador — no sentido de garantir a sua incolumidade. Não o fazendo, a primitiva esfera de responsabilidade (*responsabilidade pelo outro, ou pelos dados do outro*) convola-se numa outra esfera, mais ampla, de responsabilidade, no sentido da *liability (responsabilidade perante o outro*). A esta esfera são reconduzidos todos os danos-lesão que deveriam ser obviados pelo cumprimento do dever legal imposto, pelo que, *a priori*, cada interveniente no tratamento dos dados responderá pela totalidade do dano verificado em face do sujeito lesado. Posteriormente, pelo confronto entre a esfera de risco/responsabilidade do lesante e outras esferas de risco, aquele primitivo nexo imputacional que se desenha concretiza-se, podendo em concreto excluir-se ou conjugar-se com outros.

Não basta, contudo, que se determine um concreto nexo de imputação para que a responsabilidade seja afirmada. A este associam-se outros requisitos de uma pretensão indemnizatória procedente: a ilicitude, a culpa e o dano. Ademais, a modelação que aquele nexo conheça, exatamente porque de um nexo de ilicitude se trata, fica dependente da concreta modalidade de ilicitude desvelada e, mais amplamente, da modalidade de responsabilidade civil em causa. Nessa medida, a análise que se possa fazer da responsabilidade de cada um dos intervenientes

Teria, portanto, de se tratar de uma não imputação em termos também parciais, a obrigar a uma correção do preceito.

num procedimento de tratamento de dados fica dependente da modalidade de responsabilidade civil concretamente que se mobilize em concreto e da posição que, como responsável pelo tratamento ou como subcontratante, o sujeito assuma em relação aos mencionados dados. Importa, por isso, perceber quem é o responsável ou quem pode ser o responsável, no sentido de *controller*, e quem é ou pode ser o subcontratante, ou seja, o *processor,* por um lado, e, por outro lado, refletir sobre as suas posições à luz das diversas modalidades de responsabilidade civil.

3.1. Os possíveis responsáveis: o controller e o processor

Nos termos do artigo 4.º/7 RGPD, o responsável pelo tratamento (*controller* ou *controlador*) é "a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro".

O responsável pelo tratamento de dados ou *controller é, portanto, a pessoa, singular ou coletiva, que determina as finalidades e os meios de tratamento de dados, isto é, aquele que decide que meios são* recolhidos e tratados, como e porque é que o são. No fundo, é a pessoa que exerce o controlo sobre os dados, razão pela qual lhe são impostos especiais deveres e lhe é imputada a responsabilidade, em caso de violação de algum deles. De acordo com a explicitação do Grupo de Trabalho do

Artigo 29.º sobre a Proteção de Dados, o controlo de que aqui se fala pode resultar de três vias: de uma competência legal expressa; de uma competência tácita, no âmbito de uma relação contratual; ou de uma influência de facto[7]. Fundamental é que este controlo não seja meramente formal, pelo que, consoante se pode ler no documento europeu — embora por referência ao anterior quadro legislativo —, havendo nomeação legal do responsável pelos dados, ela deve refletir a realidade, devendo aquele que é indicado como *controller* exercer um controlo efetivo sobre os dados[8]. Do mesmo modo, nas outras vias de controlo, é essencial ter em conta as cláusulas de um eventual contrato, o grau de controlo efetivamente exercido, a imagem transmitida aos titulares dos dados, tendo sempre presente que releva mais o efetivo controlo material do que as eventuais classificações formais a que possamos ser conduzidos pelos negócios envolvidos na situação[9].

Se uma seguradora recolhe os dados dos seus clientes, quando com eles celebra um contrato de seguro, havendo, depois, uma outra entidade que armazena, digitaliza e cataloga todas as informações relevantes, de acordo com as instruções específicas fornecidas pela seguradora e para os fins que ela tenha estabelecido, então, a seguradora é, neste contexto, o *controller*, ou seja, o responsável pelo tratamento dos dados. Mas, se a seguradora X contrata a empresa Y, que presta ser-

[7] Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 14 s.

[8] Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 14 s.

[9] Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 16.

viços de *marketing direto* a várias empresas, para difundir os seus produtos junto dos seus clientes, e Y, para além de cumprir a obrigação a que está contratualmente vinculado, decide usar a base de dados que lhe foi transmitida pela seguradora para promover, também, produtos de outros clientes, então, assume uma nova finalidade para o tratamento dos dados, passando a ser um *controller*, não obstante a eventual designação que possa surgir no contrato[10]. A solução é ditada pelo artigo 28.º/10 RGPD, nos termos do qual "o subcontratante que, em violação do presente regulamento, determinar as finalidades e os meios de tratamento, é considerado responsável pelo tratamento no que respeita ao tratamento em questão", e vai ao encontro do que, por referência à anterior legislação europeia na matéria, era defendido pelo grupo de trabalho do artigo 29.º para a proteção de dados. No parecer 1/2010, sobre os conceitos de responsável pelo tratamento e subcontratante, pode ler-se que "a determinação da finalidade de tratamento está reservada ao responsável pelo tratamento", pelo que quem assumir a decisão de eleger uma nova finalidade assume, igualmente, tal estatuto[11]. O raciocínio é, aliás, estendido pelo referido grupo de trabalho às pessoas singulares que se integram na estrutura organizacional do *controller*. Se, em regra, elas agem por conta da pessoa coletiva, não se distanciando dela, para efeitos de aplicação do regulamento, se, "ultrapassando o âmbito das atividades da pessoa coletiva e escapando ao seu controlo, utilizar dados para os seus próprios fins", deve ser tratada como responsável pelo tratamento dos dados[12].

Não deixa, contudo, de ser estranha a perspetiva a que somos conduzidos por determinação legal, razão pela qual importa sobre ela tecer alguns esclarecimentos. Em primeiro lugar, resulta do exposto que a noção de *controller é uma noção dinâmica, que não se deixa aprisionar por determinações abstratas formuladas a priori*, antes procurando espelhar o efetivo controlo de facto sobre as finalidades e os meios de tratamento de dados. Por outro lado, ao dispor-se que o subcontratante que eleja uma finalidade nova e própria em relação aos dados que lhe foram transmitidos deve passar a ser tratado como responsável pelo tratamento de dados, pretende-se que, porque os dados passam a ser utilizados com outro objetivo e através de outros meios, independentemente da ilicitude que esta alteração já possa, em si mesma, comportar, as garantias de segurança que são oferecidas pelo regulamento ao titular dos dados se mantenham. Simplesmente, essa determinação só faz sentido quando a utilização dos dados segundo uma nova finalidade não tenha, por um lado, em vista uma violação dos direitos que subjazem à proteção de dados, e, por outro lado, quando a estrutura organizacional do sujeito que se convola em *controller permita* antever uma utilização dos dados em termos de efetivo controlo factual sobre eles e em termos de utilização consentânea com o regulamento, para lá da questão da ilegitimidade da utilização pela violação do consentimento. É que só nesses casos faz sentido impor ao novo *controller as medidas* protecionistas gizadas pelo legislador europeu. De

[10] A explicitação é feita pelo Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 18, que nos apresenta um caso com uma intencionalidade e uma estrutura problemáticas em tudo idênticas ao que aqui deixamos inscrito.

[11] Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 19.

[12] Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 20.

outro modo, estar-se-ia a considerar que o que atua ilicitamente — e voltamos a frisar que a atuação ilícita existe sempre, pela utilização dos dados para uma finalidade não consentida — fica ainda vinculado, nessa sua atuação que o ordenamento jurídico repudia, por determinados deveres legais. No fundo, a única solução que se admite como sustentável — sem embargo da ilicitude de base com que nos possamos confrontamos — é a que, independentemente da responsabilidade que se possa desencadear, olha para uma utilização de dados que, se fosse consentida, não seria ilícita para lhe impor regras que a tornem efetivamente segura para os titulares daqueles dados. São, portanto, preocupações protecionistas que avultam maiores a este nível. Simplesmente, estas não são compagináveis com uma utilização que, independentemente da falta de consentimento, sempre se teria de reputar de ilícita porque violadora dos direitos que estão na base da proteção de dados. Pense-se, por exemplo, na hipótese de um sujeito que se aproveita da base de dados de um *controller* para eleger como nova finalidade (sua) do tratamento de dados a promoção de uma campanha atentatória da honra dos visados. É claro que, numa situação como esta, por maioria de razão, o sujeito em questão será responsável, mas sê-lo-á, não no sentido do controlo, mas no sentido da responsabilidade civil que avulta como remédio sancionatório. E para isso não necessitamos de o converter em *controller*, no quadro regulamentar, quer porque tal implicaria uma confusão entre duas aceções do termos responsável, quer porque o funcionamento das regras dogmáticas delituais (e, como veremos, contratuais) nos permite assacar essa mesma responsabilidade sem necessidade de atestar da violação das normas do regulamento.

O que fica claro em tudo isto é que há ou pode haver situações em que nos deparamos com mais do que um *controller*. O Regulamento Geral de Proteção de Dados pressupõe explicitamente essa possibilidade, ao falar de controlo conjunto, nos termos do artigo 4.º/7 e do artigo 26.º, de acordo com o qual "quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento". Por seu turno, o artigo 82.º admite a hipótese de existência de mais do que um responsável (no sentido da *liability*). Não cremos, porém, que as duas hipóteses se sobreponham. Pelo contrário, pela violação do direito à proteção dos dados pessoais pode responder alguém que não seja responsável pelo tratamento desses dados. Isto é, embora a responsabilidade no sentido da controlabilidade possa conduzir à responsabilidade enquanto *liability*, esta pode avultar sem que a primeira se afirme.

Paralelamente, haveremos de considerar que nem todas as hipóteses de pluralidade de *controllers* conduzirão a casos de pluralidade de responsáveis. De facto, e tal como o grupo de trabalho do artigo 29.º sobre a proteção de dados já havia alertado por referência à anterior diretiva comunitária, a participação de vários sujeitos numa operação de tratamento de dados pessoais não determina necessariamente um controlo conjunto. Pelo contrário, a realidade oferece-nos diversos esquemas de participação, o que pode implicar — em concreto — que, não havendo conjunção no controlo, não seja discernível a violação das obrigações legais por parte dos diversos controladores.

Antes, porém, de tentarmos refletir sobre as hipóteses em teoria cogitáveis acerca da eventual responsabilidade que pode emergir, importa, a este propósito, tentar perceber quais as estruturas problemáticas com que podemos lidar[13].

[13] Orientar-nos-emos, neste breve excurso, pela sistematização e exemplos oferecidos pelo grupo de trabalho do artigo 29.º sobre proteção de dados, que, em muitos casos, acompanharemos de muito perto.

Para que haja controlo conjunto e, portanto, para que possamos falar de co-controladores (corresponsáveis) torna-se mister que haja efetiva partilha das finalidades e dos meios. Sempre que falhe esta conjunção, falha, também, a qualificação que se procura. Pense-se, por exemplo, na hipótese de uma seguradora que envia dados dos seus clientes a uma empresa de *rent-a-car*, sempre que seja necessário prover pela contratação de um veículo de substituição no âmbito de um seguro de responsabilidade civil automóvel. A empresa em causa recolhe dados dos clientes, assumindo-se como um *controller*. Contudo, não há conjunção, por não haver partilha de finalidades, nem partilha de meios.

Mas, se a companhia de seguros decide criar, conjuntamente com um Banco, uma plataforma de gestão dos dados dos clientes comuns que, contratando com aquele um crédito à habitação, têm associado um seguro de vida, cujo contrato é celebrado com aquela seguradora, então há efetiva partilha de finalidades e de meios, a determinar que se possa falar de um controlo conjunto[14].

O controlo conjunto a que se alude pressupõe, portanto, um domínio de facto comum dos dados, o que significa que a conjunção a que se alude envolve a possibilidade de ambas as entidades cumprirem as obrigações que o regulamento prevê. No fundo, para se falar de controlo conjunto, haveremos de estar diante de uma hipótese em que os mesmos dados são partilhados por mais do que uma entidade, unidas pela prossecução de uma finalidade comum ou pela utilização de meios

[14] Para um exemplo análogo, cf. Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 23 s.

definidos em conjunto, de tal modo que só conseguimos antever uma atividade de tratamento de dados[15].

O controlo conjunto não se confunde, portanto, com um controlo comum de certos dados que não envolva partilha de finalidades e de meios (e, portanto, que não envolva uma única atividade de tratamento de dados). Se a seguradora recolhe e trata dados dos seus funcionários para fins de gestão de salários, seguros de saúde, entre outros, e depois os transmite à autoridade tributária, como lhe compete, apesar de haver partilha de dados, não há controlo conjunto, por não haver unicidade de finalidades e de meios[16].

[15] Cf. Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 27, colocando a questão de saber se o controlo conjunto envolve sempre a responsabilidade solidária e respondendo negativamente, por considerar que os diferentes responsáveis poderão ser responsáveis pelo tratamento de dados pessoais em fases diferentes e em diferentes graus. Não cremos, porém, que a posição do grupo de trabalho possa ser sufragada, mesmo descontando o facto de ela se reportar à anterior legislação comunitária na matéria. Em primeiro lugar, havendo mais do que um responsável no âmbito delitual, a regra é a da solidariedade, independentemente do grau de responsabilidade de cada um, que apenas se torna relevante no quadro das relações internas; em segundo lugar, ainda que a atuação de dois sujeitos não seja simultânea, a decisão de tratamento dos dados com base na finalidade eleita e nos meios escolhidos implica que há apenas uma atividade de tratamento de dados, embora titulada por mais do que um sujeito, e portanto reconduzível — na convolação da responsabilidade enquanto controlabilidade para a responsabilidade no sentido da *liability — a mais do que* uma esfera de responsabilidade. O controlo conjunto é incompatível com uma ideia de não solidariedade.

[16] Para um exemplo análogo, cf. Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 24 s.

Do mesmo modo, não haverá controlo conjunto quando pensamos na articulação entre as funções da seguradora e uma rede social, que disponibilizando meios de comunicação em linha permita que a seguradora responda a contactos dos seus clientes. A rede social, enquanto prestador do serviço, define finalidades e meios de tratamento de dados, não as compartilhando com a seguradora, que, a este nível, é tida como *controller autónomo*. E o mesmo se pode dizer dos servidores web em que a seguradora tenha alojada a sua página e os seus serviços de email, se o próprio servidor proceder a um tratamento ulterior de dados, para os seus próprios fins[17]. Mas já poderá haver controlo conjunto, se as finalidades e os meios forem definidos conjuntamente, naquelas hipóteses em que a seguradora utiliza uma qualquer entidade que preste serviços de pagamentos. Neste caso, há efetivamente partilha dos meios e finalidades que são comuns[18].

O controlo pode, portanto, ser conjunto ou paralelo, simultâneo ou sucessivo.

Por seu turno, o subcontratante (*processor) é aquele que procede ao tratamento de dados por conta do controller*. A atuação por conta de outro sujeito determina que as finalidades do tratamento não possam ser definidas pelo *processor*. Não é, porém, a simples eleição de uma finalidade nova, mesmo que desarreigada da possibilidade de, em relação a ela, se cumprir

[17] Caso não o faça, poderemos estar diante de um subcontratante — cf. Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 29.

[18] Cf. Grupo de trabalho do artigo 29.º sobre proteção de dados, *Parecer 1/2010 sobre os conceitos de responsável pelo tratamento e subcontratante*, wp 169, 25 e 26.

o regulamento, que poderá determinar a qualificação, como referido anteriormente. Nessas hipóteses, o *subcontratante* deve ser, em relação aos dados na sua ligação com a nova finalidade, tratado como um terceiro, do mesmo modo que deve ser tido como terceiro se a finalidade eleita implicar uma violação dos direitos que estão na base da proteção de dados.

3.2. As hipóteses de responsabilidade civil

As diversas estruturas problemáticas que fomos reconhecendo permitem-nos estabelecer um quadro (necessariamente não exaustivo, pela impossibilidade de acompanhar a capacidade criativa da própria realidade) de hipóteses de surgimento de responsabilidade civil a este nível. Tais hipóteses reconduzir-se-ão a uma das modalidades clássicas do ressarcimento. Vejamos.

Desde logo, há a considerar a responsabilidade extracontratual. Estamos, na verdade, e conforme se constata a partir da identificação de uma relação de interioridade constitutiva entre a proteção de dados e diversos direitos de personalidade, num domínio onde se lida com direitos absolutos[19]. Por outro

[19] A relação que perfuntoriamente se estabelece entre a proteção de dados e a tutela da personalidade (e mais especificamente alguns direitos de personalidade) não tem um mero cunho genético-explicativo. Pelo contrário, ela parece fundamental para, numa compreensão sistemático-axiológica do ordenamento jurídico, garantir o acerto da interpretação que se faça de algumas regras contidas na disciplina legal da proteção de dados, podendo considerar-se que existe entre ambos uma relação de interioridade constitutiva. Sobre o ponto, cf. Mafalda Miranda Barbosa, "Proteção de dados e direitos de personalidade: uma relação de interioridade constitutiva. Os beneficiários da proteção e a responsabilidade civil", *Estudos de Direito do Consumidor*, 12, 2017, 163 s.

lado, e de forma não inócua[20], as regras previstas no Regulamento podem ser entendidas enquanto disposições legais de proteção de interesses alheios, abrindo as portas à segunda modalidade de ilicitude aquiliana[21].

Por outro lado, há que ter em conta a responsabilidade contratual. Basta para tanto que a violação dos dados ocorra pela preterição de determinados deveres que oneram o responsável pelo tratamento, numa relação contratual firmada entre ele e o titular daqueles. Ainda que o contrato não tenha como objeto essa proteção dos dados, a boa-fé pode impor determinados deveres de cuidado que, quando violados, geram responsabili-

[20] A desvelação da ilicitude com base na segunda modalidade de ilicitude tem consequências dogmáticas de não pequena monta. De acordo com o pensamento de inúmeros juristas, a primeira repercussão há-de encontrar-se logo ao nível da culpa. Sublinha Sinde Monteiro que "a culpa tem agora de se referir apenas à própria violação da norma e já não à violação dos bens jurídicos" — Sinde Monteiro, *Responsabilidade por conselhos*, *recomendações ou informações*, Almedina, Coimbra, 1989, 239.

Cf., igualmente, Christian von Bar,"Delilktsrecht, Empflieht es sich, die Voraussetzungen der Haftung für unerlaubte Handlungen mit Rücksicht auf die gewandelte Rechtswirklichkeit und die Entwicklungen in Rechtsprechung und Lehre neu zu ordnen? Wäre es insbesondere zweckmässig, die Grundtatbestände der § 823 Abstätze 1 und 2, § 826 BGB zu erweitern oder zu ergänzen?", *Gutachten und Vorschläge zur überarbeitung des Schuldrechts herausgegeben vom Bundesminister der Justiz*, Bd. II, Bundesanzeiger Verlagsges, Köln, 1981, 1696, sustentando que, no caso de violação de uma norma de perigo abstrato, a culpa se limita à ofensa da norma e que há inversão do ónus da prova quanto a ela.

Em sentido diverso, cf. Hans Stoll, *Kausalzusammenhang und Normzwek im Deliktsrecht*, Mohr, Tübingen, 1968, 22 e ss.

Não cremos, porém, que esta nota deva ser sobrevalorizada. De acordo com o modelo imputacional que tivemos oportunidade de delinear na nossa dissertação de doutoramento, no caso da primeira modalidade de ilicitude, desenha-se, em concreto, a partir da preterição de deveres de segurança no tráfego, onde se incluem deveres de cuidado (que, uma vez lesados, permitem desvelar a culpa), uma esfera de risco/responsabilidade que estará na base da imputação de um resultado ao agente. Ora, a culpa há-de referir-se a essa esfera de responsabilidade e não a todos os danos-eventos que surjam. Sobre o ponto, cf. Mafalda Miranda Barbosa, *Do nexo de causalidade ao nexo de imputação. Contributo para a compreensão da natureza binária e personalística do requisito causal ao nível da responsabilidade civil extracontratual*, Princípia, 2013, 914 s. e *Lições de Responsabilidade civil*, Princípia, 2017.

Por outro lado, a violação da norma implica, segundo a posição de alguns autores, uma presunção de culpa. A este ensejo podemos referir duas grandes posições na doutrina: os autores que defendem a existência de uma verdadeira inversão do ónus *probandi e os que se limitam a falar de uma presunção simples*. Cf. Sinde Monteiro, *Responsabilidade por conselhos*, 265.

In fine, tal antecipação teria consequências ao nível da causalidade. Prescindir-se-ia a este nível da ideia de adequação e da ideia de probabilidade que lhe anda associado. Como se compreenderá, a partir do momento em que defendemos justificadamente o afastamento da ideia de causalidade adequada de toda a construção ressarcitória, estas consequências terão necessariamente um impacto menor, até porque à mesma inversão do ónus da prova se consegue chegar a partir do momento em que se aceite o nexo de imputação por nós delineado. Cf. *Do nexo de causalidade ao nexo de imputação*, cap. X.

A mais-valia da segunda modalidade de ilicitude passa, aos nossos olhos, pelo facto de ser o legislador que, *a priori,* define os contornos da esfera de responsabilidade, ao impor uma conduta ou ao proibir outra, ao mesmo tempo que permite o alargamento do leque de interesses protegidos em sede delitual.

[21] O dado resultava inequívoco do artigo 34.º da lei de proteção de dados, nos termos do qual qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro ato que viole disposições legais de proteção de dados pessoais tem direito de obter do responsável a reparação do prejuízo sofrido. Reproduz-se, assim, em matéria de proteção de dados a regra geral de duplicidade de modalidades de ilicitude ao nível extracontratual (descontado que seja o abuso do direito, enquanto modalidade autónoma).

dade contratual. E, se o que se defende implica a adesão a duas teses — a aceitação da ideia de concurso entre modalidades de responsabilidade civil, entendido enquanto concurso de fundamentos de uma mesma pretensão indemnizatória; e a adesão à posição doutrinal segundo a qual a violação de deveres de conduta, porque reconduzidos ao núcleo da relação contratual, vista como uma relação obrigacional complexa, gera uma hipótese que é assimilada pela responsabilidade contratual —, nem por isso deve ser desconsiderado, pois são estas posições que temos vindo a defender[22].

Do mesmo modo, também a responsabilidade civil do *processor* se mostra apta a ser assimilada quer pela intencionalidade problemática da responsabilidade extracontratual, quer pela intencionalidade problemática da responsabilidade contratual.

É, portanto, à luz destas duas modalidades e dos seus concretos regimes que vamos tentar sistematizar algumas das eventuais hipóteses de surgimento, neste âmbito, de uma pretensão indemnizatória procedente, orientando-nos para o efeito pelas estruturas problemáticas recortadas: controlo conjunto; controlo paralelo; e subcontratação.

3.2.1. A responsabilidade extracontratual

a) Controlo conjunto

Imaginemos a hipótese, já referida, de uma companhia de seguros que decide criar, conjuntamente com um Banco, uma

[22] Sobre estes pontos, com maior desenvolvimento e outras referências bibliográficas, cf. Mafalda Miranda Barbosa, *Lições de responsabilidade civil*, 19 s. e 22 s.

plataforma de gestão dos dados dos clientes comuns que, contratando com aquele um crédito à habitação, têm associado um seguro de vida, cujo contrato é celebrado com aquela seguradora, havendo partilha de finalidades e de meios, a determinar que se possa falar de um controlo conjunto.

Havendo violação do direito à proteção de dados no quadro do tratamento conjunto que deles seja feito, avultará necessariamente a responsabilidade quer da seguradora, quer do Banco, em termos de solidariedade. Esta solução resulta dos artigos 82.º/2 e 4 RGPD, estando em sintonia com o disposto no artigo 497.º CC. É que o controlo conjunto a que se alude não mais representa do que uma estrutura problemática que, pela partilha de finalidade e de meios, determina que haja apenas um tratamento para o qual convergem duas esferas de responsabilidade subjetivas. Se aquele tratamento envolve a preterição de dados pessoais, então, porque o controlo de finalidades e meios é comum e determina um só tratamento, tornam-se atuantes diversas esferas de risco/responsabilidade.

b) Controlo paralelo

Retomemos, agora, a hipótese de uma seguradora que envia dados dos seus clientes a uma empresa de *rent-a-car*, sempre que seja necessário prover pela contratação de um veículo de substituição no âmbito de um seguro de responsabilidade civil automóvel. A empresa em causa recolhe dados dos clientes, assumindo-se como um *controller*. Contudo, não há conjunção, por não haver partilha de finalidades, nem partilha de meios. Se a violação dos dados ocorre no tratamento que é feito pela empresa de *rent-a-car*, então, parece que apenas esta será responsabilizada pelos danos que possam emergir.

Há que ter, no entanto, em conta alguns dados. Em primeiro lugar, a noção de tratamento de dados com que somos confrontados pelo regulamento é muito ampla. Nos termos do regulamento, o tratamento de dados é visto como uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição. Significa isto que a simples transmissão dos dados para uma outra empresa integra o conceito de tratamento. Se o primeiro *controller* não se assegura da fiabilidade do cumprimento do regulamento por parte do segundo controller poderá ser por isso responsabilizado. É claro que, sendo o regulamento imperativo para todos os agentes, se poderá chamar à colação uma ideia de confiança para afastar, a este nível, a responsabilidade do primeiro. Simplesmente, nada exclui a possibilidade de a empresa de rent-a-car estar sediada fora da União Europeia. Ora, de acordo com o Regulamento, as transferências para países terceiros (bem como para organizações internacionais) só podem ser efetuadas no pleno respeito pelo presente regulamento, ou seja, só podem ter lugar se houver garantias de cumprimento de um nível de proteção idêntico ao que o regulamento dispõe por esse novo *controller*, o que significa que, apesar de o ato diretamente violador dos dados ser perpetrado pelo último, é possível que se venha a imputar ao primeiro também a responsabilidade, operando as regras da solidariedade, nos termos do artigo 82.º/4 RGPD.

Por outro lado, há que ter em conta que o artigo 82.º/3 dispõe que "o responsável pelo tratamento (...) fica isento de responsabilidade nos termos do n.º2, se provar que não é de modo algum responsável pelo evento que deu origem aos danos". O que o preceito estabelece é a regra da inversão do ónus da prova da imputação (outrora dita causalidade), de tal modo que, havendo mais do que uma esfera de responsabilidade em relação a um mesmo conjunto de dados, relativamente ao qual se verifica um evento danoso, ambos são responsabilizados solidariamente[23], exceto se, no posterior cotejo de esferas de responsabilidade a que se processe, se perceba que a esfera de responsabilidade de um agente consome a do outro. Se deve ser assim em geral, há que sublinhar que geralmente a esfera de responsabilidade avulta unicamente a partir da constatação de um aumento do risco, ou seja, da preterição de deveres no tráfego. A especificidade que o Regulamento nos traz é, mais do que permitir que, uma vez violada uma regra por ele imposta, se presuma que a sua preterição foi culposa, considerar que o *controller* será sempre responsável pela violação dos dados, bastando que para tal esteja envolvido naquele tratamento. Se é certo que, na hipótese em análise tal não ocorre, porque o tratamento gerador da lesão é subsequente, ao considerarmos que a mera transferência de dados configura, em si mesma, um tratamento, haveremos de ter em conta que lhe cabe a si provar que não houve qualquer preterição das regras impostas em matéria de transmissão de dados.

Outras hipóteses têm que ser, ainda, consideradas ao nível do controlo paralelo. Pense-se no caso em que a seguradora X

[23] A solidariedade resulta da conjugação entre o artigo 82.º/3 e o artigo 82.º/4 CC.

contrata a empresa Y, que presta serviços de *marketing direto* a várias empresas, para difundir os seus produtos junto dos seus clientes, e Y, para além de cumprir a obrigação a que está contratualmente vinculado, decide usar a base de dados que lhe foi transmitida pela seguradora para promover, também, produtos de outros clientes, assumindo uma nova finalidade para o tratamento dos dados e passando a ser um *controller*, não obstante a eventual designação que possa surgir no contrato. Ou seja, estamos aqui a lidar com um segundo *controller* que, inicialmente, era apenas um *processor*. Ainda que o primeiro *controller* não intervenha, aparentemente, no tratamento dos dados, não se mobilizando o disposto no artigo 82.º/2 RGPD, nem por isso se afasta de imediato a responsabilidade daquele. Na verdade, Y pode ser, em relação a X, qualificado como comissário, colocando-se, portanto, o problema da assimilação do âmbito de relevância do caso assimilado pelo âmbito de relevância do artigo 500.º CC.

Para que a seguradora X possa ser responsabilizada a este nível não basta que exista uma efetiva relação de comissão entre ambos e que todos os pressupostos da responsabilidade civil se verifiquem em relação a Y, tornando-o responsável. É necessário, ainda, que o ato tenha sido praticado no exercício das suas funções. Segundo Menezes Cordeiro, "a ideia do legislador é a de delimitar o âmbito do risco que vai repercutir no comitente"[24]. Mas, nem sempre se mostram coincidentes as respostas dos autores quanto à delimitação anunciada. Antunes Varela considera que há atuação no exercício das funções quando a comissão seja causa adequada ou idónea do facto

[24] Menezes Cordeiro, *Tratado de direito civil português*, II, *Direito das Obrigações*, tomo III, Almedina, 2010, 614.

ilícito perpetrado pelo comissário. Importante é que o ato seja praticado no quadro geral de competência deste último, uma vez que, fora dele, a lesão ocorrida deixa de ser previsível, não devendo o comitente responder por ela[25].

Por seu turno, Menezes Cordeiro e Menezes Leitão acabam por aderir a um posicionamento mais amplo, sustentando

[25] Cf. Antunes Varela, *Das Obrigações em geral*, I, Almedina, Coimbra, 2003, 536 s.

No mesmo sentido, cf. Pedro Nunes de Carvalho, "A responsabilidade do comitente", *Revista da Ordem dos Advogados*, ano 48, 1988, 85 s. Porque "o comitente só será chamado à responsabilidade nos casos em que o ato praticado pelo comissário tenha determinado nexo causal com a comissão", coloca-se o problema de saber como é que ele há-de ser estabelecido. Em resposta ao quesito, o autor aduz que "não basta que haja uma mera conexão temporal ou local com a função", sendo necessário que o ato seja praticado no exercício dela. Tal conexão há-de ser suficiente e não ocasional, devendo interpretar-se a noção de acordo com o fundamento da responsabilidade do comitente, qual seja, a de se basear também no benefício que o comitente retira da atividade do comissário, não estando em debate uma mera responsabilidade pela garantia. Nessa medida, o autor sustenta que, quando o artigo 500.º/2 CC aponta para "a responsabilidade do comitente por atos praticados pelo comissário ainda que intencionalmente, deve entender-se que a referência aos atos danosos praticados intencionalmente pelo comissário no exercício da sua função se reporta apenas àqueles que sejam previsíveis (...) no quadro geral da função (teoria da causalidade adequada)".

Cf., ainda, Mota Pinto, *Teoria Geral do Direito Civil,* 4ª edição por António Pinto Monteiro e Paulo Mota Pinto, Coimbra Editora, Coimbra, 2005, 321; Ribeiro de Faria, *Direito das Obrigações*, I, 17-18, sustentando o que o nexo do facto ilícito com as funções do comissário deve ser interno, direto e causal; Antunes Varela/Pires de Lima, *Código Civil anotado*, vol. I, 4ª edição, 1987, p. 509, falando de factos ilícitos praticados por ocasião do exercício das funções mas em que o exercício não constitui uma causa adequada

que basta que os danos sejam causados no exercício da função e não por causa dela[26].

Cremos ser preferível sustentar, na esteira do entendimento mais restritivo, que a lesão deve ser vista como concretização do risco funcional, exigindo-se, por isso, a atuação no quadro geral de competência ou dos poderes conferidos ao comissário, com o que ficam excluídos os atos que não se inscrevem no esquema do exercício da função (que foi para o surgimento deles mera ocasião), embora se incluam os que se ligam àquela por um nexo meramente instrumental (designadamente nas hipóteses de abuso de funções)[27]. Simplesmente, para tanto, não aderimos a qualquer critério causal, assente quer na condicionalidade, que alargaria desmedidamente a responsabilidade do comitente, para além de todos os outros problemas dogmáticos que arrastaria, quer na causalidade adequada, por ser a probabilidade a que ali se alude uma verdadeira fórmula vazia para lidar com o problema[28]. Do que se trata, afinal, é

[26] Menezes Cordeiro, *Tratado de direito civil português*, II, *Direito das Obrigações*, tomo III, Almedina, 2010, 614; Menezes Leitão, *Direito das Obrigações* I, 9.ª edição, Almedina, Coimbra, 2010, 369

[27] A lição é de Antunes Varela, *Das obrigações*, 642, que aqui acompanhamos de perto. Note-se, porém, que não aderimos a uma conceção de causalidade entendida em termos de causalidade adequada. Sobre o ponto, cf. Mafalda Miranda Barbosa, *Do nexo de causalidade ao nexo de imputação. Contributo para a compreensão da natureza binária e personalística do requisito causal ao nível da responsabilidade civil extracontratual*, Princípia, 2013.

[28] Maria da Graça Trigo, *Responsabilidade civil delitual por facto de terceiro*, Coimbra Editora, Coimbra, 2009, 407. A autora mostra-se cética da possibilidade de densificar a noção de "exercício de funções" com recurso a um critério causal. Para ela, "a principal dificuldade radica em que o uso de expressões habitualmente conotadas com um dos pressupostos da responsabilidade civil pode levar a equívocos terminológicos e conceituais", confundindo-se o

de saber se a atribuição daquelas funções aumentou o risco de surgimento da lesão ou se ela poderia ter lugar de igual modo, ainda que não existisse a comissão que foi, assim, mera ocasião (como poderia haver outras) de surgimento da violação.

O dado parece, aliás, ser consentâneo com a lição da doutrina no sentido de afirmar que haverá responsabilidade, mesmo quando o ato tenha sido praticado intencionalmente ou contra as instruções do comitente, aproveitando-se da imagem de "aparência social que cria um estado de confiança do lesado na lisura do comportamento daquele"[29], pelo que se poderá, efetivamente, aventar a pretensa responsabilidade do primeiro *controller* pelo ato do *processor* convertido em *controller*, dependendo das especificidades do caso concreto. É que, mesmo que ele tenha contrariado as instruções do primeiro *controller* e elegido uma nova finalidade para o tratamento de dados, com meios próprios, sem o que não se converteria em *controller*, não o poderia fazer sem os meios que lhe foram facultados pela seguradora.

pressuposto comum da causalidade com um dos pressupostos específicos da responsabilidade do comitente. Apresentando o seu próprio critério (distinto, pois, da cisão entre *exercício das funções* e *por ocasião das funções,* a fazer apelo à ideia de que, neste último caso, o facto podia ter tido lugar independentemente daquelas), esclarece que a conexão causal adequada entre as funções do comissário e o facto danoso traduz-se fundamentalmente na verificação de um certo nível de probabilidade de que no decurso daquelas funções possa ocorrer um ato lesivo de terceiros, não andando por isso muito longe das soluções a que se chegam pelo denominado *Salmond Test* (o qual vem indagar se o ato se insere no âmbito dos atos autorizados pelo comitente, quer a autorização seja expressa, tácita ou mesmo aparente) — cf. pág. 342 s.

[29] Mota Pinto, *Teoria Geral do Direito Civil,* 324.

c) Subcontratação

As dúvidas em relação à responsabilidade do *controller* parecem atenuar-se no caso da violação de dados por parte do subcontratante.

Em primeiro lugar, pode haver responsabilidade direta (subjetiva) do primeiro se se provar que violou a obrigação de apenas recorrer a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas, de modo que o tratamento satisfaça os requisitos do regulamento geral de proteção de dados. O facto de o subcontratante cumprir um código de conduta aprovado ou um procedimento de certificação aprovado poderá ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento, conforme explicita o próprio Regulamento, nos seus *considerandi*.

Em segundo lugar, pode haver responsabilidade objetiva, por força do artigo 500.º CC, nos termos explicitados anteriormente.

Em qualquer dos casos, a responsabilidade do *controller* não afasta a responsabilidade própria do *processor*.

3.2.2. A responsabilidade contratual

A hipótese de responsabilidade contratual pressupõe a existência prévia de um contrato, pelo que a ela só podemos recorrer quando a legitimação para o tratamento de dados assente em base negocial. É que ainda o contrato não tenha como objeto essa proteção dos dados, a boa-fé pode impor determinados deveres de cuidado que, quando violados, geram responsabilidade contratual. A violação de deveres de conduta, porque reconduzidos ao núcleo da relação contratual, vista como uma relação obrigacional complexa, gera uma hipótese que é assimilada pela responsabilidade contratual[30].

Esta avulta, também, de forma clara nas hipóteses de controlo conjunto, quando o contrato em que se baseia a proteção de dados seja celebrado por mais do que um sujeito. Noutras hipóteses e em casos de controlo paralelo, haveremos que analisar o artigo 800.º CC. O primeiro *controller responde, como se de um ato seu se tratasse, por todos os comportamentos lesivos levados a cabo por terceiros de que se sirva para cumprimento das suas obrigações*.

O desenho estrutural do artigo 800.º CC é, então, absolutamente díspar, quando comparado com o do artigo 500.º CC. Desaparece, a este nível, a dupla imputação para se fazer responder o devedor pelos atos dos auxiliares que utilize no cumprimento da obrigação como se fossem os seus próprios atos. Como sublinha Carneiro da Frada, "a técnica da lei é distinta. O que ela faz é projetar logo a conduta do auxiliar na pessoa do devedor para verificar se desse modo o devedor incorreria ou não em responsabilidade"[31].

Trata-se do que o autor cunha por *teoria da ficção*, na medida em que "se ficciona o comportamento causador do dano na pessoa do devedor"[32], consubstanciando, de acordo com a

[30] Sobre estes pontos, com maior desenvolvimento e outras referências bibliográficas, cf. Mafalda Miranda Barbosa, *Lições de responsabilidade civil*, 19 s. e 22 s.

[31] M. Carneiro da Frada, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", *Direito e Justiça*, vol. XII, tomo I, 1998, 301.

[32] M. Carneiro da Frada, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 302; Id., *Con-*

lição de outros civilistas, uma verdadeira responsabilidade objetiva por ato alheio[33].

Duas são as situações com que podemos ser confrontados: a) o devedor atua com culpa *in elegendo*, *in instruendo* ou *in vigilando*, devendo ser responsabilizado com base em culpa, para o que não seria necessário mobilizar o artigo 800.º CC[34]; b) o devedor não atua negligentemente, mas ocorre um dano por virtude da atuação do terceiro auxiliar, e ele continua a ser responsabilizado, *ex via* artigo 800.º CC[35].

trato e deveres de protecção, Separata do Boletim da Faculdade de Direito da Universidade de Coimbra, Coimbra, 1994, 210. Em sentido próximo, cf., ainda, Menezes Cordeiro, *Da responsabilidade civil dos administradores* das sociedades comerciais, Lex, Lisboa, 1997, 487

[33] Cf. Antunes Varela, *Das obrigações em geral*, vol. II, 7.ª edição (reimpressão), Almedina, Coimbra, 2001, 103. De acordo com Carneiro da Frada, não estaria em causa uma verdadeira responsabilidade objetiva. Segundo se pode ler no estudo citado do autor, "outro poderia ter sido o caminho do legislador. Em vez da descrita ficção, uma similar amplitude de responsabilidade teria sido obtida se se tivesse abertamente consignado uma responsabilidade objetiva pela utilização de terceiros no cumprimento do programa obrigacional. Se bem se reparar, sem ter então que «representar» uma responsabilidade por facto ilícito-culposo do devedor" — M. Carneiro da Frada, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 303. Cf., também, M. Carneiro da Frada, *Contrato e deveres de protecção,* 209 s.

Aderindo à chamada teoria da ficção, cf. Maria da Graça Trigo, *Responsabilidade civil delitual,* 249 s.

[34] Para a consideração de ordenamentos jurídicos onde se chega à solução da responsabilidade contratual por facto de outrem sem que haja um preceito análogo ao artigo 800.º CC, cf. René Rodière, "Y a-t-il une responsabilité contractuelle du fait d'autrui?", *Recueil Dalloz*, Chr., 1952, 18 s.

[35] Veja-se, num sentido próximo, Ernst von Caemmerer, "Verschulden von Erfüllungsgehilfen", *Festschrift für Fritz Haupt*, Karlsruhe, 1978, 38 s. Para o autor, o devedor poderá ser responsável por culpa *in elegendo*, naquelas situações em que escolhe incorretamente o seu auxiliar (v.g., escolhe uma pessoa que não tem as competências devidas ou é inimputável); caso o seu comportamento não seja culposo, então poderá continuar a ser responsabilizado, por via do §278 BGB, desde que o terceiro auxiliar atue com culpa. A falta de culpa do auxiliar determina a exoneração da responsabilidade do devedor, já que a missão do §278 não é ampliar a responsabilidade do devedor, mas torna-lo responsável como se tivesse sido ele próprio a atuar.

O que divide a doutrina, a este ensejo, é saber se esta é uma responsabilidade objetiva por ato de terceiro ou uma direta responsabilidade do devedor. Enquanto alguns autores olham para o artigo 800.º no sentido de o preceito consagrar uma pura responsabilidade objetiva; outros entendem que as situações em que há culpa *in vigilando, in instruendo* ou *in elegendo* da parte do devedor também são assimiladas pela sua intencionalidade prático-normativa. Daqui resulta, em termos de construção dos pressupostos de relevância do preceito, uma consequência importante. Assim, enquanto a maioria dos autores sustenta que a falta de culpa do auxiliar afasta a responsabilidade do devedor[36], outros como Carneiro da Frada parecem depor em sentido contrário[37].

Importa ponderar o problema em função da intencionalidade normativa do preceito[38].

[36] Cf. Vaz Serra, "Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos", *Boletim do Ministério da Justiça*, n.º72, 1958, 280 s.; Pessoa Jorge, *Ensaio sobre os pressupostos da responsabilidade civil*, Almedina, Coimbra, 1999 143 s.

[37] M. Carneiro da Frada, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 303. Para um aprofundado debate sobre a questão, cf. Maria da Graça Trigo, *Responsabilidade civil delitual,* 247 s.

[38] Para além da chamada teoria da ficção, Carneiro da Frada indica outros tópicos para a fundamentação da responsabilidade do devedor pelos atos dos auxiliares: "se a utilização de auxiliares pelo devedor aumenta o seu raio de ação, potenciando os seus lucros, é também de elementar justiça que so-

Em face de uma obrigação, em regra, o devedor não tem o poder de recusar uma prestação efetuada por um terceiro[39]. Por outro lado, aquele que está por ela vinculado até ao momento do cumprimento integral da prestação é sempre o devedor. O risco do não cumprimento da obrigação corre, por isso, por conta dele[40]. De acordo com o ensinamento de Vaz Serra, "o devedor responde por todos aqueles que deixou penetrar no seu domínio de atividade ou que admitiu a colaborar consigo de maneira mais ou menos permanente ou mais ou menos completa na execução das suas obrigações"[41]. Entende-se que assim seja. Na verdade, se o devedor não fosse chamado a responder independentemente de culpa própria, ele encontraria um expediente simples para excluir a sua responsabilidade. Bastaria, para tanto, que chamasse um terceiro para efetuar a prestação, o que, inclusivamente, poderia abrir a porta a abusos evidentes[42].

No fundo, intervindo aqui uma ideia de confiança, o devedor responde independentemente de culpa sua pelos danos que ocorram. Simplesmente, não se verifica a dupla imputação a que somos conduzidos por via do artigo 500.º CC. E não se verifica porque o contrato que alicerça a responsabilidade define, *a priori*, o obrigado e, portanto, o responsável em caso de incumprimento (em sentido amplo). O que o artigo 800.º vem esclarecer é que a imputação dos danos ao devedor não se perde pelo simples facto de ele ter utilizado um terceiro, seu auxiliar[43], no cumprimento da

bre ele recaiam os riscos correspondentes à sua atividade. É o devedor, aliás, quem os pode controlar melhor e, em qualquer caso, absorve-los com maior facilidade. Por isso também, como correspetivo desse risco da sua atividade, se compreende que ao credor esteja vedado interferir no programa de realização da prestação elaborado pelo devedor" — M. Carneiro da Frada, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 303.

[39] Cf. artigos 767.º e 768.º CC, para fundamentar a afirmação, bem como para evidenciar as situações em que o credor pode opor-se à realização da prestação por um terceiro.

[40] Veja-se, porém, *supra* a questão de saber se se deve ou não exigir a culpa do devedor, que se presumiria nos termos do artigo 799.º CC. Sobre o ponto, cf. Karl Larenz, *Lehrbuch des Schuldrechts*, I, *Allgemeine Teil*, München, 1979, 292 s. No ordenamento jurídico alemão, cf., ainda, Berthold Kupisch, "Die Haftung für Erfüllungsgehilfen (§278)", *JuS*, 1983, 817 s.

V., ainda e novamente, Maria da Graça Trigo, *Responsabilidade civil delitual,* 251 s., dando conta da posição de Oertmann, que preconizaria a *ficção de existência de uma obrigação própria do auxiliar*, pelo que a ilicitude e a culpa teriam de se referir a essa pessoa, donde o auxiliar teria de ser imputável e não poderia ocorrer, em relação a ele, qualquer causa de exclusão da culpa; e da ideia de *ficção de que não teria sido o auxiliar a atuar, mas sim o devedor*, pelo que a questão da culpa se apuraria determinando se uma atuação correspondente do próprio devedor seria ou não culposa. Assim, se o devedor, em caso de comportamento equivalente, fosse imputável e não se verificassem causas de exclusão da culpa, haveria responsabilidade.

[41] A. Vaz Serra, "Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos", 273 s.

V., igualmente, Pessoa Jorge, *Ensaio*, 149, considerando que o artigo 800.º vem impedir que o devedor invoque a inexecução da obrigação imputável ao auxiliar e determinar que ele continua sujeito à sua obrigação inicial e à correlativa responsabilidade.

[42] Cf. A. Pinto Monteiro, *Cláusulas limitativas e de exclusão da responsabilidade*, Almedina, Coimbra, 2003, 284 s.

[43] Os autores têm sublinhado que estes auxiliares podem ser, indiferentemente e para efeitos da mobilização do regime do artigo 800.º CC, auxiliares dependentes ou independentes. Nesse sentido, cf. Pinto Monteiro, *Cláusulas limitativas*, 287 s.; Menezes Cordeiro, *Da responsabilidade civil dos administradores*, 487, n.61; Maria da Graça Trigo, *Responsabilidade civil delitual*, 242 s.; Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", *Revista de Direito e Economia*, ano XV, 82 s.

obrigação[44]. Nessa medida, ainda que objetivada, a responsabilidade há-de configurar-se como uma responsabilidade direta do devedor[45]-[46]. Em rigor, aliás, a ideia de controlo da atua-

A este propósito, *v.*, igualmente, o problema enunciado por Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", *Revista de Direito e Economia*, ano XV, 92: até que ponto se integra a atividade de um terceiro na previsão do artigo 800.º/1 CC? Em causa está, por exemplo, a determinação da eventual responsabilidade do devedor pela atividade dos correios ou dos caminhos-de-ferro, que utiliza para enviar a coisa objeto da prestação ao credor. De acordo com o ensinamento da doutrina alemão, referida por Maria Victória Rocha, haveria exclusão da responsabilidade quando a atuação da empresa fosse monopolista. Mais esclarece que o §287 BGB não é fonte de imputação de novos deveres. Cremos que o caráter monopolista ou não da atuação do terceiro não é significativo para a resolução da questão concretamente considerada. Na verdade, a solução para o problema há-de passar aos nossos olhos pela determinação do âmbito da obrigação a que se vinculou o devedor. Só a análise desse âmbito será de molde, em harmonia com a ideia de que o §287 BGB não é fonte de novos deveres (e, portanto, com a ideia de que o artigo 800.º CC não é, também, fonte de novos deveres), a esclarecer o decidente no caso concreto.

[44] A este propósito, cf. Hugo Natoli, L'attuatione del rapporto obbligatorio (appunti delle lesioni), tomo II, 2ª ed., Milano, 1967, 96-99, *apud* Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", 80 s. O autor considera que não se deve falar, em rigor, de uma responsabilidade objetiva, por se exigir a culpa do auxiliar. Apenas sucede que o facto do terceiro é imputável ao devedor como *causa causae*, o que afeta não a culpa, mas o nexo causal.

Refira-se, porém, que o nosso entendimento olha para o problema do ponto de vista da imputação e não do ponto de vista da causalidade.

[45] Para um elenco das possíveis justificações que vão sendo avançadas para a solução contida no artigo 800.º CC, cf. Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", 81: necessidades práticas económico-sociais que se manifestam na necessidade de responderem pelos riscos da atividade aqueles que dela tiram proveitos; garantia contra a eventual insolvência dos auxiliares; extraneidade do credor relativamente à escolha dos auxiliares; presunção de culpa *in viligando* ou *in elegendo*; poder de prevenção do perigo; exigência de uma garantia tacitamente prestada pelo devedor ao credor.

Para um elenco de outros possíveis fundamentos, cf. Pedro Múrias, "A responsabilidade por actos de auxiliares e o entendimento dualista da responsabilidade civil", 208 s.: ideia de confiança; ideia de responsabilidade pelo próprio círculo de vida; benefício que o devedor terá ao alargar as suas possibilidades de ação (e, assim, de lucro); necessidade funcional do tráfico negocial. O autor mostra-se crítico de todas estas justificações.

V., igualmente, Ernst von Caemmerer, "Verschulden von Erfüllungsgehilfen", 39 s.; Karl Larenz, *Lehrbuch des Schuldrechts*, 297 s.

[46] Cf., num sentido próximo, Pedro Múrias, "A responsabilidade por actos de auxiliares e o entendimento dualista da responsabilidade civil", *Revista da Faculdade de Direito da Universidade de Lisboa*, vol. 37, n.º1, 1996, 211. O autor considera que a lei estabelece inúmeras limitações ao devedor que pretenda exonerar-se dos seus deveres ou fazer perigar os fins de alguns deles através da intervenção de terceiros e considera que nesse grupo de normas se integra o artigo 800.º CC. No fundo, o fundamento do artigo 800.º passa nela tutela do credor, que não se vê assim privado de garantias por ato livre do titular do dever. Para o autor, não será, portanto, necessário recorrer a outra ordem de razões. O artigo "colhe a sua plena fundamentação na existência de um qualquer dever e na necessidade sentida pelo ordenamento de assegurar a obtenção das finalidades prosseguidas pela atribuição desse dever perante a introdução

ção do auxiliar pelo devedor como justificativa da disciplina normativa contida no artigo 800.º CC, aproximando a solução da plasmada no artigo 500.º CC, perde-se por completo se tivermos em conta os representantes legais, por cujos atos também responde o património do devedor[47]. Aproximamo-nos, assim, dos autores que sublinham que a intencionalidade do preceito não é alargar o âmbito da responsabilidade do devedor, fazendo-o assumir o risco de utilização de auxiliares. Na verdade, do que se trata é de fazer o devedor responder como se fosse ele próprio a atuar[48].

A intencionalidade normativa que foi encontrada para o artigo 800.º CC — responsabilização direta do devedor, por ser

de um terceiro no âmbito do seu cumprimento". Como veremos o autor extrai, a partir deste fundamento, conclusões que não subscrevemos. Por outro lado, em vez de se cingir aos deveres de tipo obrigacional, aloja no âmbito de relevância do preceito qualquer dever. Estes os dois pontos de dissenso em relação a Pedro Múrias, que a seu tempo densificaremos.

[47] Repare-se que Maria Victória Rocha explicita que, no tocante à responsabilidade do devedor pelos atos dos representantes legais, se os efeitos da atuação destes se projetam na esfera do incapaz, é justo que seja o património dele a suportar as consequências dessa atuação. *V.* Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", 79, n. 131.

Sobre a questão dos representantes legais, cf. Kurt Ballerstedt, "Zur Haftung für Culpa in contrahendo bei Geschäftsab-schlu durch Stellvertreter", *Archiv für die civilistische Praxis*, 151, 1950/1, 501 s.

[48] Cf. Ernst von Caemmerer, "Verschulden von Erfüllungsgehilfen", 39.

V., igualmente, Vaz Serra, "Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos", 269 s.

Para outros desenvolvimentos, cf. Mafalda Miranda Barbosa, "Acerca da aplicação do artigo 800.º CC aos ilícitos extracontratuais — breve apontamento", *O direito*, ano 147.º-III, 2015

ele o obrigado perante o credor, tratando-se o ato do auxiliar como um ato dele próprio — tem consequências ao nível da definição dos pressupostos de mobilização do regime.

Os autores costumam, a este propósito, apontar quatro requisitos para a procedência de uma pretensão indemnizatória fundada no artigo 800.º CC: a existência de uma obrigação; a relação entre o devedor e o terceiro utilizado no cumprimento; a atuação do terceiro no cumprimento[49]; e a atuação do auxiliar[50].

Ora, qualquer um destes pressupostos tem de ser densificado à luz do recorte intencional anteriormente desenhado. Por isso, embora a lei não indique expressamente que a atuação do auxiliar tem de ocorrer no cumprimento da obrigação, a doutrina tem reforçado tal entendimento, afirmando que o devedor apenas é responsável pelos atos praticados no cumprimento das obrigações e não pelos atos praticados por ocasião

[49] Segundo a maioria da doutrina, não se aplica, então, o artigo 800.º nos casos em que não está em causa o auxílio ao cumprimento, ou seja, nos casos em que os danos foram causados por terceiros a quem o devedor facultou o uso ou gozo da coisa pertencente ao credor. Neste caso, aplicar-se-ia o artigo 1044.º CC. Cf. Antunes Varela, *Das obrigações*, II, 103, n.2; M. Carneiro da Frada, *Contrato*, 217. Em sentido contrário, Pedro Múrias, "A responsabilidade por actos de auxiliares e o entendimento dualista da responsabilidade civil", 206, considerando que o artigo 1044.º é uma concretização do artigo 800.º CC.

Note-se que, nestas situações, estar-se-á, de facto, diante de uma hipótese de responsabilidade contratual. Basta pensar que entre os deveres de proteção resultantes do contrato, por via da boa-fé, se inscreva o dever de salvaguarda da propriedade alheia. A aplicação ou não do artigo 1044.º para além das hipóteses de locação ficará dependente de se poder ou não reconduzir a lesão verificada ao núcleo de relevância obrigacional.

[50] Cf. Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", 83 s.; Maria da Graça Trigo, *Responsabilidade civil delitual*, 241 s.

do cumprimento ou com relação indireta com o mesmo[51]. Estamos em crer, no entanto, que não podemos estabelecer, aqui, o paralelo com os problemas patenteados pelo artigo 500.º CC. Na verdade, se diante da necessidade de densificar o conceito de *exercício das funções*, o jurista se confronta com dificuldades imputacionais evidentes, ao nível do artigo 800.º CC somos desonerados da tarefa na medida em que a responsabilidade é balizada, *a priori*, pelos deveres que entretecem a relação obrigacional. Por isso, o nódulo problemático agigantar-se-á não diante da violação dos deveres de prestação, mas diante da violação dos deveres acessórios e dos deveres de conduta[52]-[53].

[51] Maria da Graça Trigo, *Responsabilidade civil delitual*, 241 s.; Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", 94; M. Carneiro da Frada, *Contrato*, 251.

[52] De notar, porém, que a dificuldade ultrapassa o âmbito de relevância do artigo 800.º CC. Na verdade, este problema surge paredes-meias com aquele outro que passa por saber se, mesmo quando a atuação é própria do devedor, a violação de deveres de conduta origina responsabilidade contratual ou não.

Sobre o ponto, cf. Carneiro da Frada, *Contrato*, onde o autor defende a existência de uma terceira via de responsabilidade civil. Veja-se, também, Mafalda Miranda Barbosa, "O problema da integração das lacunas contratuais à luz de considerações de carácter metodológico — algumas reflexões" e *Liberdade versus responsabilidade*, com uma posição diversa. Para outros desenvolvimentos, cf. Mafalda Miranda Barbosa, *Lições de responsabilidade civil*, Princípia, 2017.

A este propósito, *v.*, igualmente, Carneiro da Frada, *Contrato*, 154 s. e 169 s., considerando que o dano produzido por ocasião do cumprimento é um risco não típico e sensivelmente agravado pela entrada numa relação contratual. No fundo, embora o autor não reconduza todos os deveres de conduta à relação contratual, importa sublinhar que é ainda a economia negocial traçada pelas partes que permite solucionar o problema que temos em mãos.

[53] Sobre o ponto, cf. Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", 93, considerando que a expressão *no cumprimento* deve ser entendida como abrangendo a relação obrigacional no sentido de relação obrigacional complexa. No tocante aos deveres acessórios de conduta, a autora esclarece que a jurisprudência alemã parte do critério da existência ou não de uma conexão íntima entre a atividade danosa e a tarefa de que o auxiliar foi encarregado pelo devedor, tornando-se, por isso, necessário que haja uma interferência do terceiro nos bens do credor em virtude da especial relação de confiança entre credor e devedor. A autora acaba por fazer apelo a uma ideia de causalidade adequada a este nível.

Duas notas se impõem a este ensejo.

Em primeiro lugar, chamamos a atenção para a improcedência do critério da causalidade adequada, em geral, e em particular. Em segundo lugar, importa esclarecer que o sentido imputacional que se procura delinear há-de ser encontrado por referência à obrigação que o devedor assumiu. No fundo, o exercício que se terá de levar a cabo passa por questionar se, atuando daquela forma, o devedor seria ou não responsabilizado, por via da responsabilidade contratual.

Sobre o ponto, cf., ainda, Pedro Múrias, "A responsabilidade por actos de auxiliares e o entendimento dualista da responsabilidade civil", 204 s. O autor considera que devemos questionar, no tocante aos casos em que existe a violação de deveres de proteção, por ocasião do cumprimento, "se tivesse o ato sido praticado pelo devedor, ele responderia obrigacionalmente? Se sim, responde também agora pelo seu auxiliar. E não se diga que assim dispara o risco de responsabilidade para o devedor (...). O critério, seguido pela doutrina maioritária, dos *interesses ligados à relação contratual*, para determinar o quadro dos atos do auxiliar por que o devedor responderia, iria excluir a responsabilidade do relojoeiro cujo aprendiz partisse um relógio, atirando-o, em fúria, à cabeça do seu mestre, quando é patente que sem a relação contratual nunca o aprendiz teria a possibilidade de tocar no relógio, quanto mais de parti-lo". Concordamos com a solução patenteada pelo autor. Divergimos, contudo, nas conclusões a que chega. Na verdade, Pedro Múrias, considerando não estar aqui a violação de um dever contratualmente assumido, entende que estamos diante de uma responsabilidade que se funda num dever genérico de respeito pelos direitos absolutos, razão bastante para o autor não conseguir, em termos normativo-intencionais, distanciar o artigo 800.º, que aqui chama à colação, do artigo 500.º CC. Dá, portanto, um passo em frente no sentido da defesa de uma posição

Também o pressuposto da culpa deve ser compreendido a esta luz. Se a responsabilidade do terceiro auxiliar é tida como responsabilidade do próprio devedor, então deve entender-se que, uma vez excluída a culpa do primeiro, se exclui concomitantemente a responsabilidade do segundo[54]-[55].

monista em matéria de modalidades ressarcitórias. Pelo contrário, consideramos que o relojoeiro do exemplo de escola, ao assumir a obrigação principal de reparação do relógio, assume também o dever de guarda da coisa, pelo que responderá ao nível obrigacional pelo dano que ocorreu.

[54] Neste sentido, cf. Antunes Varela, *Das obrigações*, II, 103 s.

Ressalvam-se, contudo, as hipóteses em que o devedor agiu com culpa, na escolha do auxiliar.

Para outros entendimentos acerca do problema, *vide*, novamente, Carneiro da Frada, "A responsabilidade objetiva por facto de outrem face à distinção entre responsabilidade obrigacional e aquiliana", 303; Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", 97 s.; Maria da Graça Trigo, *Responsabilidade civil delitual*, 246 s. (questionando, designadamente, como poderemos aferir a culpa do auxiliar se ele não está vinculado por nenhuma obrigação).

[55] Outros problemas são também abordados pela doutrina a este nível. Assim, por exemplo, tem-se colocado a questão de saber se podem ser equiparados aos auxiliares as máquinas, quando o erro em que incorrem não se traduza num erro de programação. Sobre o ponto, cf. Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", 82 s.

Também se indaga em que medida a escolha do terceiro feita pelo credor pode ter consequências ao nível da exclusão da responsabilidade do devedor. Sobre o ponto, cf. Maria Victória Rocha, "A imputação objectiva na responsabilidade contratual", 88 s. Sublinha a autora que, se o terceiro surge como um colaborador do credor, exclui-se a responsabilidade do devedor. O mesmo não sucederá se o terceiro for escolhido entre os colaboradores do devedor. *Vide*, igualmente, Vaz Serra, "Responsabilidade do devedor pelos actos dos auxiliares, dos representantes legais ou dos substitutos", 267 s.

Quer isto dizer — com o caráter necessariamente sincopado que estas considerações denotam — que será o âmbito da obrigação previamente assumida pelo devedor que demarcará o âmbito da responsabilidade do devedor por via do artigo 800.º CC, pelo que se pode afirmar que imprescindível a este nível é que haja uma obrigação em sentido técnico, sem a qual, aliás, não existiria sequer um devedor. No fundo, a chamada à colação do regime da responsabilidade contratual, a este nível, só é possível quando a legitimação para o tratamento de dados pessoais seja negocial. Se por esta via se consegue responsabilizar o *controller*, pelos atos dos subcontratantes (e mesmo dos originários *processors que, posteriormente, se convolam em controllers*), nem por isso se garante a afirmação da responsabilidade do subcontratante.

Mas, se este é responsável extracontratualmente, pode sê-lo, também, contratualmente. Para tanto, haverá que se configurar o contrato celebrado entre o responsável pelo tratamento dos dados e o subcontratante como um contrato com eficácia de proteção para terceiros[56]. No âmbito de proteção do contrato incluir-se-iam alguns terceiros, que não poderiam exigir a prestação do devedor, mas se poderiam tornar credores

[56] Menezes Cordeiro, *Da boa fé no direito civil*, Almedina, 2001, 617 s.; Sinde Monteiro, *Responsabilidade por conselhos, recomendações e informações*, Almedina, Coimbra, 1989, 518 a 535 ; e C.A. Mota Pinto, *Cessão da posição contratual*, Atlântida Editora, Coimbra, 1970, 419 a 426; Larenz, "Entwicklungstendenzen der heutigen Zivilrechtsdogmatik", *Juristenzeitung*, 1962, 105 s.; Carneiro da Frada, , "Os deveres ditos acessórios e o arrendamento", *Revista da Ordem dos Advogados*, ano 73, 2013, 287; Mafalda Miranda Barbosa, "Arrendamento, responsabilidade civil e terceiros", *Estudos de Direito do Consumidor*, 12, 2017, 75 s.

de uma pretensão indemnizatória contra ele[57]. Segundo Mota Pinto, "este círculo de terceiros não deverá ser imprevisível e abrange aquelas pessoas que, segundo a natureza da prestação, estão, duma forma em maior ou menor grau inevitável em contacto com ela, e que (...) estão de tal modo próximos do credor que este, em termos cognoscíveis pelo devedor, confia na segurança dessas pessoas tanto como na sua"[58]. Ora, parece-nos que, destinando-se o contrato celebrado entre o responsável pelos dados e o subcontratante do tratamento de dados de terceiros, o subcontratante (*processor*) não poderá deixar de ter em conta que a sua prestação pode afetar particularmente os interesses desses terceiros, pelo que estes se devem integrar na esfera de proteção do contrato.

Para tal configuração, o artigo 28.º RGPD acaba por nos oferecer um importante contributo. Dispõe o preceito que "o tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento", devendo conter referência aos elementos constantes no citado preceito.

[57] Cf. Mota Pinto, *Cessão da posição contratual*, 422.

[58] Mota Pinto, *Cessão da posição contratual*, 423.

3.3. O papel do encarregado de proteção de dados

A figura do encarregado de proteção de dados está prevista nos artigos 38.º s. RGPD, cabendo-lhe as funções previstas no artigo 39.º RGPD.

Nos termos do artigo 38.º/3 RGPD o responsável pelo tratamento e o subcontratante asseguram que o encarregado da proteção de dados não recebe instruções relativamente ao exercício das suas funções. Esta particularidade dita o afastamento, em relação a danos por eles causados, da possibilidade de o responsável pelos dados ser responsabilizado por via do artigo 500.º CC. Do mesmo modo, não estando em causa um auxiliar no cumprimento de uma obrigação, não é possível a responsabilização do *controller* nos termos do artigo 800.º CC.

O encarregado da proteção de dados poderá ser responsabilizado em face do titular dos dados, por violação dos deveres que lhe são impostos no quadro regulamentar. Colocar-se-ão, é certo, problemas no tocante à imputação objetiva, na medida em que em nenhuma circunstância o fato lesivo dos dados é protagonizado pelo próprio.

Contudo, ao assumir as suas funções, assume concomitantemente uma esfera de risco, de tal modo que, se violar algum desses deveres a primitiva esfera de *responsabilidade pelo outro* convola-se numa *esfera de responsabilidade perante o outro*, a permitir erigir os contornos externos de uma imputação, para a qual se convocará posteriormente o necessário cotejo com a esfera de risco do *controller* e, eventualmente, do *processor*.

Este cotejo entre a esfera de responsabilidade do *controller* e outras esferas de risco torna-se, aliás, imprescindível por referência a qualquer situação problemática, por só por

meio dela ser possível chegar a uma conclusão fundada acerca da imputação objetiva e, portanto, acerca da própria responsabilidade dos sujeitos envolvidos.

3.4. A eventual responsabilidade de terceiros e a responsabilidade do controller pelos seus atos

a) O âmbito de proteção do direito. A relação de interioridade constitutiva e o problema da imputação de lesão de determinadas lesões ao controller

Independentemente das concretas diferenças de regime que se possam denotar entre o regime de proteção de dados em vigor até agora e o novo regulamento de proteção de dados, é inequívoco o papel central que o consentimento ocupa a este nível. Na verdade, ele, devendo ser informado, específico, livre e podendo ser revogado a todo o tempo, funciona como condição de licitude da recolha e tratamento de dados. Compreendem-se, portanto, as características que deve revestir. Se em causa está uma autorização do titular dos dados para a sua utilização por terceiros, então, ele só poderá ser válido se o sujeito tiver exata noção do alcance do ato que está a praticar. Daí a importância dos deveres de informação a que nos referimos *supra*. Mas daí, também, a importância vital da ligação entre o consentimento e as finalidades do tratamento de dados. A este propósito, Alexandre Sousa Pinheiro esclarece que "o consentimento válido para um tratamento implica o conhecimento dos fins a que se destina a recolha", pois, caso contrário, "a declaração de vontade mostra-se oca e destituída de conexão

com o tratamento de dados"[59]. É nesta relação *consentimento-finalidade* que o autor baseia a ideia de autodeterminação informacional.

A proteção de dados poderia autonomizar-se como "uma forma de concretização da autodeterminação informacional", ou seja, "enquanto a proteção de dados é pensada como uma garantia, o seu fundamento, ou seja, a autodeterminação informacional, exprime-se como uma liberdade"[60]. No fundo, "a autodeterminação informacional reveste a natureza de posição jurídica complexa, abrangendo elementos próprios das diferentes posições ativas (direitos, liberdades, garantias, poderes) que compõem os direitos fundamentais"[61].

Simplesmente, como o próprio autor reconhece, "o consentimento [em que aquela autodeterminação se vem a pro-

[59] Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 806. O autor acrescenta que se deve exigir uma definição clara e completa das finalidades, não sendo admissíveis meras referências a objetivos ou grandes metas. Nas suas palavras, "não são admissíveis disposições em branco, dada a sua incompatibilidade com a autodeterminação informacional e o perigo de se proceder a recolhas no vazio". Mais esclarece que, nos casos em que a finalidade tem de ser definida em termos mais amplos (por exemplo, por motivos de investigação criminal de largo espetro), se exige uma aplicação estrita do princípio da proporcionalidade.

Para um elenco dos princípios subjacentes à proteção de dados, cf. Margarida Oliveira, *A proteção de dados pessoais nas comunicações eletrónicas: o papel da CNPD e da ANACOM*, UCP, 2015, 28 s., falando de princípio da transparência, de princípio da lealdade, licitude e boa-fé, princípio do consentimento, princípio da finalidade, princípio da proporcionalidade e princípio da limitação do prazo de conservação.

[60] Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 805.

[61] Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 805.

jetar e a manifestar] é superado por razões contratuais, para o cumprimento de obrigações legais, para a proteção de interesses vitais do titular dos dados quando se encontre incapaz de o prestar e quando estejam em causa missões de interesse público ou relativas ao exercício de uma atividade pública"[62].

Diríamos mais: com o novo traçado legal, imposto pelo Regulamento europeu, ao colocar-se o consentimento em pé de igualdade com outros fundamentos da licitude da recolha e tratamento de dados, a autonomia de que se cura não poderá ser vista como o objeto da tutela, mas como um pilar fundamental para o exercício de outro bem jurídico que se protege a este nível. No fundo, e dito de uma forma mais direta, o consentimento, que corporiza a autonomia, surge, a este nível, como uma forma de afastar a ilicitude de um atentado não contra a própria autonomia que se exerce, mas contra um outro bem jurídico. Isso explica que, quando não haja consentimento (ou independentemente de o haver ou não), possa existir um tratamento de dados válido, atenta a ponderação de bens jurídicos que é feita pelo legislador.

Tendo a sensibilidade para o reconhecer, Alexandre de Sousa Pinheiro acaba por defender que a proteção de dados "deve ser integrada num direito de maior latitude", o direito à identidade informacional[63]. Este seria um "direito de personalidade, na medida em que protege um bem da personalidade composto por várias posições jurídicas"[64].

[62] Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 809.

[63] Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 810. Este parece ser, aliás, o cerne da sua dissertação de doutoramento.

[64] Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 777.

Não duvidamos, na verdade, que o direito envolvido a este nível seja um direito de personalidade. Não só está em causa a proteção de bens integrantes da pessoa, como a estrutura dos outros direitos que o ordenamento jurídico foi forjando (designadamente dos direitos reais e dos direitos de crédito) não é apta a assimilar a relevância da posição jurídica subjetiva em questão. Simplesmente, não basta considerar que existe um direito de personalidade, sendo imprescindível recortar, dentro dos diversos bens, elementos e refrações da personalidade humana, o seu concreto objeto. Ora, é neste ponto que temos dúvidas em autonomizar um direito à identidade informacional.

Em primeiro lugar, se é certo que existe um direito à identidade no quadro mais alargado do direito geral de personalidade[65], ele acaba por ter de ser analisado por referência a múltiplos elementos que o integram. A este propósito, Capelo de Sousa explica que "o bem da identidade reside (...) na própria ligação de correspondência ou identidade do homem consigo mesmo e está pois ligado a profundas necessidades humanas, a ponto de o teor da convivência humana depender da sua salvaguarda em termos de plena reciprocidade. Daí que (...) o direito tutele como bens jurídicos quer a ontologia da identidade humana quer o seu reflexo lógico ou formal ao nível do seu reconhecimento social, situando cada homem como centro autónomo de interesses, reconhecendo-lhes o seu particular modo de ser e de se afirmar e impondo aos outros o reconhecimento da sua identidade, v.g. de modo a que as referências a cada homem respeitem a sua identidade ontológica"[66]. Continua o

[65] Cf., quanto ao ponto, R. Capelo de Sousa, *O direito geral de personalidade*, Coimbra Editora, Coimbra, 1995, 244 s.

[66] R. Capelo de Sousa, *O direito geral de personalidade*, 245.

autor, dizendo que "o interesse jurídico da identidade humana é atingido não só nos casos em que os elementos ou sinais de identidade sejam falsificados, contrafeitos ou desviados dos fins próprios do respetivo titular, mas também nos casos em que a representação da pessoa não seja exata por mera omissão ou insuficiência dos elementos ou sinais retratados"[67]. E acrescenta que "a tutela juscivilística da identidade humana incide desde logo sobre a configuração somático-psíquica de cada indivíduo, particularmente sobre a sua imagem física, os seus gestos, a sua voz, a sua escrita e o seu retrato moral. Mas recai também sobre os termos da inserção sócio-ambiental de cada homem, maxime sobre a sua imagem de vida, a sua história pessoal, o seu decoro, a sua reputação ou bom nome, o seu crédito, a sua identidade sexual, familiar, racial, linguística, política, religiosa e cultural" e ainda sobre "os próprios sinais sociais de identificação humana, quer principais, como o nome e o pseudónimo, quer acessórios, como a filiação reconhecida, o estado civil, a naturalidade e o domicílio que (...) integram para certos fins o conteúdo do bem personalístico da identidade"[68]. Significa isto que o direito à identidade se sobrepõe a outros direitos ou bens da personalidade, razão pela qual pode1\\ríamos evidenciar que, ao nível da proteção de dados, está afinal em causa a tutela de todos eles. Não haveria, assim, razão para — e porque já foi suficientemente autonomizado pelo ordenamento jurídico — não considerar, a propósito da proteção de dados, direitos como o direito à imagem, o direito à voz, o direito ao nome, o direito ao crédito, entre outros.

[67] R. Capelo de Sousa, *O direito geral de personalidade*, 246.

[68] R. Capelo de Sousa, *O direito geral de personalidade*, 248 s.

Por outro lado, e mais importante, o direito à identidade pessoal — nas suas diversas vertentes — só é lesado quando haja omissões, deturpações ou usurpações, ao ponto de alguns autores o reconhecerem como um direito à verdade pessoal[69]. Ora, isto significa, por um lado, que a simples utilização não lícita de dados não põe em causa o direito à identidade pessoal e, por outro lado, que, quando tal ocorra, a partir do uso indevido de dados pessoais, outros bens da personalidade podem ser afetados, não se percebendo por que razão é que se privilegia a identidade em detrimento da privacidade, da imagem ou mesmo da igualdade.

A civilística portuguesa, aliás, tem tratado do problema da proteção de dados a propósito da privacidade[70], ou concretização do direito à privacidade[71] ou como refração do conteúdo da privacidade, enquanto elemento integrador do objeto do direito geral de personalidade[72], o que não impede que al-

[69] Cf. Orlando de Carvalho, *Teoria Geral do Direito Civil, Sumários Desenvolvidos*, Centelha, Coimbra, 1981, 16 s.; Orlando de Carvalho, *Teoria Geral do Direito Civil. Relatório sobre o programa, o conteúdo e o método de ensino*, Coimbra, 1976, 43 s.

[70] Cf. Pedro Pais de Vasconcelos, "Proteção de dados pessoais e direito à privacidade", *Direito da Sociedade da Informação*, I, Coimbra Editora, Coimbra, 1999, 249; A. Menezes Cordeiro, *Tratado de Direito Civil Português*, I, *Parte Geral*, tomo III, Almedina, Coimbra, 2004, 90, e *Tratado de Direito Civil*, IV, Almedina, Coimbra, 2007, 254 s.; R. Capelo de Sousa, *O direito geral de personalidade*, 318 s.

Veja-se, quanto ao ponto, Herminia Campuzano Tomé, *Vida privada y datos personales: su protección jurídica frente a la sociedade de la información*, Tecnos, Madrid, 2000 e, ainda, Flemming Moos, *Datensschutzrecht; schnell erfasst*, Springer, Berlin-Heidelberg, 2006

[71] Cf. A. Menezes Cordeiro, *Tratado de Direito Civil Português*, I, 90.

[72] Assim, R. Capelo de Sousa, *O direito geral de personalidade*, 318 s., considerando que "a reserva juscivilisticamente tutelada abrange não só o respeito

guns autores considerem que "a previsão do n.º1 do artigo 35.º

da intimidade da vida privada, em particular a intimidade da vida pessoal, familiar, doméstica, sentimental e sexual e inclusivamente os respetivos acontecimentos e trajetórias, mas ainda o respeito de outras camadas intermédias e periféricas da vida privada, como as reservas do domicílio e de lugares adjacentes, da correspondência e de outros meios de comunicação privada, dos dados pessoais informatizáveis, dos lazeres, dos rendimentos patrimoniais e de demais elementos privados da atividade profissional e económica, bem como (...) a própria reserva sobre a individualidade privada do homem no seu ser para si mesmo, v.g. sobre o seu direito a estar só e sobre os caracteres de acesso privado do seu corpo, da sua saúde, da sua sensibilidade e da sua estrutura intelectiva e volitiva".

O autor adere à teoria das três esferas, a propósito da privacidade. Para um olhar crítico, cf. Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 477 s.

Sobre a privacidade, enquanto objeto de um direito de personalidade, cf. ainda Paulo Mota Pinto, "Direito à reserva sobre a intimidade da vida privada", *Boletim da Faculdade de Direito*, 69, 1993, 479 s. O autor refere que, no quadro da privacidade, se incluem, então, aspetos como a identidade, dados pessoais, como a filiação, residência, o número de telefone, o estado de saúde, a vida conjugal, afetiva, os afetos, os ódios, os projetos de casamento, de divórcio, a vida do lar, o passado de uma pessoa, a sua situação financeira, as heranças que recebeu, os prémios de jogos que ganhou, os passatempos, os dias e locais de férias, as deformações físicas, os hábitos sexuais, entre muitos outros. No que tange às possíveis formas de violação do direito à privacidade, Paulo Mota Pinto fala-nos da entrada dos outro no domínio particular, a consubstanciar situações de violação do direito por intrusão (captação de fotografias e de filmes, gravações de voz, violação do domicílio, violação do segredo de correspondência ou telecomunicações, *vouyerismo*, casos de perseguição de outras pessoas), e das hipóteses de divulgação e revelação de dados da privacidade de outrem (relatos verbais, artigos de jornal ou revista difusão televisiva, comercialização de fotografias, publicação de um livro. Cf., ainda, A. Pinto Monteiro, Paulo Mota Pinto, Mafalda Miranda Barbosa, "A teoria geral do direito civil nos cem anos do Boletim da Faculdade de Direito", *Boletim da Faculdade de*

diz respeito mais propriamente ao bem da identidade da pessoa"[73]. Significa isto que, embora sublinhando a vertente da identidade, os autores não deixam — como nos parece que não devem deixar de fazer — de reconduzir para o cerne da proteção de dados a privacidade. É claro que esta não se mostra apta a explicar, por si só, a proteção de dados. O direito à proteção de dados ultrapassa o direito à privacidade, quanto ao seu âmbito de relevância[74]. E não é só a finalidade da consagração constitucional do direito — e posterior disciplina normativa instituída pelo legislador ordinário — que no-lo permitem afirmar, mas, igualmente, a perceção de que, em face da amplitude da noção de dados pessoais com que somos confrontados, podemos lidar com elementos que não se integram no núcleo estrito da privacidade, antes dizendo respeito ao conteúdo de outros direitos[75].

Direito (volume comemorativo do centenário do BFD), 91, 2015, 379-422, analisando este estudo do autor.

[73] R. Capelo de Sousa, *O direito geral de personalidade*, 322, n.812.

[74] Cf., a este propósito, Ac. STJ 16 de Outubro de 2014 (679/05.TAEVR.E2.S1)

Repare-se, a este nível, que, se ao abrigo da lei de proteção de dados os dados relativos à vida privada eram considerados dados sensíveis, tal deixa de ocorrer no quadro do regulamento europeu.

[75] Neste sentido, cf. Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 487, considerando que a proteção de dados se refere a qualquer informação relativa ao titular e que, por isso, tem autonomia em relação à proteção da vida privada e à privacidade.

Para uma consideração da ligação entre a privacidade e a proteção de dados, à época do surgimento da *Datenschutz*, na Alemanha, cf. Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 425. Refira-se, ainda, a comparação que o autor faz entre a *Datenschutz* e a *informational privacy*, que, correspondendo tendencialmente uma com a outra, não se relacionam em termos de pura identidade, já que há mais direitos associados à proteção de dados no caso europeu do que os aspetos informacionais contemplados pela

A proteção de dados pessoais afigura-se fundamental a diversos níveis. Em primeiro lugar, ela é vital para salvaguarda da identidade do sujeito, já que a divulgação de dados pessoais pode levar a que outros se apropriem daquela ou que haja dela uma deturpação, levando a que a pessoa seja confundida com outra ou que seja desvirtuada a verdade pessoal do sujeito; em segundo lugar, torna-se essencial para garantir que não se divulgam determinados elementos que, dizendo respeito ao sujeito, podem ser motivo de discriminação, sendo por isso determinante para a defesa da igualdade[76].; em terceiro lugar,

legislação americana. Com isto, o autor acaba por negar a perfeita ligação entre a privacidade e a proteção de dados.

Cf., igualmente, na obra citada pág. 771 s., distinguindo o direito à vida privada do direito à proteção de dados, evidenciando que a reserva que é definida por lei se estende a todos os dados individualizáveis e não apenas aos dados sensíveis.

Note-se, ademais, que a proteção de dados não esgota, atento o seu âmbito de relevância específico, a tutela que é dirigida aos direitos de personalidade nela envolvidos, designadamente a privacidade. Atente-se a este propósito na não aplicação do regime aos casos de recolha de dados pessoais para fins domésticos. Além disso, não está em causa a proteção de dados, quando seja o titular dos direitos de personalidade a divulgar os seus próprios dados pessoais — v.g. o problema das redes sociais. Sobre o ponto, cf. Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 814, considerando que aos dados que os utilizadores colocam numa rede social podem não se aplicar as regras de proteção de dados sobre o registo ou a autorização de tratamentos junto da entidade competente e sustentando que a qualidade de responsável pelo tratamento não pode ser alargado ao utilizador. O que não significa, obviamente, que as regras do regulamento não se apliquem às entidades que gerem os servidores onde estão alojadas as páginas pessoais dos sujeitos.

[76] Cf. Jorge Miranda/Rui de Medeiros, *Constituição Portuguesa Anotada*, tomo I, Coimbra Editora, Coimbra, 2005380. Sobre os dados ditos sensíveis, a que a Constituição se refere no artigo 35.º/3, consideram Jorge Miranda e Rui de Medeiros que são "os elementos de informação cujo tratamento informático,

ela é fulcral para a defesa da privacidade do sujeito, bem como para outros direitos de personalidade como a honra. Isto significa que a proteção de dados não tem como objeto último um direito de personalidade, mas vários direitos de personalidade do titular dos dados. E, por outro lado, significa que, e fazendo apelo a uma classificação jus-subjetiva muito cara ao constitucionalismo, estamos diante de um direito-garantia, uma guarda-avançada de certas posições jurídicas ativas.

Isto mesmo é percetível se pensarmos no problema do ponto do prisma da violação do direito. Entre nós, e porque a responsabilidade civil extracontratual se alicerça no modelo de Ihering, uma pretensão indemnizatória terá de, em princípio, fundar-se na violação de direitos absolutos ou na lesão de disposições legais de proteção de interesses alheios. Ora, deixando de lado a possibilidade de olharmos para algumas normas do regulamento europeu sobre proteção de dados como disposições daquele jaez[77], como já foi referido, haveria que identifi-

além de poder contender com a privacidade do sujeito, pode vir a dar origem a tratamentos desiguais ou discriminatórios" — cf. Jorge Miranda/Rui de Medeiros, *Constituição Portuguesa Anotada*, 386.

Sobre os dados sensíveis, para uma outra visão do problema, cf. Alexandre de Sousa Pinheiro, *Privacy e proteção de dados pessoais*, 487 s. e Spiros Simitis, "Sensitive datenzur Geschichte und Wirkung einer Fiktion", *Festschrift zum 65. Geburstag von M. Pedrazzini* (E. Bem/J. Nicolas Druey/Ernest A. Kramer/ Ivo Schwander, ed.), Stämpfli & Cie. AG., 1990, 469 s., também citado por Alexandre Sousa Pinheiro, considerando que não há dados pessoais inofensivos e que, por isso, não faz grande sentido a autonomização dos dados sensíveis, já que tudo depende do contexto global do tratamento que deles é feito.

Veja-se, igualmente, Anne Cammmilleri Subrenat/Claire Levallois-Barth, *Sensitive data protection in the European Union*, Bruylant, Bruxelles, 2007

[77] Mesmo olhando para essas normas, e portanto situando-nos na segunda modalidade de ilicitude delitual, seria importante a consideração dos interesses tutelados ao nível da proteção de dados, para efeitos de imputação.

car o direito absoluto violado. Se A recolher dados pessoais de B e, em preterição das regras de cuidado, permitir que C, com intenções malévolas, tenho a eles acesso, divulgando factos relativos à vida privada daquele, o problema que se terá de colocar é o de saber se, pese embora o comportamento do terceiro, a lesão do direito à privacidade pode ou não ser imputado a A. Do mesmo modo, se C tiver acesso a dados de identificação civil e fiscal de B e com isso se fizer passar por ele, causando-lhe sérios prejuízos, porque A violou determinadas regras de segurança no tratamento dos dados, o problema que teremos em mãos é o da recondução da lesão do direito à identidade ao comportamento de A. Finalmente, se A recolher ilicitamente dados sensíveis relativos a B e os transmitir a C que, fazendo uso deles, discrimina B num procedimento concursal, a questão que se terá de colocar é se a violação do direito à igualdade pode ou não ser imputada ao comportamento de A. Na verdade, não é possível dar uma resposta ao problema delitual se nos predicarmos exclusivamente na violação do direito à proteção os dados pessoais, porque, sendo circunscritos os sujeitos passivos das normas legais na matéria, tornar-se-ia impossível, por um lado, responsabilizar os terceiros com que nos confrontamos, e, por outro lado, encontrar um conteúdo útil para o direito que nos permitisse resolver o problema do preenchimento da responsabilidade, se ignorássemos os direitos de personalidade especiais preteridos. Ao mesmo tempo, se quiséssemos olhar para os referidos direitos, então teríamos de nos orientar pela própria fundamentação do direito, o que vem mostrar que a ilicitude se desvela, afinal, na lesão daqueles[78].

[78] O argumento avançado em texto leva pressuposto o problema da imputação objetiva e a cisão entre a causalidade fundamentadora da responsabilidade e a causalidade preenchedora da responsabilidade. sobre o ponto, cf. Mafalda Miranda Barbosa, *Do nexo de causalidade ao nexo de imputação. Contributo para a compreensão da natureza binária e personalística do requisito causal ao nível da responsabilidade civil extracontratual*, Princípia, 2013.

A este propósito uma última nota: se fundadamente virmos em algumas normas do regulamento europeu disposições legais de proteção de interesses alheios, isso não vai alterar o nosso raciocínio, embora possa alterar os termos da ponderação. Na verdade, ainda nesse caso, teremos de ter em atenção os interesses tutelados que, em última instância, se identificam com os direitos de personalidade referidos.

A vantagem de recorrer à segunda modalidade de ilicitude passa por se poder alargar o leque de interesses tutelados, podendo-se proteger aqueles que não correspondem à atribuição de uma posição dotada de eficácia *erga omnes*.

Se se conclui fundadamente que no âmbito de proteção dos dados pessoais se inclui a incolumidade dos diversos direitos que foram sendo referidos, outras situações podem-se afigurar mais problemáticas. Pense-se no caso em que A tem acesso aos dados pessoais de B, conseguindo, por meio deles, ter acesso à sua geolocalização, com o que encontra uma forma de lesar a sua integridade física. A questão que deve ser colocada — para se aferir da possível imputação daquela lesão ao *controller* — é, para além de se determinar se foram ou não violados determinados deveres por parte deste, aptos a alicerçar a convolação de uma primitiva esfera de *responsabilidade pelo outro* numa *responsabilidade perante o outro*, a de saber se esses deveres — predispostos à proteção dos dados — integram no seu âmbito de tutela a salvaguarda do direito à integridade física. No fundo, o mesmo é questionar se o direito à integridade física está ou não na base do direito à proteção de dados. Ora, parece-nos que a resposta não pode ser senão em sentido negativo, sob pena de o direito à proteção de dados se convolar num conceito voraz que tudo abarca. Mas o direito à segurança pessoal, enquanto elemento da personalidade, integrante do

direito geral de personalidade, pode já ser considerado a este nível, viabilizando-se a imputação.

b) Os deveres que oneram o controller

Não basta para que o *controller* possa ser responsabilizado por um comportamento de um terceiro que viole dados. Importa que haja, da sua parte, violação de determinados deveres em relação a eles. Sem isso não se desenha uma esfera de imputação à qual possa ser reconduzida a lesão.

A este nível há a considerar que o *controller* (bem como, aliás, o *processor*) deve adotar as medidas que correspondam um nível de segurança adequado, tendo em conta diversos fatores, quais sejam as técnicas disponíveis e mais avançadas, os custos de aplicação, os riscos envolvidos e a natureza dos dados.

Note-se que, para a aferição dos referidos riscos, deve ser feita uma avaliação de impacto da proteção de dados, sendo os resultados relevantes para a eleição das medidas a tomar. Se fundamente se concluir que o tratamento apresenta um elevado risco que não pode ser contornado por medidas adequadas, será necessário proceder à consulta da comissão nacional de proteção de dados antes de se proceder ao referido tratamento[79].

Esta autoridade de controlo deve ser notificada num determinado prazo depois de o responsável se ter percebido de que ocorreu uma violação de dados. Deve também informar o titular dos dados acerca dessa violação, de modo a que o mesmo possa tomar as providências adequadas.

[79] Cf. considerandos 83 s. RGPD.

Significa isto que a violação de qualquer destes deveres faz atualizar uma esfera de risco, convolando-a numa esfera de responsabilidade no sentido da *liability*, viabilizando a imputação[80].

[80] Há outras situações que, escapando ao traçado genérico do Regulamento, não deixam de ser relevantes, merecendo ponderação. Tomemos como exemplo uma aplicação que é disponibilizada pela empresa X através de uma plataforma de fornecimento de conteúdos digitais, vulgo designadas aplicações. Sendo certo que a referida plataforma (ou quem a detém) deve ser vista como um *controller em relação aos dados que recolhe para finalidades pré-determinadas, ela não é responsável pelo tratamento dos dados que sejam solicitados e recolhidos por cada uma das aplicações que possam ser descarregadas para dispositivos móveis. Simplesmente, uma vez alertada para o facto, poderá vir a ser responsabilizada se omitir qualquer ação apta a bloquear a aplicação ou evitar a sua disponibilização.*

A este propósito, cf. a lei das comunicações eletrónicas, embora não aplicável à proteção de dados.

A Lei n.º7/2004 estabelece a disciplina da responsabilidade dos prestadores de serviços em rede e dos prestadores intermediários, considerando que se aplica o regime comum. Já no que respeita aos prestadores intermédios de serviço em rede dispõe o artigo 12.º que eles não estão sujeitos a uma obrigação geral de vigilância sobre as informações que transmitem ou armazenam ou de investigação de eventuais ilícitos praticados no seu âmbito. Mas têm de cumprir uma série de obrigações constantes no artigo 13.º, nas condições ali previstas. Também o artigo 14.º estabelece que "o prestador intermediário de serviços que prossiga apenas a atividade de transmissão de informações em rede, ou de facultar o acesso a uma rede de comunicações, sem estar na origem da transmissão nem ter intervenção no conteúdo das mensagens transmitidas nem na seleção destas ou dos destinatários, é isento de toda a responsabilidade pelas informações transmitidas", e o artigo 15.º dispõe que "o prestador intermediário de serviços de transmissão de comunicações em rede que não tenha intervenção no conteúdo das mensagens transmitidas nem na seleção destas ou dos destinatários e respeite as condições de acesso à informação é isento de toda a responsabilidade pela armazenagem temporária e automática, exclusivamente para tornar mais eficaz e económica a transmissão posterior a nova solicitação

c) Acerca da responsabilidade do controller pelo ato de um terceiro: conclusão

Ainda que o terceiro não esteja, em concreto, vinculado pelos deveres impostos pelos diversos preceitos do regulamento geral de proteção de dados, sempre haveremos que afirmar que ele pode ser responsabilizado, no quadro da responsabilidade extracontratual, por violação de direitos de natureza absoluta.

Por seu turno, a determinação do direito concretamente lesado torna-se essencial quer para fundamentar a responsabilidade no tocante ao terceiro, quer para, tendo em conta os deveres preteridos pelo *controller*, perceber até que ponto a lesão sofrida lhe pode ou não ser imputada.

4. Conclusão

O Regulamento Geral de Proteção de Dados lida com o conceito de responsabilidade civil em duas aceções, no sentido da controlabilidade e no sentido da responsabilidade civil. Mas, embora se possam encontrar linhas de continuidade entre ambas as aceções, elas não se confundem. Para o perceber basta constatar que existem outras vias de responsabilização do sujeito para além da concreta violação da posição de *controller*.

de destinatários do serviço". Mas, haverá responsabilidade "se chegar ao conhecimento do prestador que a informação foi retirada da fonte originária ou o acesso tornado impossível ou ainda que um tribunal ou entidade administrativa com competência sobre o prestador que está na origem da informação ordenou essa remoção ou impossibilidade de acesso com exequibilidade imediata e o prestador não a retirar ou impossibilitar imediatamente o acesso". Por seu turno, o artigo 16.º/1 estabelece que "o prestador intermediário do serviço de armazenagem em servidor só é responsável, nos termos comuns, pela informação que armazena se tiver conhecimento de atividade ou informação cuja ilicitude for manifesta e não retirar ou impossibilitar logo o acesso a essa informação".

PROBLEMAS E DILEMAS DO SETOR SEGURADOR: O RGPD E O TRATAMENTO DE DADOS DE SAÚDE

Luís Poças[*]

Que particularmente ali lhe desse
Informação mui larga
Luís de Camões, *Os Lusíadas*, VII, 68, 1-2

The fewer data needed, the better the information.
Peter Drucker, *Management Tasks, Responsibilities and Practices*,
New York, Truman Talley Books & E. P. Dutton, 1986, pp. 334-335

[*] Doutor em Direito (Faculdade de Direito da Universidade de Lisboa). Diretor Jurídico da Una Seguros. Presidente da Comissão Técnica de Conduta de Mercado da APS. Membro do Conselho Diretivo da AIDA-Portugal (Associação Internacional de Direitos dos Seguros). Investigador Doutorado Integrado do DINAMIA'CET (ISCTE-IUL).

1 – Introdução

I - O presente texto versa sobre um tema candente, que afeta e preocupa a atividade seguradora: o da licitude do tratamento, pela mesma, de dados de saúde à luz do Regulamento Geral sobre a Proteção de Dados – Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Este Regulamento (doravante RGPD), que visa disciplinar uniformemente, entre os Estados-Membros, o tratamento de dados pessoais e a circulação dos mesmos, veio revogar a Diretiva 95/46/CE a partir de 25 de maio de 2018, tornando-se aplicável desde esta data no espaço da UE.

Neste quadro, o problema central identificado no presente texto prende-se com a aparente falta de uma fonte de licitude para o tratamento, por parte dos seguradores, de dados pessoais de saúde no âmbito dos contratos de seguro, sobretudo dos seguros de pessoas.

II - Em rigor, não se trata de um tema e de uma preocupação inteiramente novos. Já no âmbito de vigência da Lei n.º 67/98, de 26 de outubro (Lei da Proteção de Dados Pessoais – LPD) a problemática se suscitava e reclamava (sem grande sucesso, é certo) a atenção dos juristas. Entretanto, com a aprovação do RGPD – e no contexto de uma maior sofisticação e complexidade normativa, por um lado, e do temor gerado pela ameaça letal das coimas potenciais, por outro –, a matéria ganhou nova atualidade e alento, assumindo grande visibilidade no mundo segurador.

Tendo sido aberto, no Verão de 2017, um processo de consulta pública para aprovação de legislação nacional relativa ao RGPD, a Associação Portuguesa de Seguradores (APS) logo manifestou, no decurso de tal processo, especial preocupação pela temática objeto deste texto, em virtude dos perigos que a mesma comportava para a atividade seguradora, propondo soluções tendentes a suprir as gravosas consequências que resultariam de uma leitura formalista (e alheia ao mundo social) do RGPD.

Mais tarde, tendo o referido processo de consulta pública dado origem a um relatório final, depois objeto de alterações e consubstanciando a Proposta de Lei n.º 120/XIII/3.ª (Gov), foram igualmente encetadas diligências pela APS no sentido de alertar para o problema social, económico e jurídico iminente e para as soluções normativas passíveis de resolvê-lo. Aguarda-se, nesta data, o desfecho do processo legislativo, pelo que a análise empreendida ao longo do texto assentará estritamente no quadro normativo resultante do RGPD e nas implicações do mesmo se não se verificar uma intervenção cirúrgica e pertinente do legislador nacional.

III – Não obstante a relevância da temática, quer no anterior quadro da LPD, quer atualmente, no do RGPD, o estado da arte é bastante pobre num domínio que, atento o âmbito europeu de aplicação do tecido normativo, deveria preocupar, não apenas os seguradores nacionais, mas, igualmente, todo o setor segurador europeu.

Não obstante, talvez por falta de amadurecimento das análises ao novo regime ou pela expectativa de que o poder legislativo de cada Estado emende ainda a mão do legislador europeu, a verdade é que os parcos textos estrangeiros disponíveis sobre o impacto do RGPD no setor segurador não dão qualquer destaque (ou não fazem sequer menção) ao problema identificado[2].

[2] Cfr., por exemplo, Jean-François Henrotte e Fanny Coton, "L'impact du R.G.P.D. dans le secteur des assurances: Comment s'y conformer?", *Forum de l'Assurance*, n.º 185 (juin 2018), pp. 107-111.

Em Portugal, o panorama não é muito diferente, não se encontrando, nos escassos textos que afloram o reflexo do RGPD na atividade seguradora, referências à mencionada questão[3]. Pela nossa parte, tivemos oportunidade, aquando da investigação que deu suporte à nossa tese de doutoramento, de identificar alguns dos problemas que vieram a agudizar-se com o RGPD, tendo-os então apresentado e debatido com a mesma inquietação que assumimos hoje[4].

IV – O presente texto[5] começa por traçar um curto resumo do quadro legal que disciplina atualmente a proteção de dados, focando-se nos fundamentos de licitude para o tratamento dos mesmos (e, em particular, os respeitantes às categorias especiais de dados, entre as quais se contam os dados de saúde). Sublinhando a necessidade, para a atividade seguradora (e, em especial, para a gestão dos seguros de pessoas), do tratamento de dados de saúde, o texto equaciona o problema da aparente ausência de uma fonte de licitude que fundamente de forma clara esse tratamento. Seguidamente, é discutida a ineptidão do *consentimento* para legitimar o tratamento de dados de saúde no contexto da subscrição e execução de contratos de seguro, buscando, em alternativa, no quadro do RGPD, outras soluções normativas aptas a conferir licitude a esse tratamento, quer relativamente a seguros obrigatórios, quer aos facultativos. Sem prejuízo de se considerar que o RGPD contém já tais soluções de licitude, é discutida, como alternativa, a solução assente numa intervenção do legislador nacional.

2 – O quadro normativo da proteção de dados

2.1 – Enquadramento geral

I – Encontra-se largamente refletido em vários instrumentos de Direito internacional o direito à privacidade (*right to privacy* ou *right to be let alone*), consagrado nos EUA no início do séc. XX e posteriormente generalizado a outros ordenamentos[6]. A consagração deste direito é um produto dos tempos modernos, quer na medida em que a explosão demográfica veio colo-

[3] Cfr., por exemplo, Paula Ribeiro Alves, "Os desafios digitais no mercado segurador", *in* António Menezes Cordeiro, Ana Perestrelo de Oliveira e Diogo Pereira Duarte (Coords.), *Fintech – Desafios da Tecnologia Financeira*, Coimbra, Almedina, 2017, p. 44.

[4] Cfr. Luís Poças, *O Dever de Declaração Inicial do Risco no Contrato de Seguro*, Coimbra, Almedina, 2013, pp. 731-781 e, em especial, 843-877.

[5] Este texto tem por base a comunicação que tivemos o grato prazer de efetuar na Faculdade de Direito da Universidade de Coimbra, em 14 de abril de 2018. A mesma esteve inserida na Conferência – *Seguros, Seguradoras e o Novo Regulamento de Proteção de Dados*, organizada pelo Instituto de Direito Bancário, da Bolsa e dos Seguros, e pelo Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra. Mais recentemente, tivemos também oportunidade de publicar um pequeno artigo sobre o tema - cfr. Luís Poças, "O RGPD e os Seguros", *Revista APS,* n.º 2 (ano 2018), pp. 42-44.

[6] Cfr. o artigo 12.º da Declaração Universal dos Direitos do Homem (DUDH); o artigo 17.º do Pacto das Nações Unidas relativo aos Direitos Cívicos e Políticos do Homem; e o artigo 8.º da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais aprovada pelo Conselho da Europa. Por outro lado, nos termos do n.º 2 do artigo 16.º da Constituição da República Portuguesa (CRP), as disposições constitucionais e legais respeitantes a direitos fundamentais devem ser interpretados e integrados de harmonia com a DUDH. De resto, de acordo com o n.º 2 do artigo 8.º da CRP, quer o Pacto relativo aos Direitos Cívicos e Políticos, quer a Convenção Europeia dos Direitos do Homem, vigoram na ordem jurídica interna, em virtude da sua aprovação para ratificação (respetivamente, pelas Leis n.º 29/78, de 12 de junho, e n.º 65/78, de 13 de outubro).

cando os indivíduos em contacto próximo – o que impôs uma tutela do seu espaço íntimo – quer porque o desenvolvimento tecnológico recente veio a revelar-se especialmente intrusivo daquele espaço, potenciando a exposição ao olhar público e à curiosidade alheia, mas também à própria mercantilização do dado pessoal como utensílio de *marketing*[7].

Sem prejuízo do recente reconhecimento e autonomização de um *direito à autodeterminação de informação*, a proteção de dados pessoais filia-se, em grande medida, no referido direito à privacidade. Importa, em qualquer caso, enquadrar sumariamente a proteção de dados no âmbito do Direito europeu – de onde dimana o RGPD – e no próprio contexto do Direito interno português.

II – Em matéria de proteção de dados pessoais, e no âmbito do Direito da UE, releva (na sua versão consolidada), desde logo, o artigo 16.º do Tratado sobre o Funcionamento da União Europeia – TFUE (ex-artigo 286.º Tratado das Comunidades Europeias - TCE). Aí se dispõe, no respetivo n.º 1, que «todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito».

Por outro lado, estabelece o artigo 39.º do Tratado da União Europeia que «em conformidade com o artigo 16.º do TFUE e em derrogação do n.º 2 do mesmo artigo, o Conselho adota uma decisão que estabeleça as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação do presente capítulo, e à livre circulação desses dados» acrescentando que «a observância dessas normas fica sujeita ao controlo de autoridades independentes». É neste quadro que, em revogação da Diretiva 95/46/CE, veio a ser aprovado o RGPD[8].

III – No âmbito do nosso Direito interno, o RGPD corporiza a remissão para a lei, feita pelo n.º 2 do artigo 26.º da CRP, do estabelecimento de garantias efetivas contra a obtenção e utilização abusivas ou contrárias à dignidade humana (ou seja, que violem, designadamente, o direito à reserva da intimidade da vida privada), de informações relativas à pessoa e à família. O RGPD constitui, assim, um dos instrumentos legais de garantia do direito à reserva sobre a intimidade da vida privada (n.º 1 do artigo 26.º da CRP)[9].

[7] Cfr. Teodoro Bastos de Almeida, "O direito à privacidade e a proteção de dados genéticos: Uma perspetiva de direito comparado", *Boletim da Faculdade de Direito da Universidade de Coimbra*, Ano LXXIX (2003), pp. 376 ss.; Rita Amaral Cabral, "O direito à intimidade da vida privada (breve reflexão acerca do artigo 80.º do Código Civil)", *Estudos em Memória do Prof. Doutor Paulo Cunha*, Lisboa, Faculdade de Direito de Lisboa, 1989, pp. 385-386; Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra, Almedina, 2005, pp. 17 ss.; Januário Costa Gomes, "O problema da salvaguarda da privacidade antes e depois do computador", *Boletim do Ministério da Justiça*, n.º 319 (out. 1982), pp. 23 ss.; Paulo Mota Pinto, "O direito à reserva sobre a intimidade da vida privada", *Boletim da Faculdade de Direito da Universidade de Coimbra*, Ano LXIX (1993), pp. 512 ss. Entre a doutrina estrangeira, cfr., p. ex., Pierre Kayser, *La Protection de la Vie Privée*, 2ª Ed., Paris, Economica, 1990, pp. 4 ss.

[8] Sobre a história do processo político e legislativo que conduziu à aprovação do RGPD, cfr. Jorge Barros Mendes, "O novo regulamento de proteção de dados: as principais alterações", *Revista Portuguesa de Direito do Consumo (RPDC)*, n.º 89 (março 2017), pp. 12 ss.

[9] A tutela constitucional da reserva de intimidade da vida privada assenta na dignidade humana como valor fundamental em que se funda a República Portuguesa (artigo 1.º da CRP), e é também prosseguida pelos citados n.º 1, *in*

Da maior relevância para o tema que nos ocupa são também os n.ºs 2 a 6 do artigo 35.º da CRP, onde se consagra a proteção contra o tratamento de dados pessoais, no que é configurável como um autónomo *direito à autodeterminação sobre a informação*[10]. Com efeito, a relevância da proteção de dados pessoais, consagrada no referido artigo 35.º, não coincide nem se confunde com o direito à reserva da intimidade da vida privada, na medida em que nem todos os *dados pessoais* respeitam à esfera da vida privada e que o domínio da privacidade não se esgota na proteção de dados[11].

fine, e n.º 2 do artigo 26.º da CRP; pelo artigo 34.º; pelo n.º 8 do artigo 32.º; e pelo n.º 2 do artigo 268.º. Para além da aplicabilidade direta, por força do artigo 18.º da CRP, do direito fundamental à reserva da vida privada, o mesmo é também criminalmente tutelado (designadamente, pelo Capítulo VII do Título I do Livro II do Código Penal – *Dos crimes contra a reserva da vida privada* – artigos 190.º ss.) – cfr., desenvolvidamente, Helena Moniz, "Notas sobre a proteção de dados pessoais perante a informática (o caso especial dos dados pessoais relativos à saúde)", *Revista Portuguesa de Ciência Criminal,* Ano 7, n.º 2 (abr.jun. 1997), pp. 239 ss. Finalmente, estamos também perante um direito especial de personalidade, protegido pelos artigos 70.º e 80.º do Código Civil (doravante, CC), na medida em que a dignidade da pessoa humana requer uma margem de autonomia física e moral, de liberdade e de autodeterminação que, por seu turno, implicam a inviolabilidade da esfera pessoal de cada indivíduo. Neste contexto, a tutela legal dispensada à *vida privada*, como bem de personalidade, permite configurar a própria *privacidade* – enquanto esfera independente de liberdade individual – como valor juridicamente protegido – António Menezes Cordeiro, *Tratado de Direito Civil Português*, I, Tomo III, 2ª Ed., Coimbra, Almedina, 2007, p. 252.

[10] Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, *cit*., pp. 28-29.

[11] Teodoro Bastos de Almeida, "O direito à privacidade e a proteção de dados genéticos: Uma perspetiva de direito comparado", *cit*., pp. 390 ss.

IV – A tutela da vida privada tem por interesse subjacente o controlo sobre a informação pessoal, de caráter íntimo ou confidencial, bem como a subtração, quer à atenção alheia, quer ao acesso físico de outrem. Desta forma, quanto ao âmbito da tutela legal, a *reserva* veda, tanto a intromissão na vida privada íntima (*intrusion*), como a divulgação de factos da vida privada (*public disclosure of private facts*[12]), aspetos que traduzem dois direitos menores do titular da informação[13].

Já no quadro do direito à autodeterminação sobre a informação, que alguma doutrina autonomiza, como direito fundamental, com base no artigo 35.º da CRP, essa autodeterminação assumirá várias vertentes, como a do *habeas data* – ou seja, o direito de cada pessoa controlar e dispor dos dados que lhe digam respeito –, o direito à não difusão de dados pessoais, e o direito a uma tutela acrescida relativamente a categorias especiais de dados[14].

[12] Esta vertente é tutelada, designadamente, pelo sancionamento – disciplinar, civil e até penal – da quebra do sigilo: é o caso, p. ex., do segredo médico – Paulo Mota Pinto, "A proteção da vida privada e a Constituição", *Boletim da Faculdade de Direito da Universidade de Coimbra*, Ano LXXVI (2000), pp. 176-177.

[13] Teodoro Bastos de Almeida, "O direito à privacidade e a proteção de dados genéticos: Uma perspetiva de direito comparado", *cit*., pp. 393 ss.; Rita Amaral Cabral, "O direito à intimidade da vida privada (breve reflexão acerca do artigo 80.º do Código Civil)", *cit.,* pp. 403 ss.; Gomes Canotilho e Vital Moreira, *Constituição da República Portuguesa Anotada*, Vol. I, 4ª Ed., Coimbra, Coimbra Ed., 2007, p. 467; Paulo Mota Pinto, "O direito à reserva sobre a intimidade da vida privada", *cit*., pp. 508 e 533-534; Paulo Mota Pinto, "A proteção da vida privada e a Constituição", *cit*., pp. 164 e 169 ss. É esta, igualmente, a orientação do Tribunal Constitucional no que diz respeito ao âmbito do n.º 1 do artigo 26.º da CRP Paulo Mota Pinto, "A proteção da vida privada e a Constituição", *cit*., pp. 159 ss.

[14] Helena Moniz, "Notas sobre a proteção de dados pessoais perante a informática (o caso especial dos dados pessoais relativos à saúde)", *cit*., pp. 249

Traçada uma breve contextualização legal da proteção de dados – que apresenta ainda outras vertentes, como a da sua articulação com o Direito do consumo[15] –, importa que nos foquemos, em concreto, nos traços caracterizadores do RGPD. É esse o propósito da secção seguinte.

2.2 – Elementos principais do RGPD

I – Vários são os aspetos inovadores do RGPD face à Diretiva que vem revogar. Entre eles conta-se, desde logo, o alargamento do leque dos direitos dos titulares de dados. Com efeito, o titular dos dados assume um papel central na coerência interna do sistema RGPD, podendo falar-se de um autêntico apoderamento (*empowerment*) dos titulares sobre os seus dados – no sentido de que surgem amplamente reforçados os direitos dos mesmos e o inerente controlo sobre tais dados –, como um dos aspetos marcantes do RGPD[16].

Reflexamente ao amplo reforço dos direitos dos titulares, verifica-se, por um lado, um aumento dos deveres a cargo do responsável pelo tratamento (designadamente, quanto à segurança dos dados[17]) e, por outro lado, um alargamento dos poderes das autoridades de controlo. Associado a este, estabelece-se um aumento exponencial do limite máximo das coimas aplicáveis às contraordenações emergentes do Regulamento, a potenciar um ambiente de terror junto dos operadores económicos responsáveis pelo tratamento de dados[18]. Um outro aspeto relevante do RGPD traduz-se no alargamento do âmbito territorial da proteção de dados, abrangendo responsáveis pelo tratamento de países terceiros, não estabelecidos no espaço da UE[19].

II – Noutra vertente, o RGPD desloca a perspetiva, de uma *abordagem baseada nos direitos dos titulares*, para uma autêntica *abordagem baseada no risco*, de acordo com um princípio de responsabilidade (do responsável pelo tratamento)[20].

ss., e Januário Costa Gomes, "O problema da salvaguarda da privacidade antes e depois do computador", *cit.*, p. 49.

[15] Colocando em evidência a complementaridade entre o Direito do consumo e o Direito da proteção de dados pessoais, cfr. Natali Helberger, Frederik Zuiderveen Borgesius e Augustin Reyna, "The perfect match? A closer look at the relationship between EU consumer law and data protection law", *Common Market Law Review*, Vol. 54, n.º 5 (October 2017), pp. 1427-1466.

[16] Elena Gil González, *Big Data, Privacidad y Protección de Datos*, Madrid, Agencia Española de Protección de Datos, 2016, pp. 140 ss.; Javier Puyol Montero, "Los principios del derecho a la protección de datos", *in* José Luis Piñar Mañas (Dir.); María Álvarez Caro, Miguel Recio Gayo (Coord.), *Reglamento General de Protección de Datos: Hacia un Nuevo Modelo Europeo de Privacidad*, Madrid, Editorial Reus, 2016, p. 138; María Álvarez Caro, "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", *in* José Luis Piñar Mañas (Dir.); María Álvarez Caro, Miguel Recio Gayo (Coord.), *Reglamento General de Protección de Datos: Hacia un Nuevo Modelo Europeo de Privacidad*, Madrid, Editorial Reus, 2016, pp. 227-228. Dando também nota do papel central consagrado aos titulares dos dados na arquitetura do sistema RGPD, cfr. Mário Frota, "Dados pessoais – 'Quem os tem, chama-lhes seus'... Ou a salvaguarda de um património sensível em ordem à reserva da tutela da vida privada?", *Revista Portuguesa de Direito do Consumo*, n.º 89 (março 2017), p. 8.

[17] Sobre a segurança dos dados, cfr. Afonso Araújo Neto, "RGPD: uma revolução invisível", *Revista Portuguesa de Direito do Consumo*, n.º 89 (março 2017), pp. 35-42.

[18] Charles-Albert van Oldeneel, "Protection des données: le GDPR applicable depuis de 25 mai 2018!", *Bulletin des Assurances*, n.º 403-2 (2018), p. 287.

[19] Cfr. nºs 2 e 3 do artigo 3.º do RGPD. Sobre a problemática, cfr., desenvolvidamente, Merlin Gömann, "The new territorial scope of EU data protection law: deconstructing a revolutionary achievement", *Common Market Law Review*, Vol. 54, n.º 2 (abr. 2017), pp. 567-590.

[20] Charles-Albert van Oldeneel, "Protection des données: le GDPR applicable depuis de 25 mai 2018!", *cit.*, p. 288.

No quadro deste princípio, passa-se de um contexto em que o tratamento de dados estava sujeito a notificação ou autorização prévia da autoridade de controlo, para outro com base no qual o responsável pelo tratamento deve autonomamente assegurar a sua conformidade ao RGPD, documentando toda a sua atividade de tratamento e respondendo pelas quebras de conformidade verificadas.

III – A compreensão da lógica interna e alcance normativo do RGPD impõe, em qualquer caso, algum domínio sobre as respetivas noções-chave. Entre elas, assume particular relevância a de *dados pessoais*. Nos termos da alínea 1) do artigo 4.º do RGPD, os mesmos correspondem a *qualquer* «informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados")»[21]

Estamos, portanto, perante uma noção de um âmbito amplíssimo[22] [23].

[21] Acrescenta o preceito que «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».

[22] Esta definição provém das *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, da OCDE, de 1980. Sobre o sentido e alcance da definição, cfr. A. Barreto Menezes Cordeiro, "Dados pessoais: conceito, extensão e limites", *Revista de Direito Civil*, Ano III (2018), n.º 2, pp. 297-321. Estão em causa todas as informações relativas a pessoas singulares, sejam factuais ou subjetivas, físicas ou psicológicas, públicas ou privadas, individuais, familiares ou sociais, exatas ou inexatas, quer se trate de elementos de identificação, quer de atributos físicos, profissionais, económicos, académicos, sociais, quer mesmo de convicções ideológicas do mais variado teor, elementos de geolocalização, etc. Por outro lado, são qualificados como dados pessoais os que respeitem a uma pessoa diretamente identificada ou identificável (pelo

.Entre os dados pessoais destacam-se determinadas *categorias especiais*, que merecem um regime de tutela mais rigoroso. Aí se contam, como resulta do n.º 1 do artigo 9.º, os «dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como [...] dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, *dados relativos à saúde*[24] ou dados relativos à vida sexual ou orientação sexual de uma pessoa».

Também de amplitude vastíssima é a noção-chave de *tratamento de dados*. Nos termos da alínea 2) do artigo 4.º do RGPD, trata-se da «operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou intercone-

responsável pelo tratamento ou por terceiro), de acordo com um juízo de probabilidade razoável. *Idem*, pp. 312 ss.

[23] Alguma doutrina chama a atenção para o alargamento da noção de dados pessoais operado, da anterior Diretiva para o RGPD. Esse alargamento dá-se no sentido de se ir para além dos identificadores que permitem a associação ao nome do titular, abrangendo-se também os identificadores não associados a um nome (por exemplo, os *cookies*) – Ana Alves Leal, "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", *in* António Menezes Cordeiro, Ana Perestrelo de Oliveira e Diogo Pereira Duarte (Coords.), *Fintech – Desafios da Tecnologia Financeira*, Coimbra, Almedina, 2017, pp. 108-109.

[24] São precisamente os dados de saúde que merecerão enfoque especial ao longo do presente texto.

xão, a limitação, o apagamento ou a destruição»[25]. Neste quadro, *qualquer* contacto com dados pessoais alheios, ainda que passivo, configura uma operação de tratamento: se uma entidade entrar na posse de um dado alheio (recolha), está já a tratá-lo, outro tanto sucedendo quer conserve esse dado, quer o destrua.

O RGPD consagra um leque alargado de medidas visando a proteção da privacidade. Não obstante, a lógica normativa em que assenta a regulação do tratamento de dados apresenta-se, na sua essência, relativamente simples. Desde logo, os *titulares dos dados* pessoais são as pessoas singulares a quem os mesmos respeitam, sendo-lhes garantido um vasto conjunto de direitos sobre esses dados.

Por outro lado, os dados pessoais são confiados pelos titulares a entidades (designadas *responsáveis pelo tratamento*[26]) exclusivamente para *finalidades* de tratamento determinadas, explícitas e legítimas, por elas determinadas e que as mesmas

[25] María Arias Pou sublinha que a proteção de dados (quer no plano dos direitos dos titulares, quer dos deveres do responsável pelo tratamento) não se basta com a presença de dados pessoais, requerendo que haja *tratamento* dos mesmos – María Arias Pou, "Definiciones a efectos del Reglamento General de Protección de Datos", *in* José Luis Piñar Mañas (Dir.); María Álvarez Caro, Miguel Recio Gayo (Coord.), *Reglamento General de Protección de Datos: Hacia un Nuevo Modelo Europeo de Privacidad*, Madrid, Editorial Reus, 2016, pp. 119-120. Note-se, porém, que a noção – também ela amplíssima de tratamento (englobando operações como a simples recolha ou conservação) tornam, de algum modo, despicienda a observação da autora.

[26] Nos termos da alínea 7) do artigo 4.º do RGPD, é responsável pelo tratamento «a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais».

devem informar aos titulares[27]. Em qualquer caso, os dados pessoais apenas podem ser tratados se existir um fundamento que torne lícito esse tratamento em função das finalidades em causa, sendo o elenco de *fontes de licitude* definido pelo Regulamento. Neste contexto, cada finalidade de tratamento requer a sua própria fonte de licitude. Quando esta consista, por exemplo, no consentimento do titular dos dados, o mesmo tem de ser dado separadamente para cada finalidade que o requeira[28].

Por fim, as responsáveis pelo tratamento podem subcontratar outras entidades (entidades "subcontratantes"[29]) para tratarem dados por sua conta, assumindo, porém, a responsabilidade por tal tratamento.

2.3 – Os dados de saúde: delimitação de uma noção

I - Como vimos, os dados de saúde que se reportem a um titular identificado ou identificável são, não *apenas* dados pessoais, mas pertencem a uma categoria especial de dados, a merecer tutela reforçada do RGPD. Vejamos, porém, em maior detalhe, qual a noção de dados de saúde a considerar no âmbito do Regulamento.

Nos termos da alínea 15) do artigo 4.º do RGPD, são *dados relativos à saúde* os «dados pessoais relacionados com a saúde

[27] Cfr. alínea b) do n.º 1 do artigo 5.º do RGPD.

[28] Frédéric Lecomte, *Nouvelle Donne pour les Données: Le RGPD en Quelques Principes pour Être Prêt le 25 Mai 2018*, Paris, Fauves éditions, 2018, p. 34.

[29] Dispõe-se na alínea 8) do artigo 4.º do RGPD que é entidade subcontratante «uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes».

física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde».

Esta definição é melhor clarificada pelo Considerando 35 do RGPD, onde e lê que «deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro», acrescentando-se que «o que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*».

Também o Grupo do Artigo 29.º, refletiu sobre a matéria, considerando os dados de saúde um domínio complexo que propicia alguma incerteza jurídica entre os vários Estados-Membros. Neste quadro, considera o Grupo que os dados relativos à saúde se estendem, para além da informação produzida em contexto médico (doenças, incapacidades, diagnósticos, historial clínico, alergias, tratamentos), a informações como o QI, hábitos de consumo de tabaco ou álcool, de exercício físico ou dieta alimentar, bem como os dados gerados por equipamentos ou *apps* que, ainda que aparentemente inócuos no domínio da privacidade, possam, em conjugação com outros dados, fornecer informação sobre o estado de saúde, real ou potencial, do titular[30].

O sentido amplo da definição que vem sendo delimitada está, por outro lado, em sintonia com a jurisprudência do TJUE. No *caso Linqvist*, por exemplo, pode ler-se que «atendendo ao objeto desta diretiva [Diretiva 95/46], há que dar à expressão "dados relativos à saúde" utilizada no artigo 8.º, n.º 1, uma interpretação lata, de modo que inclua informações relativas a todos os aspetos, quer físicos quer psíquicos, da saúde de uma pessoa. Por conseguinte, [...] a indicação do facto de uma pessoa se ter lesionado num pé e estar com baixa por doença a meio tempo constitui um dado de carácter pessoal relativo à saúde»[31].

[30] Cfr. Article 29 Working Party, *Health Data in Apps and Devices*, 2015, disponível em http://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (consult. 27/08/2018). Como conclui o texto, «in summary, personal data are health data when: (1) the data are inherently/clearly medical data; (2) the data are raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person; (3) conclusions are drawn about a person's health status or health risk (irrespective of whether these conclusions are accurate or inaccurate, legitimate or illegitimate, or otherwise adequate or inadequate)» - *idem*, p. 5.

[31] Ac. TJUE de 06/11/2003 – (Proc. n.º C-101/01), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN (consult. 27/08/2018).

No mesmo sentido, e em harmonia com o referido acórdão, está a orientação da CNPD, que considera dados de saúde «não apenas aqueles que resultem do diagnóstico médico feito, mas todos aqueles que permitam apurá-lo, incluindo resultados de análises clínicas, imagens de exames radiológicos, imagens vídeo ou fotográficas que sirvam o mesmo fim»[32].

O mesmo sentido amplo encontra reflexo no Direito interno. Com efeito, o artigo 2.º da Lei n.º 12/2005, de 26/01, considera, para efeitos desse diploma, que a informação de saúde abrange todo o tipo de informação direta ou indiretamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e a sua história clínica e familiar[33].

II – Embora se trate de uma subcategoria de dados de saúde[34], os dados genéticos surgem autonomizados entre as categorias especiais de dados elencadas no artigo 9.º do RGPD. Nos termos da alínea 13) do artigo 4.º, são *dados genéticos* os «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

[32] Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, *cit*., p. 91.

[33] Quanto ao âmbito do segredo médico, será de entender que este abrange o resultado de exames e análises clínicas, diagnósticos efetuados e tratamentos prescritos a uma pessoa, bem como o dia, hora e local em que o paciente foi observado pelo médico, mas já não a própria identidade do paciente - Helena Moniz, "Segredo Médico", *Revista Portuguesa de Ciência Criminal*, Ano X, n.º 4 (out.-dez. 2000), p. 640.

[34] Cecilia Álvarez Rigaudias, "Tratamiento de datos de salud", *in* José Luis Piñar Mañas (Dir.); María Álvarez Caro, Miguel Recio Gayo (Coord.), *Reglamento General de Protección de Datos: Hacia un Nuevo Modelo Europeo de Privacidad*, Madrid, Editorial Reus, 2016, p. 174.

singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa».

III – Tem sido apontada a existência de vários círculos concêntricos de *reserva da intimidade da vida privada*, domínio onde a doutrina alemã identifica três esferas: a da vida íntima (abrangendo os factos mais estritamente pessoais e relacionais de uma pessoa, que devem ficar subtraídos do conhecimento alheio – círculo de sigilo); a da vida privada (compreendendo factos só partilhados com um restrito número de pessoas – círculo de resguardo) e a vida pública ou social (incluindo factos que podem ser divulgados sem restrições, com respeito pelo direito à imagem e à palavra)[35].

Neste contexto – e embora esta distinção seja criticável pelo seu formalismo, criando fronteiras artificiais onde se verifica uma gradação contínua[36] – as informações respeitantes à saúde física e psíquica (abrangendo a informação genética e o historial clínico e características biológicas do indivíduo, ainda que não correspondentes a situações patológicas) corresponderão ao círculo de intimidade da vida pessoal, o mesmo sucedendo com a intimidade da vida conjugal, amorosa, afetiva e sexual, os acontecimentos ocorridos no lar, o conteúdo da cor-

[35] Rita Amaral Cabral, "O direito à intimidade da vida privada (breve reflexão acerca do artigo 80.º do Código Civil)", *cit*., p. 398; Jorge Miranda e Rui Medeiros, *Constituição Portuguesa Anotada,* Tomo I, 2ª Ed., Coimbra, Coimbra Ed., 2010, pp. 620-621; Paulo Mota Pinto, "A proteção da vida privada e a Constituição", *cit*., p. 162; Rabindranath Capelo de Sousa, *O Direito Geral de Personalidade*, Coimbra, Coimbra Ed., 1995, pp. 326 ss.

[36] Pedro Pais Vasconcelos, *Teoria Geral do Direito Civil*, 6ª Ed., Coimbra, Almedina, 2010, p. 66. No mesmo sentido, criticando a rigidez conceptual da teoria, Jorge Miranda e Rui Medeiros, *Constituição Portuguesa Anotada,* Tomo I, *cit*., p. 621.

respondência e comunicações pessoais, os valores ideológicos, etc., conforme resultar das valorações sociais correntes[37].

3 – As condições de licitude para o tratamento de dados

3.1 – Fontes de licitude em geral

I - Como referimos acima, o tratamento de dados pessoais só é lícito se, em função de cada finalidade identificada pelo responsável, se verificar, pelo menos, um dos fundamentos expressamente previstos pelo Regulamento que legitime esse tratamento.

Neste contexto, e para a generalidade dos dados, as fontes de licitude são as estabelecidas no artigo 6.º do RGPD. Desde logo, na alínea a) do n.º 1 do referido artigo, surge identificado o consentimento do titular dos dados para uma ou mais finalidades específicas. Assim, estando o direito à reserva da intimidade da vida privada (ou, noutra formulação, o direito à autodeterminação informativa) na disponibilidade do respetivo titular,

[37] Teodoro Bastos de Almeida, "O direito à privacidade e a proteção de dados genéticos: Uma perspetiva de direito comparado", *cit*., pp. 403-405; Rita Amaral Cabral, "O direito à intimidade da vida privada (breve reflexão acerca do artigo 80.º do Código Civil)", *cit*., p. 399; Helena Moniz, "Notas sobre a proteção de dados pessoais perante a informática (o caso especial dos dados pessoais relativos à saúde)", *cit*., p. 237; Paulo Mota Pinto, "O direito à reserva sobre a intimidade da vida privada", *cit*., pp. 527 ss.; Paulo Mota Pinto, "A proteção da vida privada e a Constituição", *cit*., pp. 166 ss.; Rabindranath Capelo de Sousa, *O Direito Geral de Personalidade*, *cit*., pp. 317 ss. Como refere Pierre Kayser, há um *sentimento de pudor* que envolve estes dados Pierre Kayser, *La Protection de la Vie Privée*, *cit*., p. 6.

pode o mesmo, num ato de vontade livre, consciente e esclarecida, renunciar parcialmente ou limitar o respetivo exercício, permitindo, portanto, o tratamento de tais dados.

Por seu turno, a alínea b) do n.º 1 do artigo 6.º identifica como fonte de licitude a necessidade do tratamento para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados. Trata-se aqui, do nosso ponto de vista, de um consentimento implícito, na medida em que: (i) se a vontade do titular dos dados se dirige à celebração de um contrato; e (ii) se a execução do mesmo ou a realização de diligências pré-contratuais requerem necessariamente o tratamento de dados pessoais (de tal modo que, sem esse tratamento, fica comprometida a referida vontade contratual do titular dos dados); então (iii) presume-se que, não podendo querer o fim sem querer os meios necessários à prossecução do mesmo, o titular dos dados forçosamente consente – sem necessidade de uma declaração expressa – nesse tratamento[38].

Assim, se o titular dos dados pretender celebrar um contrato de seguro de responsabilidade civil geral, por exemplo, terá de, sem necessidade de recolha de consentimento expresso por parte do segurador, facultar a este, designadamente, os seus dados de identificação e morada para figurarem na apólice (alínea b) do n.º 2 do artigo 37.º do Regime Jurídico do Contrato de Seguro – doravante RJCS), bem como os seus dados bancários para cobrança do prémio, para além daqueles que o segurador considere indispensáveis à apreciação do risco proposto.

II – Para além das duas fontes de licitude referidas, que merecerão a nossa especial atenção ao longo deste texto, o n.º 1 do

[38] Cfr., mais desenvolvidamente, *infra*, 6.3.II.

artigo 6.º identifica outras situações legitimadoras do tratamento de dados. Pela sua menor relevância para o presente objeto de análise, apenas as mencionaremos sem maior desenvolvimento.

Assentam elas na necessidade do tratamento para: o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito (alínea c) do n.º 1); a defesa de interesses vitais do titular dos dados ou de outra pessoa singular (alínea d) do n.º 1); o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento (alínea e) do n.º 1); interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança (alínea f) do n.º 1).

3.2 – Categorias especiais de dados e fontes de licitude

I – Como referimos, o tratamento de *categorias especiais de dados*, merecendo uma acrescida proteção legal, requer fontes de licitude específicas, de contornos mais restritivos e exigentes do que as estabelecidas para a generalidade dos dados. Entre elas figura, desde logo, o consentimento explícito do titular dos dados, exceto na medida em que, no caso concreto, o direito da União ou de um Estado-Membro considerar que a proibição de tratamento está fora da disponibilidade do titular (alínea a) do n.º 2 do artigo 9.º do RGPD).

As outras fontes de legitimação previstas assentam na necessidade do tratamento: (i) para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados (alínea b) do n.º 2 do mesmo artigo); (ii) para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento (alínea c) do n.º 2); (iii) para a declaração, o exercício ou a defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional (alínea f) do mesmo n.º); (iv) por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados (alínea g)); (v) para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3 (alínea h))[39]; (vi)

[39] Por seu turno, dispõe o n.º 3 que o tratamento é lícito, no caso referido, se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes.

por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional (alínea i)); (vii) para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados (alínea j)).

Por fim, outras fontes de licitude são ainda consideradas: (viii) o tratamento ser efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares (alínea d) do n.º 2); (ix) o tratamento referir-se a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular (alínea e)).

II – Como acabamos de constatar, e para além do consentimento do titular, não encontramos no elenco do artigo 9.º do

RGPD uma fonte de licitude que claramente albergue o tratamento de dados de saúde no âmbito da execução de contratos de seguro, designadamente – e à semelhança do previsto na alínea b) do n.º 1 do artigo 6.º – a *necessidade* de tratamento de tais dados para a referida execução contratual. E sem tal fundamento, parece faltar a base legal que permita o tratamento de dados de saúde na execução de contratos de seguro. É esta, para já, a equação do problema que nos ocupa.

Importa, porém, verificar porquê, se, para quê, e em que medida, necessita o segurador de tratar dados de saúde. É o que veremos de seguida.

4 – Atividade seguradora e necessidade de tratamento de dados de saúde

I – Antes de mais, para efeitos da presente análise, importa reter algumas características relevantes da relação contratual de seguro. Desde logo, o seguro é tendencialmente um contrato de longa duração, tanto nos casos em que é celebrado por períodos renováveis de um ano que se vão sucessivamente prorrogando de forma automática, como naqueles em que é estipulado um prazo longo, que poderá, nos seguros de vida, prolongar-se por algumas dezenas de anos.

Por outro lado, o contrato de seguro, assente na cobertura dos efeitos económicos de um risco – de ocorrência, causas, circunstâncias e consequências incertas – assume caráter aleatório. Com efeito, no momento da conclusão do contrato são imprevisíveis as consequências económicas que dele resultarão

para qualquer das partes, designadamente, quanto cada uma irá desembolsar e receber ao longo da vigência do mesmo.

De resto, em algumas modalidades de seguros – mormente, nos chamados seguros de pessoas – o objeto do contrato assenta na cobertura riscos ligados ao ser humano, concretamente, relacionados com a vida, a saúde e a integridade física de uma pessoa ou conjunto de pessoas (n.º 1 do artigo 175.º do RJCS). Ora, os dados de saúde são precisamente elementos indispensáveis à caracterização e avaliação, quer do risco que o segurador deverá cobrir (a montante, em sede de subscrição), quer do dano resultante do sinistro (a jusante, em sede de execução do contrato).

Finalmente, conjugando a importância da variável *saúde* na caracterização do risco com a duração tendencialmente *longa* do contrato, temos que, agravando-se o estado de saúde ao longo da vida dos indivíduos, então, se cessar o contrato de seguro (ou se, por alguma razão, o segurador ficar impedido de o executar ao longo da sua vigência), a pessoa segura poderá já não se encontrar num estado de saúde que lhe permita voltar a fazer-se segurar através de um outro contrato.

II – Vejamos melhor, porém, em que medida necessita o segurador de tratar dados de saúde. Referimos acima que essa necessidade se verifica, desde logo, na fase de subscrição, isto é, no processo que conduz à conclusão do contrato. Com efeito, para poder avaliar o risco que lhe é proposto (quanto à probabilidade de ocorrência do sinistro e potencial gravidade das suas consequências) e decidir se o mesmo é aceitável o segurador necessita de conhecer esse risco antes de se vincular.

Ora, o conhecimento desse risco não se encontra na esfera do segurador, mas na do tomador do seguro ou do segurado (pessoa segura, nos seguros de pessoas). Com efeito, verifica-se uma assimetria informativa no sentido em que a generalidade

das informações e dados caracterizadores do risco apenas são conhecidos pela contraparte do segurador, quer porque sejam materialmente inacessíveis a este, quer porque a lei lhe vede o acesso direto aos mesmos, quer porque, quando possível, o custo da investigação pré-contratual das características do risco não seria exequível para o segurador.

A necessidade de cooperação no sentido de estabelecer a paridade informativa entre as partes e de, assim, evitar a viciação especulativa da *alea* contratual e da justiça comutativa inerente à proporcionalidade entre o prémio e o risco impõe, assim, ao tomador do seguro ou segurado o dever de informar o segurador sobre as características do risco proposto[40]. Neste quadro, estabelece o n.º 1 do artigo 24.º do RJCS que o tomador do seguro ou o segurado está obrigado, antes da celebração do contrato, a declarar com exatidão todas as circunstâncias que conheça e razoavelmente deva ter por significativas para a apreciação do risco pelo segurador, acrescentando o n.º 2 que o referido dever não se atém à resposta a eventual questionário fornecido pelo segurador[41]. Por outro lado, prevê-se no n.º 1 do artigo 177.º do RJCS, aplicável aos seguros de pessoas, que, *independentemente dos deveres de informação a cumprir pelo segurado*, a celebração do contrato pode depender de declara-

[40] Ao nível dos seus fundamentos, o instituto da declaração do risco situa-se na interseção, por um lado, das regras pré-contratuais de conduta decorrentes do princípio da boa fé; por outro, das regras de validade inerentes à teoria dos vícios do consentimento e assentes no princípio da autonomia da vontade; e, por fim, das regras inerentes à natureza dos contratos aleatórios. Constitui, assim, um fenómeno de superação da autonomia verificada em Direito civil entre as regras de validade e de comportamento.

[41] O regime da LCS acolhe, assim, um sistema de declaração espontânea (por oposição aos sistemas de questionário fechado). Sobre a declaração do risco, cfr., desenvolvidamente, Luís Poças, *O Dever de Declaração Inicial do Risco no Contrato de Seguro, cit*.

ção sobre o estado de saúde e de exames médicos a realizar à pessoa segura que tenham em vista a avaliação do risco.

Como referimos, nos seguros de pessoas as características do risco segurável prendem-se, em grande medida, com o estado de saúde da pessoa a segurar. Quer nos seguros de vida, quer nos de saúde, os antecedentes clínicos e o estado de saúde atual (assim como algumas circunstâncias que diretamente o influenciam) são elementos essenciais de avaliação do risco, sem o conhecimento dos quais o segurador não poderia formar a sua vontade negocial nem definir as condições contratuais (designadamente, o prémio) aplicáveis.

Ora, a receção, análise, conservação (ou destruição), pelo segurador, das informações clínicas fornecidas pela pessoa segura em sede de declaração inicial do risco constituem, como oportunamente sublinhámos, formas de tratamento de dados pessoais de saúde. Por outro lado, como acabamos igualmente de evidenciar, esse tratamento é, mais do que necessário, indispensável à celebração do contrato de seguro.

Com efeito, na ausência de declaração do risco, o segurador não poderia diferenciar os riscos em função da respetiva probabilidade de ocorrência, tendo de aplicar-lhes o mesmo prémio tarifário normal. Ora, se o prémio for idêntico para os "maus riscos" e para os "bons riscos", isto significa que estes (pagando prémios superiores às respetivas probabilidades de ocorrência do sinistro), subsidiariam os "maus riscos"[42]. Dar-se-ia então o progressivo afastamento dos "bons riscos", que optariam por outros seguradores ou pelo autosseguro. Assim, a concentração de "maus riscos" e a sua subtarifação tornariam a massa de prémios insuficiente para cobrir os sinistros, obrigando a um consequente ajustamento tarifário. Este tenderia a afastar progressivamente os "melhores riscos" e a concentrar os "piores riscos", e assim sucessivamente até ao colapso da atividade do segurador. Este fenómeno, designado por seleção adversa, ilustra a necessidade da declaração inicial do risco e, consequentemente, do tratamento de dados de saúde em algumas modalidades de seguro[43].

III – Os efeitos da declaração do risco (e a necessidade de tratamento dos inerentes dados de saúde informados) não se esgotam, porém, na fase pré-contratual. Com efeito, o incumprimento, doloso ou negligente, do dever de declaração inicial do risco confere ao segurador o direito de impugnar (anular ou resolver, respetivamente) o contrato.

Ora, sucede que a inacessibilidade, já referida, do segurador às características do risco proposto o impede de controlar a veracidade das declarações da pessoa segura quando as mesmas são prestadas. Assim, se a pessoa segura declarar que está em perfeito estado de saúde, que não padece de qualquer doença crónica, que nunca foi objeto de intervenções cirúrgicas, que não toma qualquer medicação, etc., não tem o segurador a possibilidade de aferir da exatidão dessas declarações, sendo forçado a confiar nas mesmas.

Com efeito, o incumprimento do dever de declaração do risco apenas é, em regra, constatado *a posteriori*, na sequência da participação do sinistro (quando então se verifica que

[42] Thomas R. Foley, "Insurers' misrepresentation defence: The need for a knowledge element", *Southern California Law Review*, Vol. 67 (mar. 1994), pp. 665 ss.; Julie-Anne Tarr, "Disclosure in insurance law: Contemporary and historical economic considerations", *International Trade and Business Law Annual*, 6, 2000, p. 211.

[43] Sobre a seleção adversa, cfr. Luís Poças, "Aproximação económica à declaração do risco no contrato de seguro", *Revista de Direito e de Estudos Sociais*, Ano LVII, n.º 1-4 (jan.-dez. 2016), pp. 291 ss.

as causas do mesmo se prendiam com factos já conhecidos da pessoa segura aquando da conclusão do contrato e omitidos ao segurador). Desta forma, o segurador necessita de revisitar posteriormente os dados de saúde que lhe tenham sido comunicados na fase pré-contratual.

IV – Para além das situações referidas, nos seguros de pessoas a execução do contrato de seguro – sobretudo, na sequência da participação do sinistro – dificilmente poderá prescindir do tratamento de dados de saúde.

Assim, no exemplo típico do seguro de saúde, o tratamento dos dados clínicos tenderá a ser imprescindível para a sua execução continuada e durante todo o período de vigência do contrato. Na verdade, consistindo a prestação do segurador no reembolso de despesas clínicas (honorários médicos, elementos auxiliares de diagnóstico, intervenções cirúrgicas, medicamentos, etc.), o mesmo não poderá deixar de inteirar-se da informação clínica de suporte, de modo a controlar se os atos médicos praticados e despesas incorridas têm cabimento contratual.

Também nos outros casos de seguros de pessoas – e até em seguros de responsabilidade civil em que se produzam danos corporais nos terceiros lesados – o tratamento de dados de saúde é indispensável à aferição da dimensão do dano, bem como, eventualmente, das causas e circunstâncias do sinistro. Assim, quando o seguro tenha caráter indemnizatório, só a determinação da extensão do dano corporal permite determinar o próprio montante da prestação a cargo do segurador, possibilitando a realização do objeto do contrato.

Também no caso de um seguro de vida com uma cobertura complementar de morte ou incapacidade por acidente (em que o capital seguro é, portanto, mais elevado nessas circunstâncias), o tratamento de dados clínicos poderá ser – em situações como as de afogamento, envenenamento, etc. – indispensável à determinação da causa da morte ou incapacidade e, portanto, também, do montante do capital que o segurador deve prestar.

Em qualquer caso, como nem todo o universo de eventos possíveis se encontra contratualmente coberto, necessita o segurador de verificar se as circunstâncias em que se produziu o sinistro correspondem a uma exclusão de cobertura[44]. Para o efeito, estando essas circunstâncias ligadas à saúde da pessoa segura, a necessidade de tratamento de dados clínicos é também, para o efeito, incontornável.

Em suma, o objeto e a natureza do risco de certas modalidades de seguro – como é o caso, nomeadamente, dos seguros de vida, dos de saúde, de acidentes pessoais ou de trabalho – implica necessariamente o tratamento de dados de saúde, que é, assim, condição indispensável à realização desse fim.

V – Uma palavra é devida relativamente à orientação que a CNPD vinha seguindo no âmbito da vigência da LPD quanto à necessidade de tratamento de dados de saúde por parte do segurador, designadamente no que respeita a seguros de vida. Neste contexto, vinha defendendo a CNPD que «é no momento da celebração do contrato que a seguradora tem que calcular o risco e, por isso, fazer as diligências sobre o estado de saúde do segurado»[45], parecendo, portanto, desconsiderar a necessidade de tratamento aquando da regularização do sinistro.

[44] Philippe Biclet, "Respet du contrat ou respet du secret, un dilemme", *Médecine et Droit*, n.º 10 (janfev 1995), p. 6.

[45] Cfr. http://www.cnpd.pt/bin/decisoes/2001/htm/del/del05101.htm (consult. 25/06/2010).

Na mesma linha, defendia a CNPD que «o consentimento para o acesso aos dados pessoais de saúde dos titulares segurados já falecidos, para efeitos de pagamento/recebimento de indemnização em virtude de contrato de seguro do ramo Vida, *deve ser limitado* à origem, causas e evolução da doença ou acidente de que resultou a morte do titular segurado. A restante informação de saúde do titular dos dados pessoais, entretanto falecido, é excessiva face à finalidade de aferir do dever de indemnizar em virtude da morte dos segurados, não devendo ser abrangida pelo tratamento – acesso – consentido pelos mesmos segurados»[46].

Esta orientação, extremamente restritiva – e que culminava com o entendimento de que «não será de autorizar o acesso das seguradoras à informação clínica de um segurado para efeito de instrução de processo relativo a seguro de vida»[47] – traduzia, na verdade, pouco conhecimento e sensibilidade face às características da relação de seguro e às necessidades e constrangimentos inerentes à execução deste contrato. Embora visando a defesa dos direitos dos titulares dos dados, essa orientação da CNPD, não isenta de pré-entendimentos contra a atividade seguradora[48],

[46] Sublinhado nosso. Cfr. http://www.cnpd.pt/bin/decisoes/2006/htm/del/del07206.htm (consult. 25/06/2010).

[47] Cfr. http://www.cnpd.pt/bin/decisoes/2006/htm/del/del07206.htm (consult. 25/06/2010).

[48] Citem-se, a título ilustrativo, as declarações públicas de um alto responsável da CNPD, no sentido de que «às vezes as pessoas que nos procuram pensam que ao não autorizarmos o acesso aos dados lhes estamos a dificultar a vida, mas não percebem que o que as seguradoras querem é eventualmente arranjar nos dados clínicos um motivo para não pagar» – citado em "Seguradoras acedem a dados clínicos, mesmo após a morte", *Público*, Ano XXII, n.º 7659 (27 mar. 2011, p. 4).

era de molde, precisamente, a impedir a normal execução do contrato (e regularização do sinistro), suscitando, por vezes, a evitável necessidade de recurso ao litígio judicial.

5 – O problema

I – Constatámos atrás (*supra*, 3.1) que a alínea b) do n.º 1 do artigo 6.º reconhece a licitude do tratamento de dados em geral quando o mesmo seja necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados.

Verificámos igualmente (*supra*, 3.2) que essa fonte de licitude não se encontra prevista para o tratamento de categorias especiais de dados – designadamente (no que releva para o nosso objeto de análise) – os dados de saúde. Cremos ter demonstrado, no entanto (*supra*, 4), que o referido tratamento é indispensável, tanto na fase pré-contratual como na de execução do contrato, relativamente a diversas modalidades de seguros.

II – Com efeito, relativamente ao tratamento de dados de saúde, só parcelarmente encontramos o referido fundamento de licitude previsto na alínea b) do n.º 1 do artigo 6.º (necessidade do tratamento dos dados para a execução de um contrato no qual o titular dos dados é parte) na alínea h) do n.º 2 do artigo 9.º, na menção «por força de um contrato com um profissional de saúde».

Assume, portanto, o legislador que, quem se vincule mediante um contrato com um profissional de saúde, necessariamente haverá de querer (e, portanto, de consentir) no trata-

mento de dados clínicos no âmbito desse contrato. Com efeito, e como referimos já[49], o mencionado fundamento de licitude previsto na alínea b) do n.º 1 do artigo 6.º do RGPD assenta num critério de coerência da vontade do titular: se este voluntariamente se vinculou mediante um contrato; se, consequentemente, a sua vontade se dirige à execução desse contrato; se essa execução *depende* do tratamento de dados pessoais do titular (de tal forma que a mesma não é possível sem esse tratamento); se o titular tem conhecimento dessa necessidade de tratamento e da respetiva finalidade e âmbito; então o titular não pode simultaneamente querer a execução do contrato e não querer o tratamento de dados que sabe serem imprescindíveis para essa execução[50].

Porém, o RGPD não retira a mesma conclusão lógica para outros contratos que, pela sua natureza, requeiram necessariamente o tratamento de dados de saúde, como é o caso de algumas modalidades de seguro, parecendo admitir que o titular dos dados possa querer contratar um seguro e simultaneamente impedir o segurador de cumprir as obrigações que emergem desse contrato. Como refere Ana Alves Leal, «afigura-se contraditório que o cliente esteja interessado na satisfação de um crédito do qual é titular, e que fora constituído negocialmente, mas que, naquilo que dependa de si, não possibilite à instituição financeira essa satisfação»[51].

III – Em suma, e como sublinha a CNPD, verifica-se «a ausência no RGPD de fundamento direto de licitude dos tratamentos de dados de saúde no âmbito dos contratos de seguros [...]»[52]. Assim, e como decorre do RGPD, sem fonte de licitude não pode o segurador tratar dados pessoais após 25 de maio de 2018.

Esta mesma consequência (bem como os esforços feitos pelo setor segurador no sentido do reconhecimento público do problema e da procura de uma solução) é referenciada pela autoridade de controlo: «não pode a CNPD deixar de assinalar o facto de o RGPD, no seu artigo 9.º, não legitimar diretamente o tratamento de dados de saúde no âmbito dos contratos de seguro, aspeto que a Proposta de Lei não acautelou apesar dos alertas emitidos pelo setor da atividade seguradora. Sendo certo que a consequência desta ausência de disciplina legal é o dever de eliminação dos dados de saúde tratados pelas seguradoras»[53].

Desta forma, sem solução à data de aplicação do RGPD, haveria o setor segurador de ter eliminado todos os dados de saúde na sua posse, deixando, portanto (por impossibilidade material e normativa) de executar os contratos vigentes. Essa impossibilidade, objetiva, superveniente e alheia ao segurador, haveria de ditar a extinção de todos os contratos de seguro que implicassem o tratamento de dados de saúde.

As consequências, nos planos social e económico, seriam, naturalmente, catastróficas: o colapso do setor segurador em seguros de pessoas; e todo o universo dos respetivos segurados que ficaria privado de cobertura para os sinistros já ocorridos ou futuros. Acresce que, no caso dos seguros de vida – e mesmo que o problema viesse a ser superado em momento futuro –, as

[49] *Supra*, 3.1.I.

[50] Cfr., mais desenvolvidamente, *infra*, 6.3.II.

[51] Ana Alves Leal, "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", *cit.*, p. 161.

[52] Parecer n.º 20/2018, da CNPD, de 02/05/2018 - https://www.cnpd.pt/bin/decisoes/Par/40_20_2018.pdf, p. 41v. (consult. 03/08/2018).

[53] Parecer n.º 20/2018, da CNPD, de 02/05/2018, *cit.*, p. 37 v.

pessoas seguras, tendo perdido uma cobertura contratual de longo prazo (que as protegeria mesmo que as respetivas condições de vida e de saúde se viessem a agravar acentuadamente), não conseguiriam voltar a obter no mercado segurador cobertura para o mesmo risco.

IV – Eis, assim, formulado o problema que nos ocupa e para o qual procuraremos debater, no quadro vigente, as soluções que se nos afiguram possíveis. Começaremos, para o efeito, por consagrar alguma atenção ao consentimento como fonte de licitude, explicando porque não pode ser esta – diversamente do que era comummente aceite no quadro legal anterior – a solução para o problema equacionado.

6 – O consentimento como fonte de licitude

6.1 – Aspetos gerais: a definição legal de consentimento

I – Como referimos, entre as fontes de licitude para o tratamento – quer dos dados pessoais, em geral, quer das categorias especiais de dados, como é o caso dos de saúde – encontra-se, em papel de destaque, o consentimento do titular para uma ou mais finalidades específicas (respetivamente, alínea a) do n.º 1 do artigo 6.º, e alínea a) do n.º 2 do artigo 9.º, ambos do RGPD).

No quadro da LPD era entendimento pacífico que, apesar das dificuldades que os requisitos do consentimento já apresentavam, o tratamento de dados de saúde na execução de contratos e seguro apenas poderia ser efetuado com base no prévio consentimento do titular. No caso, por exemplo, dos seguros de vida, a posição da CNPD era a de que esse prévio consentimento constituía a única forma de o segurador (ou os familiares da pessoa segura) acederem a informação clínica após a morte desta[54].

Ora, enquanto na LPD o consentimento assumia a posição de fonte-*regra* de licitude do tratamento dos dados, figurando as outras fontes de licitude como *exceções* (cfr. artigos 6.º e 7.º da LPD), no RGPD o consentimento surge mais claramente como uma fonte de licitude ao lado das demais previstas[55].

É certo que, para alguns autores, o tratamento de dados clínicos por seguradores não poderá deixar de ter o consentimento por fonte de licitude[56]. Porém, a perspetiva atualmente domi-

[54] Referia a CNPD que «não existe na Lei 67/98 ou noutra disposição legal qualquer norma que autorize a Companhia de Seguros, nestas circunstâncias (sem consentimento *e* depois da morte), a aceder à informação clínica em poder dos hospitais ou centros de saúde» http://www.cnpd.pt/bin/decisoes/2001/htm/del/del05101.htm (consult. 25/06/2010). Como também se afirmava na Deliberação n.º 72/2006, «não havendo, como não há, lei formal que preveja e legitime o acesso aos dados pessoais de saúde de titulares falecidos, pelas Companhias de Seguros e pelos familiares desses titulares, para efeitos de pagamento/recebimento de indemnizações em virtude da morte dos titulares segurados, esse acesso apenas pode decorrer do consentimento dos titulares: artigo 35º da Constituição da República Portuguesa (CRP) e nº 2 do artigo 7º da Lei de Proteção de Dados (LPD)» - http://www.cnpd.pt/bin/decisoes/2006/htm/del/del07206.htm (consult. 25/06/2010).

[55] Neste sentido (embora discordando, de *iure condendo*, desta equiparação), Borja Adsuara Varela, "El consentimiento", *in* José Luis Piñar Mañas (Dir.); María Álvarez Caro, Miguel Recio Gayo (Coord.), *Reglamento General de Protección de Datos: Hacia un Nuevo Modelo Europeo de Privacidad*, Madrid, Editorial Reus, 2016, p. 158.

[56] Cfr., por exemplo, Jean-François Henrotte e Fanny Coton, "L'impact du R.G.P.D. dans le secteur des assurances: Comment s'y conformer?", *cit.*, pp. 109-110.

nante é bem outra. Por um lado, porque o consentimento, em virtude dos seus requisitos legais, assume caráter efémero e precário[57], não constituindo, portanto, um fundamento de licitude apto a albergar o tratamento de dados de saúde no âmbito da execução de contratos de seguro. Por outro lado, porque, precisamente pelas suas características, o consentimento passou, na prática, a assumir, de algum modo, um papel de subsidiariedade relativamente às outras fontes de licitude[58].

[57] Este caráter está associado ao papel central do titular dos dados, conferido pelo RGPD, sugerindo que o sentido passivo do consentimento (face a uma ação do responsável pelo tratamento) seja substituído pela noção de liberdade ou autodeterminação dos dados, que emana, de resto, dos direitos reforçados do titular, consagrados no Regulamento – neste sentido, Borja Adsuara Varela, "El consentimiento", *cit.*, pp. 168-169; María Álvarez Caro, "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", *cit.*, p. 228.

[58] Com efeito, obedecendo o consentimento a requisitos apertados, quando o responsável pelo tratamento disponha cumulativamente de vários fundamentos de licitude de que possa lançar mão e opte por fazer o tratamento com base no consentimento, não poderá posteriormente (e de forma retroativa) invocar outro fundamento, ficando então sujeito – como veremos melhor – às vicissitudes do consentimento - Grupo de Trabalho do Artigo 29.º, *Orientações Relativas ao Consentimento na Aceção do Regulamento (UE) 2016/679* - https://www.cnpd.pt/bin/rgpd/docs/wp259rev0.1_PT.pdf, p. 26 (consult. 07/09/2018). Isto significa, na prática, que o responsável pelo tratamento deverá, podendo, optar por qualquer outro fundamento de licitude, só recorrendo ao consentimento na falta do mesmo: «o artigo 9.º, n.º 2, não reconhece "necessário para a execução de um contrato" como uma exceção à proibição geral de tratamento de categorias especiais de dados. Por conseguinte, os responsáveis pelo tratamento e os Estados-Membros que se defrontam com esta situação devem recorrer às exceções previstas no artigo 9.º, n.º 2, alíneas b) a j). Caso nenhuma das exceções que constam das alíneas b) a j) se aplique, a obtenção de consentimento explícito em conformidade com as condições aplicáveis ao consentimento válido no RGPD será a única exceção lícita possível para tratar os referidos dados» - *idem*, p. 22.

Vejamos, porém, mais detidamente porque, na falta de outro fundamento para o tratamento de dados de saúde em seguros, não poderá o segurador efetuar esse tratamento repousando no consentimento do titular.

II – No contexto do RGPD, o consentimento do titular dos dados é definido, na alínea 11) do artigo 4.º, como «uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento». Vejamos paulatinamente os vários requisitos do consentimento e os problemas que os mesmos suscitam.

III – Desde logo constatamos, na comparação entre a redação do artigo 9.º e a do artigo 6.º do RGPD, que aquela se refere ao consentimento *explícito* do titular, enquanto esta apenas se refere o *consentimento* do titular. Com base nesta diferente formulação, vários autores reclamam para o consentimento do artigo 9.º um requisito adicional de *explicitação*[59]. Ora, como decorre da citada definição da alínea 11) do artigo 4.º, *todo* o consentimento deve ser *explícito*[60], entre outros requisitos,

[59] Cfr., por exemplo, Jean-François Henrotte e Fanny Coton, "L'impact du R.G.P.D. dans le secteur des assurances: Comment s'y conformer?", *cit.*, p. 109; Ian Long, *Data Protection – The New Rules*, Bristol, Jordan Publishing, 2016, p. 128.

[60] *Explícito* será, assim, sinónimo de *expresso*, preferencialmente (mas não necessariamente) prestado por declaração assinada – Grupo de Trabalho do Artigo 29.º, *Orientações Relativas ao Consentimento na Aceção do Regulamento (UE) 2016/679*, *cit.*, p. 21.

pelo que não deverá ser atribuído sentido especial ao adjetivo *explícito* do artigo 9.º por oposição ao do artigo 6.º.

Com certa generosidade interpretativa, alguma doutrina qualifica como consentimento *explícito* o livre fornecimento de dados, pelo titular, depois de ser informado dos fins a que o tratamento se destina. Neste sentido, se um passageiro de uma companhia de aviação solicita uma cadeira de rodas, a companhia ficará autorizada a tratar este dado de saúde, ainda que o titular não tenha assinado uma declaração de consentimento nesse sentido[61]. Do mesmo modo – dir-se-ia, por analogia – se uma pessoa segura fornecesse informação clínica ao segurador para a subscrição de um contrato de seguro ou para a regularização de um sinistro, considerar-se-ia ter dado o seu consentimento explícito ao tratamento para o fim em causa. Cremos que, apesar da assertividade lógica desta posição, a exigência do caráter *explícito* da vontade manifestada vai precisamente no sentido contrário desta interpretação, que se bastaria com a natureza *implícita* (ou tácita) da manifestação de vontade.

A definição legal acolhe duas formas de *manifestação* do consentimento: (i) a declaração; e (ii) o ato positivo inequívoco. Se os adjetivos *positivo* e *inequívoco* se reportam ao ato, a verdade é que também a declaração não poderá deixar de os verificar[62]. Em qualquer caso, se o ato positivo inequívoco poderá traduzir-se no assinalar de uma opção num formulário (o "picar" de um campo onde se pergunte – «consente no tratamento... para a seguinte finalidade...? Sim / Não»), pensamos que não poderá bastar-se com uma simples manifestação tácita, presumida ou implícita, ainda que a mesma decorra de um ato positivo que pressuponha necessariamente o dito consentimento (exemplos dados no parágrafo anterior).

[61] Ian Long, *Data Protection – The New Rules*, Bristol, *cit*., pp. 128-129. Em sentido contrário – recorrendo precisamente ao mesmo exemplo – Grupo de Trabalho do Artigo 29.º, *Orientações Relativas ao Consentimento na Aceção do Regulamento (UE) 2016/679*, *cit*., p. 22.

[62] Borja Adsuara Varela, "El consentimiento", *cit*., p. 152.

6.2 – Cont.: a especificidade do consentimento

I – Um dos requisitos do consentimento é, como referimos, o da *especificidade* («manifestação de vontade [...] específica»). Este requisito encerra, na perspetiva do Grupo do Artigo 29.º, várias vertentes. Assim, haverá de atender à própria especificidade das finalidades para as quais o consentimento é dado (cfr. alínea a) do n.º 1 do artigo 6.º e alínea a) do n.º 2 do artigo 9.º do RGPD), no sentido de que deverá haver um consentimento para cada finalidade singular e delimitada, sendo recolhido separadamente para cada uma delas (granularidade) e com base em informação discriminada, tudo de modo a assegurar a transparência e a permitir ao titular um maior controlo sobre o tratamento dos seus dados[63].

Sobre o requisito da especificidade – que se suscitava já no âmbito da LPD –, vem defendendo a CNPD que o mesmo «deve significar que o consentimento se refere a uma contextualização factual concreta, a uma atualidade cronológica precisa e balizada e a uma operação determinada, sendo o mais individualizado possível. O consentimento específico afasta os casos de consentimento preventivo e generalizado, prestado

[63] Grupo de Trabalho do Artigo 29.º, *Orientações Relativas ao Consentimento na Aceção do Regulamento (UE) 2016/679*, *cit*., pp. 12 ss.

de modo a cobrir uma pluralidade de operações»[64]. De forma clarificadora, sublinhava a CNPD, na nota 38 da Deliberação n.º 51/2001, que «não será suficiente um "consentimento genérico", como já se tem visto em contratos de seguro enviados à CNPD, no qual se admite o "acesso à informação clínica existente em hospitais, centros de saúde ou médicos particulares". Este consentimento, pelo seu carácter demasiado genérico, não configura o "consentimento expresso" legalmente exigível»[65].

II – Constatámos, porém, que o contrato de seguro assenta na imprevisibilidade e incerteza relativamente ao risco coberto e (sobretudo no ramo Vida) é tendencialmente de longo prazo. Neste contexto, é impossível ao segurador saber, no momento de recolha do consentimento (início do contrato), quais as circunstâncias concretas de tempo, lugar e modo em que irá proceder ao tratamento de dados, nos termos que vinham sendo requeridos pela CNPD.

Assim, por exemplo, num seguro de acidentes pessoais ou de vida, deverá ser de todo imprevisível a eventual ocorrência, na vigência do contrato, de um sinistro (morte, acidente, incapacidade), bem como, mais ainda, as circunstâncias, momento, causas e consequências do mesmo. Não podem, assim, as partes antever que, vários anos após a celebração do contrato e a inerente obtenção do consentimento, o segurador irá necessitar,

[64] http://www.cnpd.pt/bin/decisoes/2006/htm/del/del07206.htm (consult. 25/06/2010).

[65] http://www.cnpd.pt/bin/decisoes/2001/htm/del/del05101.htm (consult. 25/06/2010). Cfr. também Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, *cit*., p. 207; e Helena Moniz, "Notas sobre a proteção de dados pessoais perante a informática (o caso especial dos dados pessoais relativos à saúde)", *cit*., p. 238.

para poder cumprir a sua obrigação contratual (regularização do sinistro) de analisar um relatório de autópsia, ou de alta hospitalar, ou determinados exames ou análises clínicas concretas.

Também num seguro de saúde é uma impossibilidade prática e lógica, tanto para a pessoa segura (titular dos dados) como para o segurador (responsável pelo tratamento), poder antecipar quais os atos médicos, elementos auxiliares de diagnóstico, etc., que a pessoa segura irá realizar na vigência do contrato, bem como, portanto, quais os dados clínicos que o segurador necessitará de tratar (e em que momento) para poder cumprir a sua obrigação contratual.

Como decorre dos exemplos dados, o consentimento que o segurador solicitava que lhe fosse concedido para efeito de execução do contrato sempre teria de ser formulado em moldes suficientemente latos e abrangentes, de modo a cobrir todas as eventualidades possíveis. Porém, num momento posterior, quando o segurador verificava a necessidade de efetuar o tratamento dos dados para dar cumprimento à sua obrigação pecuniária, já a CNPD se manifestava pela ineficácia do consentimento e, consequentemente, pela ilicitude do tratamento em causa[66].

III – A solução para o problema descrito – o requisito da *especificidade* do consentimento, sobretudo no entendimento que do mesmo vinha fazendo a CNPD na vigência da LPD –

[66] Numa orientação antagónica, a jurisprudência francesa admite a validade de uma cláusula contratual segundo a qual a cobertura fica expressamente subordinada à condição do consentimento da pessoa segura quanto ao levantamento do segredo médico, em caso de morte da mesma Sabine Abravanel-Jolly, "Le secret médical en assurance de personnes", *Revue Générale du Droit des Assurances*, 2005, n.º 4, p. 899; Maxime Cauchy e Amélie DionisiPeyrusse, "Le droit au secret médical et son application en matière d'assurances", *Recueil Dalloz*, 2005, n.º 20, Chroniques, p. 1315.

não poderá ter por solução a recolha de um consentimento por cada situação (sinistro) que requeira o tratamento de dados de saúde. Com efeito, em casos como os do seguro de saúde, em que a recorrência da apresentação de despesas clínicas (consultas médicas, elementos auxiliares de diagnóstico, medicamentos, etc.) implica o regular tratamento de dados clínicos, seria impraticável, pela ineficiência, complexidade e demora que passaria a afetar a regularização dos processos de sinistro.

Por outro lado, esta via de solução sempre se depararia com situações em que se verificasse a impossibilidade de o titular dos dados dar, durante a vigência do contrato, o seu consentimento, designadamente porque pudesse ter falecido, ou estar temporária ou definitivamente incapaz e sem aptidão física ou mental para prestar esse consentimento (sinistros de morte em seguros de vida ou de acidentes). Mas poderia igualmente dar-se o caso de o titular dos dados, sem prejuízo da sua pretensão à prestação do segurador, poder pretender obstar ao tratamento dos dados porque o mesmo lhe fosse adverso (pela suscetibilidade de revelar uma qualquer situação que determinasse a perda do direito à prestação do segurador).

Em suma, o requisito da especificidade do consentimento – sobretudo na orientação que do mesmo vinha seguindo a CNPD relativamente à necessidade de tratamento de dados de saúde na execução de contratos de seguro – é de molde a inviabilizar a obtenção do consentimento do titular como fonte de licitude daquele tratamento. Não obstante, outros requisitos do consentimento comprometem a sua aptidão como fundamento da licitude do tratamento de dados de saúde. Vejamos de seguida quais e em que moldes.

6.3 – Cont.: a liberdade do consentimento

I – Como referimos, um dos requisitos do consentimento traduz-se no caráter voluntário – livre, portanto – do mesmo. Este requisito verte, designadamente, dos considerandos 32 e 43; da alínea 11) do artigo 4.º; do artigo 7.º; da alínea c) do n.º 2 do artigo 13.º; e da alínea d) do n.º 2 do artigo 14.º, todos do RGPD.

Vimos que o tratamento de dados de saúde é *necessário* para a execução de alguns contratos de seguro. Por outro lado, sendo o mesmo igualmente necessário para a própria formação do contrato (aferição e controlo, pelo segurador, da declaração inicial do risco), o segurador, na falta de outra fonte de licitude, haveria de obter o consentimento do titular logo na fase pré-contratual. *Quid iuris*, porém, se, sendo o consentimento *livre*, o titular dos dados se recusar a dá-lo logo na fase pré-contratual? Poderá o segurador condicionar a celebração do contrato à prévia obtenção do consentimento? Será um consentimento obtido nestes termos efetivamente *livre*?

Sobre o caráter livre do consentimento, clarifica o considerando 43, parte final, do RGPD que se presume «que o consentimento não é dado de livre vontade se [...] a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento *apesar de o consentimento não ser necessário para a mesma execução*». Esta regra encontra-se igualmente consagrada no n.º 4 do artigo 7.º: «ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais *que não é necessário para a execução desse contrato*».

Assim, como resulta das citadas disposições, o consentimento não é livre se for imposto (ou extorquido) ao titular como contrapartida de um serviço ao qual o tratamento visado *não seja necessário* (tal seria o caso, por exemplo, se o segurador exigisse, como contrapartida da celebração do seguro, o consentimento ao tratamento de dados para efeitos de *marketing*).

Pensamos que o preceito, porém, não admite uma leitura *a contrario*, no sentido de que o consentimento seja livre (e, portanto, válido) se o tratamento visado for efetivamente necessário à execução de um contrato ou à prestação de um serviço cuja execução ou prestação fiquem dependentes da obtenção de tal consentimento (como seria o caso do tratamento de dados de saúde na execução de contratos de seguro)[67]. Simplesmente, na coerência lógica interna do RGPD, a solução de licitude, neste caso, não assentaria já no consentimento, mas na necessidade do tratamento para a execução do contrato ou prestação do serviço (alínea b) do n.º 1 do artigo 6.º, sem correspondente, como vimos, quanto à licitude do tratamento de dados de saúde)[68].

[67] Claramente neste sentido, Grupo de Trabalho do Artigo 29.º, *Orientações Relativas ao Consentimento na Aceção do Regulamento (UE) 2016/679*, *cit*., p. 9. Como se refere neste documento, «regra geral, o RGPD prevê que se o titular dos dados não puder exercer uma verdadeira escolha, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido» – *idem*, p. 6.

[68] Como refere o Grupo do Artigo 29.º, «o RGPD assegura que o tratamento dos dados pessoais relativamente ao qual se solicita o consentimento não pode ser direta ou indiretamente uma contrapartida da execução de um contrato. Os dois fundamentos para o tratamento lícito dos dados pessoais, ou seja, o consentimento e o contrato, não podem fundir-se nem misturar-se. [...] Se o responsável pelo tratamento pretender tratar dados pessoais que são efetivamente necessários para a execução do contrato, o consentimento não é o fundamento legal» – Grupo de Trabalho do Artigo 29.º, *Orientações Relativas ao Consentimento na Aceção do Regulamento (UE) 2016/679*, *cit*., pp. 8-9.

Em suma, e como resulta da orientação do Grupo do Artigo 29.º[69], na falta de outra fonte de licitude para o tratamento dos dados o segurador não poderia condicionar a celebração do contrato à obtenção do consentimento, na medida em que um consentimento assim obtido seria inválido, tornando ilícito o tratamento de dados de saúde.

II – O princípio da liberdade contratual, que encontra reflexo no artigo 405.º do CC, é expressão do mais amplo princípio da autonomia privada, o qual traduz a margem de liberdade deixada aos privados para autorregularem os seus interesses. A liberdade contratual manifesta-se no exercício da *vontade* autónoma dos sujeitos, através da livre negociação, estipulação, celebração e execução dos contratos[70]. Porém, obrigando-se as partes, ficam as mesmas sujeitas ao princípio *pacta sunt servanda*, que se manifesta no n.º 1 do artigo 406.º do CC, também designado por princípio da estabilidade contratual ou da vinculatividade.

Também o direito de autodeterminação informativa do titular dos dados pessoais sobre os mesmos radica, afinal, na *vontade* autónoma e soberana desse titular no sentido de de-

[69] «Em termos gerais, qualquer elemento que constitua pressão ou influência desadequada sobre o titular dos dados (que se pode manifestar de formas muito diversas) e que o impeça de exercer livremente a sua vontade tornará o consentimento inválido» – cfr. Grupo de Trabalho do Artigo 29.º, *Orientações Relativas ao Consentimento na Aceção do Regulamento (UE) 2016/679*, *cit*., p. 6.

[70] Cfr. Jorge Morais Carvalho, *Os Limites à Liberdade Contratual*, Coimbra, Almedina, 2016, pp. 24 ss.

terminar e controlar a utilização (ou tratamento) de que os seus dados pessoais são objeto.

Não obstante, ao vincular-se contratualmente, cada parte aceita as consequências das obrigações que assume e que geram expectativas de cumprimento na contraparte. Assim, em algumas modalidades de seguro, uma dessas consequências é a necessidade de tratamento de dados de saúde. Porém, a depender esse tratamento de um consentimento livre (tão livre como a liberdade contratual, mas independente ou autónomo em relação a esta), o titular dos dados teria cobertura legal para incumprir licitamente o contrato, o que não será admissível. É esta necessidade de sintonia, de coerência, que faz com que no artigo 6.º do RGPD se legitime o tratamento de dados necessário à execução de um contrato (e é ela que torna incompreensível que a mesma solução não seja acolhida no artigo 9.º).

Do nosso ponto de vista, a fonte de licitude consagrada na alínea b) do n.º 1 do artigo 6.º do RGPD – necessidade do tratamento para a execução de um contrato no qual o titular dos dados seja parte, ou para diligências pré-contratuais a pedido do titular dos dados – não se funda na consideração de que o contrato, e as inerentes vinculações assumidas pelo titular dos dados perante a contraparte, seriam objetivamente mais valiosos do que o direito de autodeterminação do titular dos dados sobre os mesmos, devendo, portanto, aquelas prevalecer sobre este direito.

Fundar-se-á antes, de acordo com um princípio de coerência lógica, na própria vontade livre e esclarecida do titular. Com efeito, ao *querer* vincular-se contratualmente – e ao *saber* que, fazendo-o, isso comportará *necessariamente* o tratamento de dados pessoais – o titular dos dados não poderá deixar de *querer*, como consequência forçosa, o tratamento desses dados. Por outras palavras, a *vontade contratual*, quando implique inevitavelmente o tratamento de dados pessoais (e o titular disso tenha consciência), é incindível da *vontade* (consentimento) dirigida a tal tratamento.

Dito ainda de outra forma, quando o tratamento dos dados seja (consabidamente) necessário para a execução de um contrato no qual o titular dos dados seja parte, ou para diligências pré-contratuais a pedido do mesmo, há uma *presunção inilidível de consentimento* do titular nesse tratamento. Será sempre a vontade, livre e esclarecida, do titular a prevalecer. Porém, diversamente do que sucede com a fonte de licitude prevista na alínea a) do n.º 1 do artigo 6.º, e na alínea a) do n.º 2 do artigo 9.º – um autónomo consentimento, que não poderia presumir-se e que, por isso, terá de ser explícito e inequívoco – o consentimento subjacente à alínea b) do n.º 1 do artigo 6.º vem, por uma questão de coerência, incindivelmente fundido com a vontade dirigida ao contrato.

Se o contrato não prescinde do tratamento de dados e se não pode subsistir sem este, então o titular dos dados poderá não querer o contrato, mas não poderá querer o contrato e não querer o tratamento. É esta a lógica inerente à alínea b) do n.º 1 do artigo 6.º do RGPD. Significará isto que, ao vincular-se contratualmente, o titular renuncia ao seu direito à autodeterminação informativa sobre os seus dados? Não será, de todo, o caso. Simplesmente, o destino do tratamento dos dados será incindível do destino do contrato: o titular sempre poderá desvincular-se, nos termos permitidos pelo Direito[71], fazendo

[71] Em última instância, tratando-se de uma desvinculação ilícita, emergirá um dever de indemnização da contraparte.

cessar então, inerentemente, o tratamento de dados requerido por tal contrato. O que o titular não poderá é ter a pretensão de manter o contrato em plena execução e vigência, mas obstar ao tratamento de dados de que aquela execução depende.

Ora, esta lógica, bem vincada no artigo 6.º do RGPD, desaparece depois no tratamento de categorias especiais de dados (artigo 9.º). Relativamente a estes – no caso, aos dados de saúde – o legislador do RGPD, ao permitir uma cisão entre a vontade dirigida ao contrato e a vontade dirigida ao tratamento dos dados requerido pelo contrato, parece ignorar a incongruência paradoxal que do regime resulta. Admite que ao titular dos dados, parte num contrato, não possa ser exigido o consentimento para o tratamento dos dados indispensáveis à execução de tal contrato. E também que, sendo esse consentimento dado inicialmente, não possa o titular que pretenda retirá-lo ser prejudicado (designadamente, com a suspensão da execução do contrato), ainda que essa execução dependa do tratamento de dados, agora privado da sua fonte de licitude originária.

Para além do insuperável absurdo lógico gerado, o legislador do RGPD abre igualmente caminho a que o titular dos dados faça uma utilização abusiva, ou mesmo fraudulenta, à medida das conveniências de cada momento, do direito à autodeterminação informativa sobre os seus dados. Pode, assim, o titular dos dados, por exemplo, tendo efetuado uma declaração inicial do risco com omissões ou inexatidões dolosas sobre o seu estado de saúde, vir mais tarde, após qualquer ocorrência suspeita, impedir o segurador de investigar aquelas declarações mediante a retirada do consentimento.

III – O requisito em análise (*liberdade*) tem, efetivamente, como corolário o direito de retirada – ou revogação unilateral – do consentimento a todo o tempo. Na verdade, estabelece o n.º 3 do artigo 7.º do RGPD que «o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar».

Significa esta regra que, se o segurador tiver – confiando num consentimento, para o tratamento de dados de saúde, obtido aquando da conclusão do contrato – celebrado um seguro para cuja execução seja necessário esse tratamento, poderá ser surpreendido, a qualquer momento, com a retirada do consentimento e com a consequente inviabilidade dessa execução.

Com efeito, para os autores que sustentam ser o consentimento a base legal de tratamento de dados de saúde em contratos de seguro, a retirada do consentimento terá por efeito a imediata cessação do tratamento dos dados[72] e, inerentemente, a impossibilidade legal da sua execução por parte do segurador, mormente quando se trate de regularizar o sinistro.

Desta forma, a retirada do consentimento, nos seguros em que seja indispensável o tratamento de dados de saúde, está na origem de uma impossibilidade objetiva superveniente do cumprimento por causa imputável ao credor. Neste quadro, e nos termos do n.º 1 do artigo 790.º do CC (disposição sem cor-

[72] Cfr., por exemplo, Jean-François Henrotte e Fanny Coton, "L'impact du R.G.P.D. dans le secteur des assurances: Comment s'y conformer?", *cit.*, p. 110.

respondente no RJCS), essa impossibilidade determina a extinção da obrigação[73].

Ora, nos termos resultantes do RGPD, o consentimento só será inteiramente livre se da sua retirada não resultarem consequências adversas para o titular dos dados[74]. Com efeito, e conforme resulta do considerando 42, «não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados [...] não puder recusar nem retirar o consentimento sem ser prejudicado»[75].

[73] Noutros casos, a retirada do consentimento não tornará *impossível* a prestação do segurador, mas reduzirá de forma substancial os meios de defesa e controlos indispensáveis à determinação da prestação devida, deixando o segurador vulnerável, designadamente, a práticas de fraude (omissões ou inexatidões pré-contratuais dolosas, simulação ou provocação intencional do sinistro ou do dano corporal, agravamento de danos, etc.). Neste contexto, pensamos que a revogação do consentimento, quando não determine exatamente a impossibilidade do cumprimento, se traduzirá numa justa causa de resolução do contrato de seguro, nos termos e para os efeitos previstos no artigo 116.º do RJCS.

[74] Esta era já, aliás, a orientação que resultava da LPD. Com efeito, quanto ao caráter livre do consentimento, afirmava Catarina Sarmento e Castro que o mesmo «será livre quando seja dado sem qualquer pressão e quando possa ser retirado sem restrições ou oposição, e sem que o titular dos dados sofra qualquer consequência» — Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, *cit*., p. 207.

[75] Conforme o entendimento do Grupo do Artigo 29.º, «o responsável pelo tratamento tem de demonstrar que é possível recusar ou retirar o consentimento sem que o titular dos dados seja prejudicado (considerando 42)» – Grupo de Trabalho do Artigo 29.º, *Orientações Relativas ao Consentimento na Aceção do Regulamento (UE) 2016/679*, *cit*., p. 11. Assim, «se o responsável pelo tratamento for capaz de demonstrar que o serviço inclui a possibilidade de retirar o consentimento sem que daí advenham quaisquer consequências negativas, nomeadamente que a prestação do serviço perca qualidade prejudicando o utilizador, tal pode servir para comprovar que o consentimento foi dado livremente» – *idem*, p. 12.

Na lógica do RGPD, os prejuízos decorrentes da retirada do consentimento são a demonstração de que o mesmo não foi dado livremente e de que era, portanto, inválido. Sendo esse o caso, será ilícito o próprio tratamento de dados efetuado no passado (e, por maioria de razão, no futuro). Por outro lado, e sem embargo de outras consequências no plano civil, as condições de consentimento estão entre aquelas cujo incumprimento dá lugar a procedimento contraordenacional e determina, conforme previsto na alínea a) do n.º 5 do artigo 83.º do RGPD, a aplicação de coimas até € 20 000 000,00 ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado.

Quid iuris, porém, quanto ao contrato? É certo que, sendo o tratamento de dados de saúde indispensável à execução do contrato, e não sendo esse tratamento possível, o contrato não poderá subsistir, cessando nos termos acima referidos. Independentemente de outras considerações, as consequências de toda esta cadeia de eventos, revelam-se catastróficas nos planos social e económico. No domínio social, antecipa-se que muitas pessoas seguras deixariam, inadvertidamente, de beneficiar de cobertura de um seguro, sem possibilidade, em muitos casos (pelo agravamento do risco decorrente da degradação das suas próprias condições de saúde) de virem posteriormente a obtê-la junto de outro segurador. No plano económico, antecipa-se o colapso dos ramos de seguros afetados pela problemática em análise.

IV – Adicionalmente, a retirada do consentimento poderá ser agravada por uma etapa subsequente. Com efeito, o con-

siderando 65, bem como a alínea b) do n.º 1 do artigo 17.º do RGPD, estabelecem que o titular dos dados pessoais tem direito a obter do responsável do tratamento o apagamento dos seus dados ("direito a ser esquecido") sempre que, designadamente, aquele retire o consentimento.

É certo, porém, que a alínea b) do n.º 3 do artigo 17.º salvaguarda os casos em que o tratamento se revele necessário ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito. Tal é o caso das obrigações de conservação de dados que decorrem, designadamente, do artigo 40.º do Código Comercial; do n.º 4 do artigo 123.º do Código do IRC; do n.º 1 do artigo 52.º do Código do IVA; bem como do n.º 1 do artigo 51.º da Lei n.º 83/2017, de 18 de agosto (Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo).

Em qualquer caso, e fora das circunstâncias previstas no n.º 3 do artigo 17.º, a configuração de um direito ao apagamento de dados de saúde, quando os mesmos sejam imprescindíveis à execução de um contrato de que o titular seja parte, traduz, do nosso ponto de vista, um suplementar e incompreensível paradoxo, a acrescer à já mencionada possibilidade de retirada do consentimento.

V - Dispõe o considerando 171 do RGPD que «os tratamentos de dados que se encontrem já em curso à data de aplicação do presente regulamento deverão passar a cumprir as suas disposições no prazo de dois anos após a data de entrada em vigor». Acrescenta-se, por outro lado, que, «se o tratamento dos dados se basear no consentimento dado nos termos do disposto na Diretiva 95/46/CE, não será necessário obter uma vez mais o consentimento do titular dos dados, se a forma pela qual o consentimento foi dado cumprir as condições previstas no presente regulamento, para que o responsável pelo tratamento prossiga essa atividade após a data de aplicação do presente regulamento».

Ora, não obstante, como vimos, o tratamento de dados de saúde em seguros assentar, à luz da LPD, no consentimento do titular, algumas das principais incongruências e contradições de que temos dado conta verificavam-se já então. Por esta razão, e sem embargo de os seguradores, em regra, assumirem o encargo de recolha sistemática dos consentimentos dos titulares para o efeito, a conformidade de tais consentimentos com os respetivos requisitos legais era já, no mínimo, muito duvidosa. E se o era então, é-o agora por maioria de razão.

Neste quadro, e na falta de outra fonte de licitude para o tratamento de dados de saúde, verificar-se-á, nos termos do dito considerando 171 a obrigatoriedade de renovação dos consentimentos[76]. Porém, ainda que o consentimento fosse uma fonte de licitude apta a suportar o tratamento de dados de saúde *necessários* à execução de um contrato de seguro, a obtenção de novos consentimentos seria tarefa impraticável.

Desde logo, pela dificuldade do segurador em contactar e obter retorno de *todos* os clientes titulares de dados, quer porque nem sempre os contactos estejam atualizados, quer porque, em regra, a inércia prevalece e a simples ausência de resposta corresponde à recusa do consentimento. Ademais, muitos titulares, be-

[76] Esta obrigatoriedade decorrerá da falta de preenchimento dos requisitos legais do consentimento no RGPD, e não de se pretender tratar agora os dados para fim diverso do inicialmente visado. Borja Adsuara Varela, "El consentimiento", *cit.*, p. 154.

neficiando já de seguros em vigor, não veriam proveito na renovação do consentimento.

Na impossibilidade legal, de outra forma, de tratar dados de saúde para a execução de contratos de seguro, o insucesso do segurador na obtenção de novos consentimentos inviabilizaria a execução de uma proporção muito significativa de tais contratos e, com ela, a própria subsistência dos mesmos. As consequências sociais e económicas de tal cenário seriam, uma vez mais, dramáticas.

VI - Impõe-se uma palavra conclusiva sobre o consentimento como fonte de licitude para o tratamento de dados de saúde que sejam necessários à execução de um contrato, designadamente de seguro.

Como vimos, há uma notória dificuldade de preenchimento dos requisitos do consentimento, tal como resultam atualmente do RGPD[77]. Ora, quando não se verifiquem esses requisitos, a respetiva consequência será a invalidade do consentimento dado[78]. Porém, quando se conclua que, relativamente à tipologia de situações e de tratamentos de dados, os requisitos do consentimento são, pura e simplesmente, insuscetíveis (impossíveis) de verificar-se, a consequência deveria ser, não a invalidade do consentimento, mas a desqualificação (por impossível) do requisito em causa como condição de validade do consentimento[79].

[77] Cfr. Elena Gil González, *Big Data, Privacidad y Protección de Datos*, *cit*., p. 122.

[78] Ana Alves Leal, "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", *cit*., p. 147.

[79] Ana Alves Leal, "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", *cit*., p. 152.

Para além de um claro desfasamento entre o RGPD e algumas vertentes da realidade social, económica e tecnológica que visa regular, fica a conclusão de que o consentimento, nos moldes e com os requisitos traçados, assume um caráter efémero e precário que é incompatível com a função de suporte legitimador do tratamento de dados de saúde quando este se revela necessário à execução de um contrato de que o titular seja parte. Em síntese, o tratamento de dados de saúde não pode basear-se no consentimento.

7 – Perspetivas de solução: a fonte de licitude nos seguros obrigatórios

I – Cumpre agora passar da esfera do problema jurídico enunciado para a das soluções normativas proporcionadas no quadro do RGPD.

Para tanto, como melhor veremos, importa distinguir – e focarmo-nos, por ora – no tratamento de dados de saúde no contexto dos seguros legalmente obrigatórios, cujo leque é diversificado. Entre eles figuram vários seguros de responsabilidade civil passíveis de cobrir danos corporais nos terceiros lesados, destacando-se, pela sua relevância social e económica, o seguro obrigatório de responsabilidade civil automóvel (doravante, SORCA). Não menos relevantes são o seguro obrigatório de acidentes de trabalho (quer seja celebrado por conta própria ou por conta de outrem), ou várias situações de seguros obrigatórios de acidentes pessoais.

É sabido, dispensando especial desenvolvimento, que, para poder regularizar um sinistro automóvel em que o terceiro lesado tenha sofrido um dano corporal, o segurador terá de avaliar as causas, dimensão e sequelas desse dano, o que não permite prescindir do tratamento de dados de saúde. Outro tanto ocorrerá com um sinistro de acidente de trabalho ou de acidentes pessoais. Qual, então, a particularidade destes seguros, a justificar a autonomização da sua análise?

II – Desde logo, o facto de se tratar de seguros *obrigatórios*, o que os reveste de especiais características. Assim, embora o seguro obrigatório consista num contrato celebrado entre o segurador e o tomador do seguro, a disciplina que regula as relações contratuais das partes resulta de um regime injuntivo estabelecido por lei. Este regime, de fonte legal, traduz-se, frequentemente, num clausulado uniforme. Verifica-se, assim, uma limitada liberdade contratual das partes[80], no âmbito da qual as obrigações emergentes do contrato resultam, não da faculdade de estipulação, mas de normas legais injuntivas. Frequentemente, como sucede

[80] Aurelio Donato Candian, *Responsabilità Civile e Assicurazione*, Milano, Egea, 1993, p. 358; Filipe Albuquerque Matos, "O contrato de seguro obrigatório de responsabilidade civil automóvel: Breves considerações", *in* Júlio Gomes (Coord.), *Estudos Dedicados ao Prof. Doutor Mário Júlio Almeida Costa*, Lisboa, Universidade Católica Portuguesa, 2002, pp. 608 ss.; Afonso Moreira Correia, "Seguro obrigatório de responsabilidade civil automóvel – Direito de regresso da seguradora", *in* António Moreira e M. Costa Martins (Coords.), *II Congresso Nacional de Direito dos Seguros – Memórias*, Coimbra, Almedina, 2001, p. 198. Com efeito, o tomador do seguro não tem liberdade de não contratar, mas apenas de escolha da contraparte. Relativamente ao segurador, o mesmo pode não explorar o ramo em causa, ou recusar o risco que lhe é proposto ou definir a tarifa aplicável e ajustar o prémio concreto às características do risco – Luís Poças, *Seguro Automóvel – Oponibilidade de Meios de Defesa aos Lesados,* Coimbra, Almedina, 2018, pp. 14-15.

com o SORCA ou com o seguro de acidentes de trabalho, os deveres de conduta do segurador transcendem o próprio contrato, resultando diretamente de comandos legais.

A *necessidade*, para o segurador, de tratamento de dados de saúde resulta, no caso do SORCA, designadamente, das disposições injuntivas dos artigos 35.º, 37.º e 39.º do Decreto-Lei n.º 291/2007, de 21 de agosto – Lei do SORCA, doravante LSORCA, sendo inerente (ou um pressuposto lógico) do cumprimento de uma obrigação legal. Por seu turno, quanto ao seguro de acidentes de trabalho, aquela necessidade verte, designadamente, dos artigos 19.º ss.; 23.º ss.; 25.º ss.; 48.º ss.; etc., da Lei dos Acidentes de Trabalho (Lei n.º 98/2009, de 4 de setembro).

Mas porque se preocupa o legislador em disciplinar injuntivamente estes contratos de seguro, em vez de deixar ao normal funcionamento do mercado (e da liberdade contratual das partes) a estipulação da disciplina aplicável? Precisamente porque se trata de seguros obrigatórios, cujo intuito de proteção social se evidencia por si próprio. Assim, logo o preâmbulo da LSORCA alude ao propósito de atualização do sistema de proteção dos lesados por acidentes de viação baseado no SORCA e de aumento da proteção desses lesados. A própria Diretiva Codificadora Automóvel (Diretiva 2009/103/CE, de 16 de setembro), que procedeu à codificação, num único diploma, das disposições contidas nas cinco diretivas automóveis que a precederam, alude recorrentemente (considerandos 12, 21, 29, 30 e 31) ao propósito, subjacente à legislação europeia na matéria, de proteção das vítimas de acidentes de viação. Essa função de proteção social, relativamente às vítimas de acidente rodoviário, é também evidenciada, quer pela jurisprudência – nacional

e da UE[81] – quer pela doutrina[82]. Também no caso do seguro de acidentes de trabalho o propósito de proteção social do trabalhador exposto a riscos de acidente é patente[83].

[81] Cfr., por exemplo, Ac. STJ de 18/12/2002 – Proc. 2B3891 (Moitinho de Almeida), http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/ac0ad956c57d941c80256ce10035e2a6?OpenDocument&Highlight=0,moitinho,autom%C3%B3vel (consult. 13/10/2018); Ac. TJ de 28/03/1996 – Proc. n.º C-129/94 (caso *Ruiz Bernáldez*), http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130d508646c29cf6542debf7cfc74e5fc6d46.e34KaxiLc3eQc40LaxqMbN4PaNiPe0?text=&docid=99719&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=1799316 (consult. 13/10/2018); Ac. TJ de 30/06/2005 – Proc. n.º C-537/03 (caso *Katja Candolin*) – Cfr. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62003CJ0537&from=GA (consult. 12/10/2018); Cfr. Ac. TJ de 19/04/2007 – Proc. n.º C-356/05 (caso *Elaine Farrell*), https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62005CJ0356&from=EN (consult. 12/10/2018); Ac. TJ de 17/03/2011 – Proc. n.º C-484/09 (caso *Carvalho Ferreira Santos*), https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62009CJ0484&from=PT (consult. 13/10/2018); Ac. TJ de 11/07/2013 – Proc. n.º C-409/11 (caso *Csonka e o.*), https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62011CJ0409&from=EN (consult. 13/10/2018); Ac. TJ de 20/07/2017 – Proc. n.º C-287/16 (caso *Fidelidade – Companhia de Seguros*), http://curia.europa.eu/juris/document/document.jsf?text=&docid=193034&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=240772 (consult. 13/10/2018).

[82] Cfr., por exemplo, Jorge Sinde Monteiro, *Estudos Sobre a Responsabilidade Civil*, Coimbra, s.n., 1983. Como refere o autor, chamando a atenção, na reparação do dano por acidente de circulação, para uma passagem de um paradigma de justiça comutativa para outro de justiça distributiva, «o problema da reparação dos danos pessoais não é hoje em dia algo que diga respeito ao lesante e ao lesado, mas a toda a coletividade; porque isto é assim, as técnicas tradicionais, individualistas por natureza, tendem a ser substituídas por outras que procuram resolver os problemas numa perspetiva social global» - p. 116.

[83] Esse propósito resulta, designadamente, da configuração que o próprio acidente de trabalho veio a assumir ao longo do tempo, com os contornos progressivamente mais abrangentes que a lei e a jurisprudência têm vindo a

A função de proteção social dos seguros obrigatórios – no sentido da tutela dos sujeitos lesados em consequência de uma atividade cujo grau de risco suscita a proteção do Direito – é, portanto, notória e manifesta[84]. É, de resto, o que justifica o seu caráter obrigatório e, consequentemente, universal.

III – Mas os seguros obrigatórios encerram ainda uma outra particularidade. Com efeito, e à exceção de casos pontuais – como os seguros de acidente de trabalho por conta própria – em regra, os titulares dos dados de saúde cujo tratamento é requerido em sede de execução do contrato não são parte do mesmo, mas sim *terceiros*.

Desta forma, mesmo que a alínea b) do n.º 1 do artigo 6.º do RGPD encontrasse equivalente no artigo 9.º, relativamente às categorias especiais de dados, ainda assim a referida fonte de licitude não seria aplicável a estes casos, em virtude de os titulares não serem parte do contrato.

IV – Tudo visto, pensamos que o tratamento de dados de saúde necessário para a execução de seguros obrigatórios encontra a sua fonte de licitude na alínea b) do n.º 2 do artigo 9.º do RGPD[85]. Com efeito, refere esta disposição que o tratamen-

esculpir. Cfr. Júlio Vieira Gomes, *O Acidente de trabalho – O Acidente In Itinere e a sua Descaracterização*, Coimbra, Coimbra Ed., 2013.

[84] Antigono Donati e Giovanna Volpe Putzolu, *Manuale di Diritto delle Assicurazioni*, 8ª Ed., Milano, Giuffrè Editore, 2006, p. 237; Luís Poças, *Seguro Automóvel – Oponibilidade de Meios de Defesa aos Lesados*, *cit*., pp. 11-12 e 14.

[85] Quando não estejam em causa categorias especiais de dados, a fonte de legitimação decorrerá, já não, como vimos, da alínea b) do n.º 1 do artigo 6.º do RGPD (necessidade para a execução de um contrato *de que o titular seja parte*) mas da alínea c) do mesmo n.º (necessidade para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito).

to de categorias especiais de dados é lícito se «for necessário para efeitos do *cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social*, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados».

Como julgamos ter demonstrado, esse tratamento é, de facto: (i) *necessário*; (ii) para o cumprimento de *obrigações* do responsável pelo tratamento (e do exercício de direitos específicos do titular dos dados), as quais decorrem de normas injuntivas da legislação que rege os seguros obrigatórios em causa; (iii) essa legislação é de natureza laboral (no que toca, designadamente, aos seguros de acidentes de trabalho[86]) e, em qualquer caso, de *proteção social*, função indelevelmente associada ao caráter obrigatório (e, portanto, universal) do seguro.

Como resulta do considerando 45 do RGPD (e decorre também das traduções oficiais do regulamento na generalidade das outras línguas), a obrigação *jurídica* consiste numa obrigação *legal*, e não de fonte contratual – também neste sentido, Ana Alves Leal, "Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação", *cit.*, p. 164. Em qualquer caso, é essa a natureza das obrigações injuntivamente estabelecidas por lei para os seguros obrigatórios.

[86] No caso do seguro de acidentes de trabalho, a respetiva obrigatoriedade é estabelecida no n.º 5 do artigo 283.º do Código do Trabalho e no n.º 1 do artigo 79.º da Lei dos Acidentes de Trabalho, assumindo ambos os diplomas natureza laboral.

V – A conjugação de referências, na alínea b) do n.º 2 do artigo 9.º do RGPD, a *legislação laboral* e a *convenção coletiva* permite ainda, para além do perímetro acima traçado, alargar o âmbito do tratamento de dados de saúde legitimado à luz desta disposição. Com efeito, um domínio extremamente relevante da atividade seguradora consiste nos designados seguros de *employee benefits*, compreendendo seguros de vida, de saúde e de acidentes pessoais contratados pela entidade patronal a favor dos respetivos trabalhadores e enquadrado, em regra, por instrumentos de regulamentação coletiva de trabalho (IRCT) que preveem a sua contratação como parte do pacote remuneratório.

Neste contexto, estamos também perante seguros obrigatórios, na medida em que a entidade patronal fica vinculada pelo IRCT aplicável, decorrendo da Lei a obrigatoriedade da observância deste e as consequências, civis e contraordenacionais, do seu incumprimento (respetivamente, n.º 3 do artigo 520.º e artigo 521.º do Código do Trabalho). É certo que – diversamente do que sucede com os seguros cuja obrigatoriedade resulta diretamente da lei (como o SORCA ou o seguro de acidentes de trabalho) – em regra, em matéria de *employee benefits*, não decorrem da lei laboral ou do IRCT deveres para o responsável pelo tratamento (o segurador), deveres esses que vertem, sim, do próprio contrato de seguro. Cremos, porém, que o enquadramento no domínio da legislação laboral (a que acresce a referência do RGPD ao tratamento permitido por convenção coletiva[87]), o propósito de proteção social e o caráter obrigatório do seguro, permitem estender a estes casos, no seu conjunto,

[87] Esta permissão não carecerá de ser expressa e dirigida ao segurador, que não é parte na convenção coletiva. Com efeito, sendo estabelecida por IRCT a obrigatoriedade da contratação do seguro pelo empregador, o tratamento (pelo segurador) dos dados necessários será forçosamente permitido, ou ficaria

a *ratio* das outras situações de seguro obrigatório, a justificar o mesmo fundamento legitimador do tratamento.

Em suma, no caso dos seguros obrigatórios o problema da licitude do tratamento de dados de saúde encontra solução na alínea b) do n.º 2 do artigo 9.º do RGPD.

8 – As soluções de licitude nos seguros facultativos

8.1 – Obrigações emergentes de legislação de proteção social

I – Se o tratamento de dados de saúde em seguros obrigatórios encontra, como vimos, respaldo na b) do n.º 2 do artigo 9.º do RGPD, a solução será menos evidente no que respeita aos seguros facultativos. Quanto aos requisitos desta disposição, não se suscitarão dúvidas quanto ao caráter necessário do tratamento. As dúvidas colocar-se-ão, sim, quanto à existência de uma obrigação jurídica (de fonte legal) do responsável (o segurador) e, por outro lado, quanto à natureza da legislação de onde a mesma provenha.

II – Vejamos, em primeiro lugar, se, e em que medida, poderemos considerar o enquadramento dos seguros de pessoas facultativos (seguros de vida, de saúde e de acidentes pessoais) em matéria de legislação de *proteção social*.

Neste domínio, embora a regulação dos seguros facultativos de pessoas não surja propriamente em legislação de segu-

inviabilizado, na prática, o cumprimento da obrigação de contratação do seguro pelo empregador.

rança social, cremos ser pacífico (e dispensando, portanto, uma demonstração aturada) que tais seguros se destinam precisamente a complementar o regime de proteção social consagrado pelo Sistema Previdencial de Segurança Social. Com efeito, os riscos cobertos por estas modalidades de seguro coincidem com eventualidades garantidas por aquele sistema (bem como pelo sistema nacional de saúde), acrescendo à proteção social conferida pelos mesmos. Constituem, desta forma, soluções voluntárias (facultativas) de complemento aos referidos sistemas, assumindo, portanto, fins de proteção social.

E vários são os exemplos demonstrativos desta asserção. Desde logo, o artigo 84.º da própria Lei de Bases da Segurança Social (Lei n.º 4/2007, de 16 de janeiro), esclarece que «os regimes complementares [de segurança social] de iniciativa individual são de instituição facultativa, assumindo, entre outras, a forma de planos de poupança-reforma, de *seguros de vida*, de seguros de capitalização e de modalidades mutualistas».

Mais clarificadora e abrangente é a conclusão que podemos extrair do n.º 3 do artigo 76.º do Código dos Regimes Contributivos do Sistema Previdencial de Segurança Social. Aí se estabelece que «não integra o conceito de remuneração mensal efetiva as importâncias despendidas pela entidade empregadora, a favor do trabalhador, na constituição de *seguros de doença, de acidentes pessoais e de seguros de vida que garantam exclusivamente o risco de morte, invalidez* ou reforma por velhice, no último caso desde que o benefício seja garantido após os 55 anos de idade, desde que não garantam o pagamento e este se não verifique nomeadamente por resgate ou adiantamento de qualquer capital em vida durante os primeiros cinco anos». A *ratio* do preceito é cristalina: constituindo os

seguros de vida, de saúde e de acidentes pessoais uma extensão complementar da proteção social conferida pelo Sistema Previdencial de Segurança Social e pelo Sistema Nacional de Saúde, não faria sentido que as importâncias despendidas pela entidade empregadora, a favor do trabalhador, para a aquisição de tais seguros, fossem consideradas como remuneração efetiva do trabalhador, ficando sujeitas a contribuições para a segurança social. A não sujeição a tais contribuições é demonstrativa, portanto, da referida complementaridade e do propósito comum de proteção social.

Num outro exemplo, estabelece o n.º 2 do artigo 43.º do Código do IRC que são considerados gastos, enquanto *realizações de utilidade social*, do período de tributação, até ao limite de 15 % das despesas com o pessoal contabilizadas a título de remunerações, ordenados ou salários respeitantes ao período de tributação, os suportados com contratos de *seguros de acidentes pessoais, bem como com contratos de seguros de vida, de doença ou saúde* (neste caso, em benefício dos trabalhadores, reformados ou respetivos familiares) contribuições para fundos de pensões e equiparáveis ou para quaisquer regimes complementares de segurança social, que garantam, exclusivamente, o benefício de reforma, pré-reforma, complemento de reforma, benefícios de saúde pós-emprego, invalidez ou sobrevivência a favor dos trabalhadores da empresa. De novo, a dedutibilidade fiscal consagrada no preceito atende precisamente aos fins de proteção social inerentes aos gastos em causa.

Reflexamente, verifica-se, quanto a tais gastos, para os trabalhadores com eles beneficiados, uma exclusão de tributação em sede de IRS, nos termos das alíneas a) e b) do n.º 1 do artigo 2.º-A do Código do IRS. Aí se estabelece que não se consideram

rendimentos do trabalho dependente as prestações efetuadas pelas entidades patronais para regimes obrigatórios de segurança social, *ainda que de natureza privada*, que visem assegurar exclusivamente benefícios em caso de reforma, invalidez ou sobrevivência, bem como os benefícios imputáveis à utilização e fruição de *realizações de utilidade social* mantidas pela entidade patronal, desde que observados os critérios estabelecidos no referido artigo 43.º do Código do IRC. De novo, para promover as mencionadas medidas complementares de *proteção social*, o legislador fiscal exonera de tributação os beneficiários das mesmas.

Crendo que sem necessidade de outros exemplos demonstrativos do enquadramento legal de proteção social dispensado aos seguros de saúde[88], de vida e de acidentes pessoais[89], importa verificar se do regime legal aplicável decorrem obrigações para o responsável pelo tratamento (o segurador)

[88] A própria CNPD reconhece o caráter de proteção social dos seguros de saúde, embora, inexplicavelmente, não o reconheça também quanto aos seguros de vida nem de acidentes pessoais: «o contrato por si só não é condição de licitude para tratar dados sensíveis, e a alínea b) do n.º 2 daquele artigo [9.º] limita a intervenção do legislador nacional às matérias de legislação laboral, de segurança social e de proteção social. Deste modo, *apenas se poderia enquadrar aqui os seguros de saúde*, na medida em que se possa considerá-los ainda como uma forma de proteção social» – Parecer n.º 20/2018, da CNPD, de 02/05/2018, *cit*., p. 37 v.

[89] A demonstração efetuada, com remissão para vários exemplos de disposições legais, assume relevância quanto aos seguros de *employee benefits* não previstos em IRCT. Essa previsão, a existir, conferiria já, como defendemos na secção anterior, caráter obrigatório aos seguros em causa, justificando então um mais claro enquadramento na fonte de licitude a que se reporta a alínea b) do n.º 2 do artigo 9.º do RGPD.

relativamente às quais o tratamento de dados de saúde seja necessário.

III – Vimos que a necessidade tratamento de dados de saúde em seguros se coloca tanto na fase pré-contratual (análise do risco) como na de execução do contrato, designadamente para a regularização do sinistro.

O dever, a cargo do segurador, de análise e seleção criteriosas do risco, e de adequação ao mesmo das condições tarifárias aplicáveis, poderá configurar-se como um ónus no plano meramente contratual (da relação entre o segurador e o tomador do seguro), mas consiste num verdadeiro *dever* legal no plano do exercício da atividade seguradora (de relação entre o segurador e a mutualidade de segurados, ou entre aquele e a ASF).

Com efeito, o Regime Jurídico de Acesso e Exercício da Atividade Seguradora e Resseguradora (doravante, RJASR), aprovado pela Lei n.º 147/2015, de 9 de setembro, estabelece um sistema de regras que, visando a proteção dos tomadores de seguros, segurados e beneficiários, requerem uma gestão sã e prudente dos seguradores e o controlo de riscos associados à atividade seguradora, entre eles, o de subscrição (análise do risco proposto em sede de subscrição e adequação ao mesmo das condições contratuais aplicáveis). Para tanto, e sem prejuízo de outras disposições, o n.º 1 do artigo 72.º (sob a epígrafe *sistema de gestão de riscos*), estabelece que as empresas de seguros e de resseguros devem dispor de um sistema de gestão de riscos eficaz que compreenda a estratégias, processos e procedimentos de prestação de informação que permitam, a todo o tempo, identificar, mensurar, monitorizar, gerir e comunicar os riscos, de forma individual e agregada, a que estão ou podem vir a estar expostas e as respetivas interdependências. Ora, nos termos

da alínea a) do n.º 4 do mesmo artigo, o sistema de gestão de riscos abrange, precisamente, a *subscrição*. Desta forma, está o segurador obrigado a uma seleção criteriosa do risco subscrito, para o que não pode, no caso dos seguros de pessoas, deixar de tratar os dados de saúde indispensáveis a tal análise e seleção.

Mas também do RJCS vertem deveres legais para o segurador que implicam o tratamento de dados de saúde em sede de subscrição do contrato. Assim, e sem preocupações de exaustividade, do n.º 3 do artigo 24.º do RJCS resulta, como desenvolvidamente sustentamos noutro escrito[90], um verdadeiro *dever legal* de cooperação e controlo, pelo segurador, da declaração do risco, cominando o seu incumprimento com a sanção de inimpugnabilidade do contrato (inoponibilidade da anulabilidade)[91] [92]. Por outro lado, resultam literalmente de outras disposições, como o artigo 178.º do RJCS, deveres a cargo do segu-

[90] Cfr. Luís Poças, *O Dever de Declaração Inicial do Risco no Contrato de Seguro*, *cit*., pp. 383-450, sobretudo pp. 391 ss.

[91] Embora a heterogeneidade de situações abrangidas pela enumeração enunciativa do n.º 3 do artigo 24.º do RJCS obscureça a sua *ratio*, este preceito terá por fundamento unitário o abuso do direito e, em particular, o *venire contra factum proprium*. Neste quadro, as alíneas a) a c) do n.º 3 do artigo 24.º referem-se a *falhas manifestas* na declaração do risco, incluindo incoerências; contradições; referências ilegíveis ou incompreensíveis; informações imprecisas; omissões de resposta; etc. Por seu turno, e em parcial sobreposição, as alíneas d) e e) do n.º 3 do artigo 24.º abrangem factos culposamente desconhecidos (ou não atualmente representados) pelo segurador ou pelo seu representante.

[92] Identificando também no preceito um dever legal a vincular o segurador, Arnaldo Oliveira, "Artigo 24.º – Anotação", *in* Pedro Romano Martinez *et al*., *Lei do Contrato de Seguro Anotada*, 3ª Ed., Coimbra, Almedina, 2016, p. 134. Como refere o autor, do n.º 3 do artigo 24.º resulta um dever «*de verificação do declarado cujo teor e circunstâncias sejam de molde a razoavelmente levantar suspeitas de inexatidão ou falsidade a um profissional medianamente*

rador que necessariamente implicam, nos seguros de pessoas, o tratamento de dados de saúde.

Igualmente em sede de execução do contrato – em especial, aquando da participação do sinistro – o segurador está obrigado ao cumprimento de vários deveres legais, decorrentes do RJCS, que implicam, em regra, o tratamento de dados de saúde em seguros de pessoas. Com efeito, estabelece-se no n.º 1 do artigo 102.º deste diploma que o segurador se *obriga* a satisfazer a prestação contratual a quem for devida, *após a confirmação da ocorrência do sinistro e das suas causas, circunstâncias e consequências*[93], acrescentando o n.º 2 que, para esse efeito, dependendo das circunstâncias, pode ser necessária a prévia quantificação das consequências do sinistro.

IV – Em suma, cremos ter demonstrado que também relativamente aos seguros facultativos de pessoas se verificam os requisitos da alínea b) do n.º 2 do artigo 9.º do RGPD. De facto, assumindo os seguros facultativos de pessoas, nos termos do respetivo enquadramento legal, caráter de proteção social, de tal enquadramento decorre também a existência de deveres legais, incidindo sobre o responsável pelo tratamento (o segurador), para cujo cumprimento é necessário o tratamento de dados de saúde. O tratamento será, portanto, lícito à luz da alínea b) do n.º 2 do artigo 9.º do RGPD.

8.2 – Serviços de saúde ou de ação social

diligente, sem prejuízo, naturalmente, do dever do tomador do seguro e do segurado de cumprimento diligente da declaração inicial do risco» (*ibidem*).

[93] Nos termos do artigo 104.º do RJCS, a obrigação do segurador vence-se decorridos 30 dias sobre o apuramento destes factos.

I – Ainda que se considere que a alínea b) do n.º 2 do artigo 9.º do RGPD não alberga um fundamento de licitude para o tratamento de dados de saúde em seguros facultativos de pessoas, o regulamento proporciona, do nosso ponto de vista, outras soluções normativas onde ancorar esse fundamento de licitude.

Assim, nos termos da alínea h) do n.º 2 do artigo 9.ºdo RGPD, o tratamento de dados de saúde é lícito se «for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3». Por seu turno, acrescenta o referido n.º 3 que «os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes»[94].

[94] Sem prejuízo da limitação às finalidades estabelecidas na referida alínea h), em virtude do caráter evolutivo das problemáticas associadas às categorias especiais de dados, é dada margem aos Estados-Membros para manter as condições estabelecidas no RGPD; para definir condições adicionais; ou para estabelecer limitações ao RGPD (n.º 4 do artigo 9.º). Cfr. Javier Puyol Montero, "Los principios del derecho a la protección de datos", *cit.*, p. 148.

II – Abstraindo das referências à medicina do trabalho, encontramos na citada alínea h) vários requisitos: (i) *as finalidades* do tratamento, que hão de assentar na medicina preventiva, no diagnóstico médico, na prestação de cuidados ou tratamentos de saúde ou de ação social, ou na gestão de sistemas e serviços de saúde ou de ação social; (ii) *o enquadramento* em que repousa o tratamento, que há de ser o Direito da União ou dos Estados-Membros ou um contrato com um profissional de saúde; e (iii) o tratamento por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade.

Começando pelo terceiro requisito, logo o damos por verificado face ao dever de sigilo profissional que incide sobre o segurador e que é extensivo aos administradores, trabalhadores, agentes e demais auxiliares do segurador (não cessando com o termo das respetivas funções), nos termos do artigo 119.º do RJCS.

Quanto às finalidades, haverá que reconhecer que a expressão *ação social* é algo imprecisa e ambígua. Apoiando-nos em várias versões oficiais do Regulamento, encontramos expressões como *social care* (inglês), *asistencia social* (espanhol), *protection sociale* (francês), *servizi sociali* (italiano), ou *Sozialbereich* (alemão). Na verdade, não nos encontramos numa dimensão diversa da *proteção social* referida na alínea b) do n.º 2 do artigo 9.º (a tradução oficial francesa, por exemplo, utiliza a mesma expressão em ambas as alíneas). Ora, como vimos, a gestão de contratos de seguros de pessoas não se encontra fora deste domínio. Em particular, os seguros de saúde têm precisamente por finalidade – e são, portanto, instrumentais – da prestação de cuidados de medicina preventiva, de

diagnóstico médico e da prestação de cuidados ou tratamentos de saúde. A gestão de seguros de saúde assume, portanto, uma identidade incontornável com a própria gestão de serviços de saúde, assim como a gestão de seguros de pessoas, em geral, encontra o mesmo paralelismo na gestão de serviços de ação ou proteção social.

Por fim, quanto ao enquadramento do tratamento de dados no Direito da União ou dos Estados-Membros, o mesmo foi já referenciado na análise à alínea b) do n.º 2 do artigo 9.º. Mas ainda que tal enquadramento faltasse, sempre relevaria uma palavra quanto à referência feita a um contrato com um profissional de saúde. Como já referimos, a única menção que encontramos a um fundamento de caráter contratual, entre as fontes de licitude do tratamento previstas para categorias especiais de dados (artigo 9.º do RGPD), é precisamente a que verte da citada alínea h). Ora, essa referência encontra o mesmo fundamento e justificação do que a fonte de licitude prevista na alínea b) do n.º 1 do artigo 6.º do RGPD. Na verdade, não faria sentido que o titular dos dados celebrasse um contrato com um profissional de saúde (implicando, por natureza, o tratamento de dados clínicos), mas pretendesse vedar esse tratamento. É o caráter de inerência do tratamento (e, portanto, um consentimento presumido) que justifica a fonte de legitimação prevista. Ora, também aqui há total paralelismo com os seguros de vida, saúde e acidentes pessoais, aos quais é inerente o tratamento necessário de dados de saúde, de tal modo que o titular não poderá querer a contratação daqueles sem anuir no indispensável tratamento.

III – Face ao exposto, pensamos que a letra da alínea h) do n.º 2 do artigo 9.º comporta já o sentido de que é lícito, desig-

nadamente, o tratamento de dados de saúde quando necessário para a subscrição e execução de contratos de seguro de vida, de saúde e de acidentes pessoais, na medida em que os mesmos consubstanciam a *gestão de serviços de saúde ou de ação social* e que, em qualquer caso, os seguros de saúde visam a prestação de cuidados de medicina preventiva, o diagnóstico médico e a prestação de cuidados ou tratamentos de saúde. Não obstante, mesmo considerando que a interpretação literal do preceito não alberga o referido sentido, sempre o mesmo resultará de uma interpretação extensiva de tal disposição.

Assim, e em suma, mesmo que se rejeitasse a alínea b) do n.º 2 do artigo 9.º como fonte de licitude para o tratamento de dados de saúde relativamente a seguros facultativos de pessoas, seria a alínea h) do mesmo número apta a fundamentar a licitude desse tratamento.

8.3 – Intervenção legislativa

I – Defendemos acima que o RGPD acolhe soluções normativas para o problema equacionado. Se se considerar que tal não é, porém, o caso, a solução teria de passar por uma hipotética intervenção legislativa. Neste contexto, algumas vias de abordagem se perspetivam.

Assim, noutros ordenamentos, registam-se intenções ou atuações do poder legislativo no sentido de assegurar uma solução legal para o problema que nos ocupa. Por exemplo, na Bélgica, perspetiva-se a aprovação de legislação que reconheça o tratamento de dados de saúde quando «necessário no quadro de uma finalidade legal (p. ex., a declaração do risco em seguros)»[95].

Outra abordagem resulta da alínea g) do n.º 2 do artigo 9.º. Aí se consagra a licitude do tratamento de dados de saúde se o mesmo «for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados»[96].

Desta forma, o reconhecimento expresso, pelo Direito português ou pelo Direito da União Europeia, de que os seguros facultativos de pessoas (seguros de vida, de saúde e de acidentes pessoais) – e, inerentemente, o tratamento de dados de saúde requerido pelos mesmos – se revestem de *interesse público importante*, constituiria, em conjugação com a citada alínea g) do n.º 2 do artigo 9.º (e verificados os demais requisitos desta alínea) fonte de licitude bastante para o dito tratamento.

[95] Charles-Albert van Oldeneel, "Protection des données: le GDPR applicable depuis de 25 mai 2018!", *cit.*, p. 288 (tradução nossa).

[96] Como se esclarece no considerando 45, «o presente regulamento não exige uma lei específica para cada tratamento de dados. Poderá ser suficiente uma lei para diversas operações de tratamento [...]. Deverá também caber ao direito da União ou dos Estados-Membros determinar qual a finalidade do tratamento dos dados. Além disso, a referida lei poderá especificar as condições gerais do presente regulamento que regem a legalidade do tratamento dos dados pessoais, estabelecer regras específicas para determinar os responsáveis pelo tratamento, o tipo de dados pessoais a tratar, os titulares dos dados em questão, as entidades a que os dados pessoais podem ser comunicados, os limites a que as finalidades do tratamento devem obedecer, os prazos de conservação e outras medidas destinadas a garantir a licitude e equidade do tratamento».

II – Esta mesma via de solução é enunciada no Parecer n.º 20/2018, da CNPD, de 02/05/2018. Aí se refere que «no mais, sobraria ainda a hipótese de o legislador, nos termos da alínea g) do mesmo número, considerar de interesse público importante o tratamento de dados de saúde na atividade seguradora»[97].

Segundo a CNPD, essa intervenção legislativa seria indispensável em virtude de não poder extrair-se do Direito vigente em Portugal que a atividade seguradora assumisse já caráter de interesse público importante. Como se refere no citado Parecer, «se se consegue acompanhar que no âmbito dos seguros obrigatórios é já reconhecido o interesse público importante, já o mesmo não acontece relativamente aos restantes seguros, designadamente os seguros de vida. Note-se que ainda que se possa reconhecer à atividade seguradora algum interesse público (enquanto atividade sujeita a regulação pública), muito dificilmente é suscetível de ser um interesse público qualificado, como exige aquela alínea g)»[98].

III – Alguma doutrina parece encontrar reservas ao tratamento de dados de saúde por seguradores por motivos de interesse público. Com efeito, entende Jorge Barros Mendes que as «atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como [...] as companhias de seguros [...]»[99].

[97] Parecer n.º 20/2018, da CNPD, de 02/05/2018, *cit*., p. 37 v.

[98] *Ibidem*.

[99] Jorge Barros Mendes, "O novo regulamento de proteção de dados: as principais alterações", *cit*., p. 22.

A observação do autor haverá, porém, de contextualizar-se numa outra fonte de licitude para o tratamento de dados de saúde. Com efeito, refere a alínea i) do n.º 2 do artigo 9.º que é lícito o tratamento «necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional». É quanto a esta alínea – e não a citada alínea g) – que o considerando 54 esclarece que «tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias».

IV – Em aparente contradição com as considerações tecidas sobre a virtualidade de uma intervenção legislativa futura, no quadro da alínea g) do n.º 2 do artigo 9.º do RGPD, no sentido do reconhecimento legal do interesse público da atividade seguradora, aponta ainda a CNPD um outro caminho. Com efeito, estabelece o n.º 4 do artigo 9.º do RGPD que «os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de [...] dados relativos à saúde».

Embora se afigure que a previsão do citado n.º 4 do artigo 9.º, quanto à possibilidade de *imposição de novas condições, incluindo limitações*, vai no sentido da restrição dos requisitos a que há de obedecer o tratamento de dados, e não da sua ampliação, ainda assim considera a CNPD que «para os seguros

que não sejam obrigatórios ou de saúde, apenas o n.º 4 do artigo 9.º poderá servir para legitimar os Estados-Membros a prever em lei novas condições do tratamento»[100].

IV – Em suma, e como tivemos oportunidade de sublinhar, do nosso ponto de vista o RGPD contém já solução, no seu normativo, que permite albergar o tratamento, pelo segurador, de dados de saúde em seguros facultativos de pessoas. Porém, ainda que assim se não entenda, haverá margem para uma intervenção legislativa no sentido, designadamente, do reconhecimento do importante interesse público dos seguros de pessoas, ficando então o tratamento legitimado nos termos da alínea g) do n.º 2 do artigo 9.º do RGPD.

Qualquer que seja o caminho de uma intervenção legislativa, considera a CNPD ser «imperioso que a lei nacional preveja não apenas a possibilidade de efetuar o tratamento de dados de saúde, mas também o respetivo regime do mesmo, designadamente, os limites a que necessariamente tem de estar sujeito e as medidas de segurança e de mitigação do impacto sobre os direitos dos titulares dos dados – o que, na perspetiva da CNPD, terá mais sentido ser concretizado na legislação que regula este setor de atividade»[101].

9 – O litígio como solução de recurso

I – Como sublinhámos já reiteradamente, o problema equacionado não se encontra, do nosso ponto de vista, sem solução

[100] Parecer n.º 20/2018, da CNPD, de 02/05/2018, *cit*., p. 37 v.

[101] Parecer n.º 20/2018, da CNPD, de 02/05/2018, *cit*., p. 38.

normativa no quadro do RGPD. Porém, num cenário em que a autoridade de controlo nacional em matéria de proteção de dados – a CNPD – não reconheça, para o tratamento de dados de saúde, por seguradores, em contratos de seguro facultativos de pessoas, as fontes de licitude que acima identificámos, fica a solução à mercê de uma intervenção legislativa. Esta, para além de incerta (quer quanto à sua verificação, quer quanto à sua eficácia), peca já, atualmente, por tardia.

Assim, no referido cenário, e na pendência de uma eventual intervenção legislativa, ficaria o segurador impedido de tratar dados de saúde da sua carteira de clientes. Por outras palavras, nos contratos em vigor (e não havendo fundamento, por qualquer das partes, para fazê-los cessar), não seria lícito ao segurador regularizar sinistros na medida em que os mesmos exigissem o tratamento de dados de saúde. Perante este impasse, o RGPD proporciona uma solução de recurso: o litígio.

Com efeito, recusando-se o segurador a efetuar a sua prestação contratual por sinistro (porquanto ilícita)[102], não restará à pessoa segura (ou aos beneficiários de um seguro de vida ou de acidentes pessoais) outra alternativa senão conformarem-se ou apelarem para um veredito do poder judicial.

Sucede que, como resulta da alínea f) do n.º 2 do artigo 9.º do RGPD, o tratamento de dados de saúde será já lícito quando «for necessário à declaração, ao exercício ou à defesa de

[102] Alberto Polotti di Zumaglia, "Profili civilistici e assicurativi della cartella clinica", *Diritto ed Economia dell'Assicurazione*, Ano 34, n.º 4 (out.-dez. 1992), p. 749; Sabine AbravanelJolly, "Le secret médical en assurance de personnes", *cit*., p. 888.

um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional».

Em suma, portanto, ao não reconhecer a licitude do tratamento de dados de saúde necessários à execução de um contrato de que o titular seja parte, o RGPD, na falta de outra solução, seria um promotor de litígios, única porta de licitude à regular execução de tais contratos. Esta lógica normativa revela-se, porém, tão surreal e desconcertante que não poderá ser aceite sem as maiores reservas[103].

II – A solução, sendo paradoxal no quadro do RGPD e do tratamento de dados, arriscar-se-ia também a ser injusta quanto à questão material de fundo. Com efeito, não será inédito que o tribunal entenda que a *necessidade* de tratamento de dados de saúde é, essencialmente, um problema do segurador, e não do titular dos dados (pessoa segura) ou dos beneficiários de um seguro de vida. Assim, ao segurador cumpriria efetuar a sua prestação por sinistro, cabendo-lhe o ónus de alegar e demonstrar os meios de defesa de que dispusesse, independentemente da necessidade que tivesse, para o efeito, de tratar dados de saúde (tratamento não autorizado ou considerado ilícito pelo tribunal).

Tal foi, por exemplo, o teor do Ac. TRL de 21/06/2012 – Proc..º 208/10.0YXLSB.L1-2 (Sérgio Almeida)[104], em cujo sumário pode ler-se:

[103] Sobre a solução, no quadro da LPD, cfr. Luís Poças, *O Dever de Declaração Inicial do Risco no Contrato de Seguro*, *cit*., pp. 850-851.

[104] http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/bcda3a2d05d99f9b80257a470050b355?OpenDocument (consult. 12/10/2018).

"I. Os dados relativos à saúde são pessoais, contêm-se na esfera privada do sujeito e estão protegidos pela lei fundamental e pela lei ordinária. II. Perecendo o segurado num contrato de seguro de vida a obtenção de dados sobre o seu estado de saúde e causas de morte importa invasão da esfera da vida privada do segurado, que continua a ser protegida, não tendo o beneficiário livre acesso aos dados do falecido, salvo se este o tiver autorizado de forma livre, específica e informada. III. Cabe à seguradora pagar a importância segura ao beneficiário verificada a morte do segurado, a menos que ocorra qualquer facto que exclua a sua responsabilidade. IV. O ónus da prova de tal exclusão recai sobre a seguradora[105] [106].

[105] Veja-se também, a propósito, o Ac. TRP de 07/11/2005 – Proc. 554793 (Martins Lopes). Numa ação interposta contra um segurador para cumprimento de um contrato de seguro de vida, alegou a Ré «que quando lhe foi participada a morte do tomador do seguro D, solicitou certidão de óbito com a causa da morte. E, no caso de ter sido provocada por doença, também o relatório do médico assistente. Acontece que à Ré, apenas foi enviado o assento de óbito, onde refere apenas o falecimento, sem referência à causa da morte. Entende a Ré que, para que possa dar cumprimento às suas obrigações que emergem do contrato que celebrou com o tomador do seguro, necessita de saber quais as causas que provocaram a ocorrência da morte. Tão só porque a mesma pode estar diretamente incluída nas exclusões abrangidas no art.º 10º das condições contratuais da apólice (riscos excluídos). Como também pode ter sido provocada por doença que o tomador do seguro tenha omitido no questionário médico que acompanhou proposta de seguro». [...] Assim, decidiu o acórdão no sentido de «sobre ela, Seguradora, recair o ónus de alegação e prova no sentido de demonstrar toda uma factualidade suscetível de conduzir com segurança à convicção de que uma Pessoa Segura se encontra numa situação de exclusão [...]». Cfr. http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/31899f43162d8f5e802570c00044fecd?OpenDocument (consult. 16/10/2018).

É também, por vezes, sublinhada a instrumentalização, pelo titular dos dados e ao sabor das conveniências[107], dos seus direitos, privando o segurador de meios de defesa probatórios. Assim, o segredo sobre dados clínicos, cujo levantamento depende do consentimento do titular, confere-lhe uma autêntica imunidade, podendo ser perspetivado como um verdadeiro instrumento de fraude nos seguros de pessoas[108].

[106] Considere-se também como exemplo o Ac. TRL de 17/03/2011 – Proc. n.º 2360/08.6YXLSB.L12 (Maria José Mouro), onde se considerou que «no âmbito de um contrato de seguro – ramo vida – nos termos do nº 2 do art. 342 do CC compete à seguradora, R. no processo, a prova de que o segurado produziu declarações inexatas ou reticentes quando da celebração do contrato» e que «da circunstância de se ter apurado que o tomador do seguro faleceu em 22 de abril de 2007 constando do certificado de óbito que a causa direta da morte foi meningite criptocócica devida ou consecutiva a infeção por vírus da imunodeficiência humana *não resulta necessariamente que à data de celebração do contrato de seguro (em 11 de outubro de 2006), quando respondeu ao inquérito clínico, tivesse conhecimento da sua infeção por aquele vírus (nem mesmo que a devesse conhecer)*». Em consequência, e porque «a documentação [clínica sobre a data do diagnóstico da doença] não foi obtida dada a posição assumida pelo Centro Hospitalar de Setúbal, no sentido de não ser autorizado o acesso das seguradoras à informação clínica de um segurado para efeito de instrução de processo relativo a seguro de vida», foi a seguradora condenada ao pagamento da sua prestação. Cfr. http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/9c0e1cafd56e83c68025788e0035577a?OpenDocument (consult. 16/10/2018).

[107] Nota Durry que «se o segurado ou os seus herdeiros não têm nada a esconder, apressam-se a solicitar os certificados médicos que apresentarão ao segurador, já que, para eles, não há lugar a segredo médico. Em contrapartida, se receiam revelações inconvenientes, não somente não apresentam qualquer certificado, mas ainda proibirão, em nome do segredo médico, aqueles que sabem, de produzir qualquer informação a terceiros» Georges Durry, "Le secret médical opposé à l'assureur: la fin des incertitudes?", *Risques*, n.º 61 (jan.-mar. 2005), p. 132 (trad. nossa).

10 – Conclusões

Considerando a aparente falta de uma fonte de licitude para o tratamento, por parte dos seguradores, de dados pessoais de saúde na celebração e execução de contratos de seguro, foram apresentadas e discutidas várias hipóteses de solução, partindo do enquadramento normativo do tema e da identificação dos principais traços caracterizadores do RGPD.

Neste contexto, foi, desde logo, demonstrada a *necessidade* do tratamento de tais dados, pelo segurador – mormente, no caso dos seguros de pessoas – de tal modo que esse tratamento é imprescindível à gestão dos referidos contratos. Porém, constatou-se que, diversamente do que ocorre quanto à generalidade dos dados pessoais, a disposição que regula a licitude do tratamento das categorias especiais de dados não reconhece a licitude do tratamento quando o mesmo seja necessário para a execução de um contrato no qual o titular dos dados seja parte, ou para diligências pré-contratuais a pedido do titular. Ora, na ausência de fonte de licitude expressa, ficaria o segurador impedido de tratar dados de saúde após 25/05/2018, devendo mesmo destruir os que estivessem na sua posse, com a consequente extinção dos contratos de seguro afetados.

[108] Sabine AbravanelJolly, "Le secret médical en assurance de personnes", *cit.*, p. 889. Sobre o tema e, em particular, a (i)licitude da prova produzida, cfr., desenvolvidamente, Luís Poças, *O Dever de Declaração Inicial do Risco no Contrato de Seguro*, *cit.*, pp. 859 ss.

Verificámos igualmente a ineptidão do consentimento como fonte de licitude para o tratamento de dados de saúde no contexto em análise. Com efeito, a inviabilidade de observância dos requisitos da *especificidade* do consentimento (como vem sendo entendida pela CNPD) e, sobretudo, da *liberdade* do mesmo, tornam-no inválido, com as inerentes consequências contraordenacionais. Por outro lado, os direitos à retirada do consentimento e ao apagamento dos dados fazem desta fonte de licitude um fundamento precário e efémero de tratamento, incompatível com a estabilidade e duração tendencialmente longa do seguro.

Analisando mais detidamente as fontes de licitude previstas para o tratamento de dados de saúde, constatámos que a alínea b) do n.º 2 do artigo 9.º do RGPD legitima o tratamento de dados quando necessário para o cumprimento de obrigações legais do responsável pelo tratamento em matéria de legislação laboral e de proteção social, dando cobertura a tal tratamento no caso dos seguros obrigatórios de acidentes de trabalho (enquadrados por legislação laboral) e dos seguros obrigatórios de responsabilidade civil e de acidentes pessoais (disciplinados por legislação de proteção social). Igualmente legitimado fica o tratamento de dados de saúde no âmbito dos seguros de *employee benefits* (vida, saúde e acidentes pessoais), quando obrigatórios no âmbito da legislação laboral e do IRCT aplicável.

Por seu turno, também os seguros de vida, saúde e acidentes pessoais de iniciativa individual, ou constituindo *employee benefits* não previstos em IRCT (portanto, de constituição facultativa) assumem natureza de complementaridade face ao Sistema Previdencial de Segurança Social e ao Sistema Nacional

de Saúde e, logo, caráter de proteção social. Por seu turno, do enquadramento legal dos mesmos decorrem deveres a cargo do responsável pelo tratamento (o segurador), pelo que a licitude do tratamento encontra igualmente base na alínea b) do n.º 2 do artigo 9.º do RGPD.

Ainda que assim não fosse, também a alínea h) do n.º 2 do artigo 9.º seria apta a fundar a licitude do tratamento de dados de saúde relativamente a seguros facultativos de vida, de saúde ou de acidentes pessoais, porquanto os mesmos consubstanciam a *gestão de serviços de ação social* (e os seguros de saúde visam a prestação de cuidados de medicina preventiva, o diagnóstico médico e a prestação de cuidados ou tratamentos e serviços de saúde), sendo o tratamento enquadrado no Direito nacional e efetuado sob a responsabilidade de entidades e pessoas sujeitas a obrigação de sigilo profissional.

Desta forma, o RGPD contém soluções normativas para o problema objeto do presente texto. Se esta perspetiva não for, porém, acolhida, designadamente, pela CNPD, a solução não dispensará uma intervenção do poder legislativo[109]. Esta poderia consistir no reconhecimento legal expresso de que os seguros facultativos de pessoas assumem *interesse público importante*, por conjugação com a alínea g) do n.º 2 do artigo 9.º do RGPD. Em alternativa, a intervenção poderia traduzir-se, ao abrigo do n.º 4 do artigo 9.º do RGPD, no estabelecimento de novas condições legais de tratamento de dados relativos à saúde.

[109] É esta a posição veiculada pela CNPD, que aponta «a necessidade de definição de um regime legal específico sobre esse tratamento [de dados de saúde no âmbito dos contratos de seguros], advertindo desde já que não é suficiente a mera previsão legal do tratamento» – Parecer n.º 20/2018, da CNPD, de 02/05/2018, *cit*., p. 41 v.

A alternativa às vias de solução acima desenhadas revela-se peculiar. Com efeito, caso não fosse reconhecida a licitude no quadro do RGPD nem proporcionada solução legislativa, o segurador ficaria impedido de tratar dados de saúde na execução de seguros de pessoas facultativos, o que inviabilizaria o cumprimento da sua prestação em caso de sinistro. Esta circunstância levaria o credor dessa prestação a demandar judicialmente o segurador, ficando então o tratamento de dados legitimado ao abrigo da alínea f) do n.º 2 do artigo 9.º. Este caminho depara-se, porém, frequentemente, com a oposição dos tribunais, que, abstraindo dos constrangimentos da proteção de dados para o segurador, lhe exigem, não obstante, um impossível cumprimento do ónus da prova.

Em maré de incerteza quanto à solução que o destino reserva ao problema objeto do presente texto, aguarda-se – da autoridade nacional de controlo (enquanto intérprete qualificada e fiscalizadora do cumprimento do RGPD), do legislador (que tem na Proposta de Lei n.º 120/XIII uma oportunidade de ouro para regular de forma clara e definitiva a questão) e, em última instância, dos tribunais (quanto ao sentido de equilíbrio e justiça que deve norteá-los) – uma solução coerente e responsável para um problema cujas consequências potenciais são de uma invulgar gravidade e que, no essencial, não é dos seguradores, mas de toda a sociedade civil.

A PROTEÇÃO DOS DADOS PESSOAIS E O DIREITO À SEGURANÇA INFORMÁTICA NO COMÉRCIO ELETRÓNICO

Alexandre L. Dias Pereira[*]

Resumo — Este trabalho versa sobre a proteção dos dados pessoais e a segurança informática no comércio eletrónico. Identifica e analisa os direitos dos consumidores à proteção dos dados pessoais e à segurança informática ("cibersegurança") face ao Regulamento Geral de Proteção de Dados (RGPD) e à Diretiva da Segurança das Redes e da Informação (DRSI) aplicável aos operadores de serviços essenciais e aos prestadores de serviços digitais.

Palavras-chave: comércio eletrónico — dados pessoais — segurança informática —mercado digital — consumidor

Introdução

A proteção dos dados pessoais no comércio eletrónico é um tema de grande atualidade e interesse face ao Regulamento Geral de Proteção de Dados (RGPD)[1], plenamente aplicável

[*] Professor Auxiliar e Membro do Instituto Jurídico da Faculdade de Direito da Universidade de Coimbra, Portugal.

[1] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Sobre a proteção de dados pessoais na bibliografia portu-

a partir de 25 de maio de 2018. No setor segurador têm especial importância os dados relativos à saúde, que o RGPD define como os "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" (artigo 4/15). É uma noção muito ampla, especialmente se tivermos em conta que o considerando (35) acrescenta: "no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, a essa pessoa singular, como qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde, as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e

guesa ver, designadamente, Garcia Marques & Lourenço Martins, *Direito da Informática*, 2.ª ed., Almedina, Coimbra, 2006, p. 129-313, 422-442, 330-391; Paulo Mota Pinto, «O direito à reserva sobre a intimidade da vida privada», *Boletim da Faculdade de Direito de Coimbra* 64 (1993) p. 479-586; Helena Moniz, «Notas sobre a protecção de dados pessoais perante a informática: o caso especial dos dados pessoais relativos à saúde», *Revista Portuguesa de Ciência Criminal*, 7/2 (1997), p. 231-298; Eduarda Gonçalves, *Direito da Informação — Novos Direitos e Formas de Regulação na Sociedade da Informação*, 2.ª ed., Almedina, Coimbra, 2003, p. 82-111, 173-183; Catarina Castro, *Direito da informática, privacidade e dados pessoais*, Almedina, Coimbra, 2005; A. Sousa Pinheiro, *Privacy e protecção de dados pessoais*, AAFDL, Lisboa, 2015. Em castelhano vide, por ex., J.P. Aparício Vaquero e A. Batuecas Caletrío (coord,), *En torno a la privacidad y la protección de datos en la sociedad de la información*, Granada. Comares, 2015; López Calvo, J., *Comentarios al Reglamento Europeo de Protección de Datos*, Madrid, Sepin, 2017.

quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro."

"Principiologia" da proteção de dados pessoais

A proteção de dados pessoais, em especial de saúde, é uma componente fundamental do comércio eletrónico. As empresas, incluindo as seguradoras, têm que adaptar a sua política de privacidade e de dados pessoais às novas exigências do RGPD[2], que é já a 3.ª geração de leis de dados pessoais na União Europeia.

O RGPD prevê diversos princípios relativos ao tratamento de dados pessoais, designadamente a licitude, a lealdade e transparência, a limitação das finalidades, a minimização dos dados, a exatidão, a limitação da conservação, a integridade e confidencialidade, e a responsabilidade pelo tratamento.

Estabelece a proibição geral de tratamento de dados pessoais relativos à saúde (artigo 9/1), exceto se for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, diagnóstico médi-

[2] Para uma análise do impacto do RGPD nos sites dos operadores de comércio eletrónico, *vide* M. Weigl, «The EU General Data Protection Regulation's Impact on Website Operators and eCommerce», *Computerrecht-international* 4 (2016), p. 102-108.

co, prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva de determinadas condições e garantias. O tratamento de dados de saúde é ainda permitido e for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional.

O preâmbulo do RGPD contém extensos considerandos sobre estas derrogações à proibição geral de tratamento de dados. Assim, o considerando (52) indica que são justificadas derrogações nomeadamente "para fins de segurança, monitorização e alerta em matéria de saúde, prevenção ou controlo de doenças transmissíveis e outras ameaças graves para a saúde." Mais acrescenta que "Essas derrogações poderão ser previstas por *motivos sanitários*, incluindo de saúde pública e de gestão de serviços de saúde, designadamente para assegurar a qualidade e a eficiência em termos de custos dos procedimentos utilizados para regularizar os pedidos de prestações sociais e de serviços no quadro do regime de seguro de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos."

Para além de dados de saúde o tratamento de outras categorias especiais de dados poderá ter justificação "para fins

relacionados com a saúde quando tal for necessário para atingir os objetivos no interesse das pessoas singulares e da sociedade no seu todo, nomeadamente no contexto da gestão dos serviços e sistemas de saúde ou de ação social, incluindo o tratamento por parte da administração e das autoridades sanitárias centrais nacionais desses dados para efeitos de controlo da qualidade, informação de gestão e supervisão geral a nível nacional e local do sistema de saúde ou de ação social, assegurando a continuidade dos cuidados de saúde ou de ação social e da prestação de cuidados de saúde transfronteiras, ou para fins de segurança, monitorização e alerta em matéria de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos baseados no direito da União ou dos Estados-Membros e que têm de cumprir um objetivo, assim como para os estudos realizados no interesse público no domínio da saúde pública" (considerando 53). Mais acrescenta este considerando que: "Os Estados-Membros deverão ser autorizados a manter ou introduzir outras condições, incluindo limitações, no que diz respeito ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde. Tal não deverá, no entanto, impedir a livre circulação de dados pessoais na União, quando essas condições se aplicam ao tratamento transfronteiriço desses dados."

A saúde pública justifica o tratamento de dados sensíveis sem o consentimento do respetivo titular indicando o considerando (54) que são aí abrangidos "todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despe-

sas e o financiamento dos cuidados de saúde, e as causas de mortalidade." Todavia ressalva este considerando, *in fine*: "Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, *como os empregadores ou as companhias de seguros e entidades bancárias*" (*itálico nosso*).[3]

[3] A exceção para fins de investigação científica justifica tratamentos derivados ou secundários (consentimento amplo), tratamentos de categorias sensíveis de dados pessoais sem consentimento do respetivo titular, bem como derrogações ao direito de apagamento e do direito de oposição ao tratamento, mediante salvaguardas adequadas. Os fins da investigação científica abrangem pro ex. o desenvolvimento tecnológico, a investigação aplicada e a investigação financiada pelo setor privado, a realização de um espaço europeu de investigação, ou estudos de interesse público realizados no domínio da saúde pública (considerando 159 do RGPD).

A exceção ao princípio da limitação do tratamento atende à natureza dinâmica da investigação e pretende justificar a aplicação de inteligência artificial (IA) às minas de dados pessoais. Os tratamentos posteriores para fins de investigação científica são considerados compatíveis com o consentimento inicial (art. 5/1-b), lendo-se no considerando 33 que "os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de investigação científica, desde que estejam de acordo com padrões éticos reconhecidos para a investigação científica."

Por outro lado, os fins de investigação científica justificam a possibilidade de tratamento de categorias especiais de dados pessoais, com os dados de saúde (art. 9/2-j). Parte-se do princípio de que, nos termos do considerando 157: "Combinando informações provenientes dos registos, os investigadores podem obter novos conhecimentos de grande valor relativamente a problemas médicos generalizados, como as doenças cardiovasculares, o cancro e a depressão." Ressalva-se, todavia, que os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde, ou seja, os Estados-Membro podem adotar regras mais restritivas a nível nacional relativamente a estas categorias de dados. Por ex., em Portugal a Lei 12/2005, de 26 de janeiro,

prevê limites à utilização de informação genética em sede de investigação sobre o genoma humano (Artigo 16/4: "A investigação sobre o genoma humano em pessoas não pode ser realizada sem o *consentimento informado* dessas pessoas*, expresso por escrito,* após a explicação dos seus direitos, da natureza e finalidades da investigação, dos procedimentos utilizados e dos riscos potenciais envolvidos para si próprios e para terceiros."), e estabelece inter alia o princípio da *proibição da discriminação* em função do património genético (art. 11) e uma *proibição geral* de testes genéticos ou informação genética para a celebração de contratos de seguro de vida ou acidente, trabalho, ou na adoção (arts. 12 a 14). Ainda ao nível da legislação interna, o referido Código Deontológico da Ordem dos Médicos permite o acesso a informação de saúde para fins de investigação, mas desde que *anonimizada*. Note-se, a este respeito, que os *dados anónimos* não são regulados pelo RGPD nos termos do considerando 26: "Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação."

A Lei n.º 26/2016, de 22 de agosto, sobre o acesso aos documentos da administração e à sua reutilização, estabelece que "O acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento ou nos termos da lei, é exercido por intermédio de médico se o titular da informação o solicitar, com respeito pelo disposto na Lei n.º 12/2005" (artigo 7/1). Além disso, esta lei possibilita o acesso a dados de saúde a terceiros sem consentimento do titular dos dados embora por intermédio do médico e limitado à "informação estritamente necessária à realização do interesse direto, pessoal, legítimo e constitucionalmente protegido que fundamenta o acesso" (artigo 7/4). A este propósito, o RGPD ressalva que os organismos públicos podem tratar dados pessoais sem o consentimento dos titulares para execução de tarefa no *interesse público* (art. 6-e). De todo o modo, os dados licitamente tratados para fins de investigação científica não podem ser livremente tratados por terceiros, nomeadamente por seguradoras, conforme se lê no considerando 54 do RGOD: "O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública, sem o consentimento do titular dos dados. (...) Tais atividades de tratamento de dados

Direitos do titular e deveres do responsável pelo tratamento dos dados pessoais

Ao titular de dados é reconhecido um leque de direitos, incluindo o direito de informação na recolha de dados (artigos 13 e 14), o direito de acesso (artigo 15)[4], o direito de retificação (artigo 16), o direito ao apagamento dos dados (artigo 17 — «direito a ser esquecido»)[5], o direito à limitação do tratamento (artigo 18), o direito de portabilidade dos dados (artigo 20), e o direito de oposição a definição de perfis e decisões automatizadas (artigo 21).

Por seu turno, o responsável pelo tratamento e o seu subcontratante têm vários deveres a seu cargo, designadamente o dever de segurança de tratamento, o dever de notificação de uma violação de dados pessoais à autoridade de controlo e de comunicação da violação ao titular dos dados (artigos 32 e 33). Em certas condições, o responsável pelo tratamento poderá ser obrigado a ter um Encarregado de Proteção de Dados (EPD/DPO, instituído pelo Regulamento (artigo 37 e seguintes), para além da previsão de códigos de conduta e de artigo 40 e seguintes) com o Selo Europeu de Proteção de Dados, e organismos de certificação (artigo 40 e seguintes). As transferências

sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias."

A exceção de investigação científica está sujeita a certas condições (art. 89). Por um lado, são exigidas medidas técnicas e organizativas adequadas para cumprir o princípio da minimização do tratamento. Remete-se, a este propósito, para os *padrões éticos* da investigação científica, sem prejuízo de se estabelecer que a a *pseudonimização* e *a cifragem* dos dados pessoais são medidas adequadas (art. 32/1-a; a pseudonimização surge definida no art. 4/3-b). Todavia, a pseudonimização só é obrigatória "desde que os fins visados possam ser atingidos desse modo" (art. 89/2). Quando ao dever de informação, decorrente do princípio da transparência dos dados, a investigação científica afasta-o se os dados forem obtidos por terceiros ou a partir de fontes públicas acessíveis ou se o cumprimento desse dever impossibilitar ou dificultar seriamente a prossecução dos objetivos visados, na medida em que sejam adotadas medidas adequadas.

Para terminar, referir ainda que os fins de investigação científica justificam outras exceções aos direitos dos titulares de dados pessoais, como o direito ao apagamento, em caso de necessidade superveniente (art. 17/3-), ou o direito de oposição, havendo interesse público na investigação em causa (art. 21/6). Além disso, a lei interna dos Estados-Membros pode estabelecer exceções adicionais aos direitos de acesso, retificação, limitação ou oposição, ressalvando-se, todavia, que o tratamento de dados para fins científicos deverá igualmente respeitar outra legislação aplicável, tal como a relativa aos ensaios clínicos. (art. 89). Em Portugal, o projeto de lei de "regulamentação" do RGPD prevê que os fins de investigação científica prevalecem sobre os direitos de acesso, retificação, limitação do tratamento e de oposição (art. 31/2). Por seu turno, a investigação clínica é regulada pela Lei n.º 21/2014, de 16 de abril.

[4] O direito de acesso significa, em matéria de dados de saúde, que os seus titulares têm direito de lhes aceder, como refere o considerando (63), "por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados."

[5] Este "direito a ser esquecido" foi afirmado pelo Tribunal de Justiça da União Europeia no acórdão de 13 de maio de 2014, proc. C131/12, *Google Spain SL e Google Inc c. Associação Espanhola de Dados Pessoais (AEPD)* c. *Mário Costeja Gonzalez* (pedido de decisão prejudicial apresentado pela Audiencia Nacional). ECLI:EU:C:2014:317. Sobre este acórdão ver por ex. Indra Spiecker, «A new framework for information markets: Google Spain», *Common Market Law Review,* 52 (2015), p. 1033-1058; Sofia Casimiro, «O direito a ser esquecido pelos motores de busca: o Acórdão Costeja», *Revista de Direito Intelectual*, 2014/2, p. 307-353; Filipa Calvão, «A protecção de dados pessoais na internet: desenvolvimentos recentes», *Revista de Direito Intelectual,* 2015/2, p. 67-84 (preferindo falar em "direito à desassociação").

de dados pessoais para países terceiros ou organizações internacionais são feitas com base numa decisão de adequação, e são sujeitas a garantias adequadas.[6]

Prevê-se ainda um esquema de trabalho em rede e de cooperação entre a autoridade de controlo principal e as autoridades de controlo interessadas. Para efeitos da aplicação efetiva do RGPD é instituído um Comité europeu para a proteção de dados e uma Autoridade Europeia para a Proteção de Dados.[7]

A obrigação de segurança e confidencialidade dos dados pessoais

O responsável pelo tratamento de dados tem uma obrigação de segurança e confidencialidade do tratamento, "incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas", conforme se lê no considerando (39).[8] A

[6] O protocolo *Safe Harbor* de transferência de dados da União Europeia para os EUA foi declarado inválido pelo TJUE no acórdão de 6 de outubro de 2015, proc. C-362/14, *Maximillian Schrems v Data Protection Commissioner*. Posteriormente, em fevereiro de 2016, a União Europeia e os EUA chegaram a um acordo sobre a transferência de dados pessoais, denominado "*Privacy Shield*" (Escudo de Privacidade), tendo sido adotada posteriormente a Decisão de Execução (UE) 2016/1250 da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho.

[7] <https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_pt>

[8] Já a Lei 67/98, de 26 de outubro (que transpôs a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção

segurança da rede e da informação, em sede de tratamento de dados pessoais, consiste nos termos do considerando (49) do RGPD na "capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas, pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrónicas e por fornecedores de tecnologias e serviços de segurança". Entende-se que a segurança informática, assim caraterizada, constitui um interesse legítimo do responsável pelo tratamento, justificando, por exemplo, "impedir o acesso não autorizado a redes de comunicações eletrónicas

das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados) obrigava o responsável pelo tratamento de dados a adotar medidas especiais de segurança adequada ao controlo da entrada nas instalações, dos suportes de dados, inserção, da utilização, de acesso, da transmissão, da introdução (o quê, quando e por quem), do transporte, a separação lógica dos dados de saúde e da vida sexual, incluindo os genéticos, dos restantes dados pessoais. Por seu turno, a Lei 12/2005, de 26 de janeiro, sobre informação pessoal genética e de saúde estabelece deveres do responsável pelo tratamento da informação de saúde, como sejam a confidencialidade e segurança das instalações e dos equipamentos, o controlo do acesso à informação, sigilo e educação deontológica dos profissionais, a proibição de acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde, níveis de segurança contra destruição, acidental ou ilícita, alteração, difusão ou acesso não autorizado ou qualquer outra forma de tratamento ilícito da informação, a realização regular e frequente de cópias de segurança (back-up regulares).

e a distribuição de códigos maliciosos e pôr termo a ataques de «negação de serviço» e a danos causados aos sistemas de comunicações informáticas e eletrónicas" (*ibidem*).

A violação de dados pessoais é definida como "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (artigo 4/12).

Um dos princípios que regem o tratamento é o da integridade e confidencialidade. Significa que o tratamento dos dados deve garantir "a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»)" (artigo 5/1-f).[9]

Por outro lado, a segurança dos dados pessoais é regulada no artigo 32 do RGPD: o responsável pelo tratamento e o subcontratante devem ter em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, e aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

[9] A confidencialidade dos dados de saúde é uma das condições da telemedicina, nos termos do Código Deontológico da Ordem dos Médicos, aprovado pelo Regulamento n.º 707/2016, de 21 de julho. Sobre o tema, Alexandre L. Dias Pereira, «Telemedicina e farmácia online: aspetos jurídicos da eHealth», *Revista da Ordem dos Advogados* 75 I/II (2015), p. 55-78.

1 — A pseudonimização e a cifragem dos dados pessoais[10];

2 — A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, e de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;

3 — Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. A segurança informática é também um requisito da subcontratação do tratamento, podendo ser demonstrada através do cumprimento de um código de conduta aprovado ou um procedimento de certificação aprovado — artigo 32/ 3 e considerando (81).

Por outro lado, o responsável pelo tratamento tem o *dever de notificar* uma violação de dados pessoais à autoridade de controlo, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares, devendo nesse caso ser acompanhada dos motivos do atraso (artigo 33/1). Quanto ao seu *conteúdo* a notificação deve descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados

[10] A cifragem é apontada como uma medida de controlo dos riscos de segurança no tratamento de dados pessoais, "tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais" (considerando 83 do RGPD).

afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa. Além disso, a notificação deve comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações, e descrever as consequências prováveis da violação de dados pessoais e as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos (artigo 33/3).

Para além da notificação à autoridade competente, com os referidos elementos, o responsável pelo tratamento deve comunicar ao titular dos dados, sem demora injustificada, a violação de dados pessoais quando essa violação puder implicar um *elevado risco* para os direitos e liberdades das pessoas singulares, salvo se o responsável: a) tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem, ou b) tiver tomado medidas subsequentes que assegurem que o referido elevado risco para os direitos e liberdades dos titulares dos dados já não é suscetível de se concretizar; ou c) implicar um esforço desproporcionado. Não comunicando justificadamente a violação ao titular dos dados, deverá ser feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz (artigo 34/3).

Obrigação de avaliação de impacto

A obrigação de *avaliação de impacto* sobre a proteção de dados das operações de tratamento significa que o responsável pelo tratamento deve solicitar o parecer do *encarregado da proteção de dados*, nos casos em que este tenha sido designado, e a avaliação incluirá, pelo menos, *inter alia*, as medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o RGPD, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa (artigo 35).

Direito do consumidor à segurança informática?

A Constituição da República (CRP) consagra o direito fundamental à liberdade e à segurança (artigo 27/1), e atribui aos trabalhadores e aos consumidores o direito à segurança (artigos 59/1-c e 60/1). O regime da utilização da informática previsto no artigo 35 da CRP não contempla a segurança informática *qua tale*. Trata dos dados pessoais, máxime informatizados, remetendo a sua proteção para diploma legal, e estabelece a garantia de acesso universal e livre às redes informáticas de uso público.[11] Por seu turno, a Lei de Defesa do Consumidor

[11] Embora sem consagração na letra da lei constitucional, a jurisprudência tem encontrado no espírito do artigo 35 um "direito à autodeterminação informativa" – cf. por ex. o acórdão do Supremo Tribunal de Justiça de 16 de outubro de 2014, proc. 679/05.7TAEVR.E2.S1, Cons. Helena Moniz, <www.dgsi.pt>. O Tribunal Federal Constitucional Alemão (BFGH) utilizou a expressão no âmbito

de um processo relativo a informações pessoais coletadas durante o censo de 1983. O BFGH considerou que, no contexto do processamento moderno de dados, a proteção do indivíduo contra a recolha, armazenamento, uso e divulgação ilimitados de seus dados pessoais é abrangida pelos direitos gerais das pessoas garantidos na constituição alemã. Este direito fundamental garante, a este respeito, a capacidade do indivíduo para determinar, em princípio, a divulgação e o uso de seus dados pessoais. As limitações a esta autodeterminação informacional só são permitidas em caso de interesse público primordial (BVerGE, Acórdão de 15 de dezembro de 1983: «Recht auf informationelle Selbstbestimmung**»,** *Cinqüenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*, org. Leonardo Martins, Montevideo, 2005). A figura foi recebida pela doutrina portuguesa: o "direito à autodeterminação informativa previsto no art. 35.º, da CRP, (...) protege uma amplitude de direitos fundamentais para lá do direito à privacidade (...) dá 'a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em «simples objeto de informação»'" — J. J. Gomes Canotilho, Vital Moreira, *Constituição da República Portuguesa Anotada*, vol. 1, 4.ª ed., Coimbra Editora, 2007, p. 55; cf. o referido acórdão do STJ de 16 de outubro de 2014). Segundo J. Sousa Ribeiro («A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas», in *Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho,* vol. III, Coimbra Editora, p. 85), este direito «impede que o 'eu' seja objeto de apropriação pelos outros, como matéria de comunicação na esfera pública. Nela conjuga -se o *direito ao segredo* (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes) e um *direito à reserva* (proibição de revelação)».

«Por autodeterminação informativa poderá entender-se o direito de subtrair ao conhecimento público factos e comportamentos reveladores do modo de ser do sujeito na condução da sua vida privada», considerou o Tribunal Constitucional no seu acórdão nº 442/2007, de 14 agosto de 2007. Em um outro acórdão, em processo relativo à conservação de dados no SIRP, julgou que o direito à reserva sobre a intimidade da vida privada faz parte do núcleo do direito ao livre desenvolvimento da personalidade previsto no art. 26 da CRP e inclui, como diferentes manifestações, o *direito à solidão*, o *direito ao anonimato* e o *direito à autodeterminação informativa* (Acórdão do TC n.º 403/2015, proc. 773/15).

A figura seria consagrada pela jurisprudência em vários outros acórdãos. Alguns tratam da existência de «justa causa» de levantamento de sigilo bancário em processo de divórcio para apurar o património do casal, pronunciando-se os tribunais pela prevalência do interesse público da administração de justiça sobre o segredo bancário protegido nos termos dos artigos 78 e 79 do Regime Geral de Instituições de Crédito (RGIC): vide acórdão do TC nº 278/95, de 31 de maio de 1995; acórdão do TC nº 442/2007, de 14 agosto de 2007 (o sigilo bancário não integra a esfera íntima da vida privada); acórdão do STJ de Uniformização de Jurisprudência nº 2/08, de 13 de fevereiro de 2008; acórdão do Tribunal da Relação de Coimbra, de 6 de abril de 2010, proc. 120-C/2000.C1; acórdão do Tribunal da Relação de Évora, de 14/9/2017, proc. 2829/16.9T8PTM-B.E1). Outros acórdãos tratam do ressarcimento de danos morais traduzidos em humilhação, vergonha, embaraço causados pela utilização de dados pessoais sobre nomeações político-partidários. Considerando que subjacente à proteção de dados está o "direito à autodeterminação informativa" e a proteção da privacidade, o STJ considerou que o facto de os referidos dados serem públicos não autorizaria o seu tratamento em termos de afixação de um mapa de pessoal com os nomes e os respetivos vencimentos, filiação partidária e contratação por concurso ou por nomeação (acórdão do STJ de 16 de outubro de 2014). O «direito à autodeterminação informativa» é também referido na jurisprudência a propósito de um sistema de registo informatizado das idas ao WC numa empresa, tendo sido julgado que tal não constituiria devassa por meio informático para efeitos do artigo 193 do Código Penal, em razão de ser um sistema aceite pela CNPD destinado a controlar a produtividade dos trabalhadores e não a sua vida privada, já que o sistema não registaria a atividade no interior do WC mas apenas o número de vezes de utilização e o tempo aí passado pelo trabalhador (Acórdão do Tribunal da Relação do Porto, de 31 de maio de 2006, proc. 0111584).

Finalmente, encontram-se ainda acórdãos sobre o tema no domínio sensível dos dados pessoais de saúde. O sigilo médico é objeto de proteção legal (Lei 12/2015, CDOM, LADAR), todavia o Código de Processo Penal prevê a possibilidade de dispensa de sigilo, estabelecendo no artigo 135º/2 que "Havendo dúvidas fundadas sobre a legitimidade da escusa, a autoridade judiciária perante a qual o incidente se tiver suscitado procede às averiguações necessárias. Se, após estas, concluir pela ilegitimidade da escusa, ordena, ou requer ao tribunal que ordene, a prestação do depoimento". Com base nisto, o Tribunal da Relação

(LDC)[12] protege a segurança do consumidor (artigos 3/b e 5). O artigo 8/3 estabelece que "Os riscos para a saúde e segurança dos consumidores que possam resultar da normal utilização de bens ou serviços perigosos devem ser comunicados, de modo claro, completo e adequado, pelo fornecedor ou prestador de serviços ao potencial consumidor." Além disso, o artigo 21/2 da LDC atribui à Direção-Geral do Consumidor poderes para "d) Ordenar medidas cautelares de cessação, suspensão ou interdição de fornecimentos de bens ou prestações de serviços que, independentemente de prova de uma perda ou um prejuízo real, pelo seu objeto, forma ou fim, acarretem ou possam acarretar riscos para a saúde, a segurança e os interesses económicos dos consumidores."

A segurança informática não é aqui expressamente prevista, mas deve considerar-se uma dimensão do direito do consumidor à segurança.[13] Por isso, no comércio eletrónico, a segurança informática do consumidor (diferente da segurança pública) poderá justificar a adoção de medidas restritivas,

do Porto considerou que o sigilo profissional médico pode ser dispensado em processo de burla tributária (acórdão de 13 de março de 2013, proc. 605/10.1T3AVR-A.P1, Des. Álvaro Melo). Todavia, o mesmo tribunal, citando o acórdão do TC nº 155/2007, decidiu que pode ser feita recolha de saliva através de zaragatoa bucal para obter prova, mas essa diligência tem que ser ordenada por juiz e não pelo MP (acórdão de 10 de julho de 2013, proc. 1728/12.8JAPRT.P1, Des. Joaquim Gomes).

[12] Lei 24/96, de 31 de julho, com alterações posteriores.

[13] Seguimos de perto a comunicação sobre o direito do consumidor à segurança informática (*cibersecurity*) que apresentámos no I Congresso Internacional de Direito do Consumidor: Os Desafios do Mercado Digital para os Contratos de Consumo, organizado pelo Instituto Jurídico da Universidade Portucalense Infante D. Henrique Porto nos dias 19 e 20 de janeiro de 2018.

incluindo providências concretas contra um prestador de serviços, à circulação de um determinado serviço da sociedade da informação proveniente de outro Estado membro da União Europeia na medida em que possa lesar ou ameaçar gravemente os consumidores, nos termos do artigo 7/1 do DL 7/2004, de 7 de janeiro.[14]

O regime da segurança das redes e da informação

Os deveres de segurança informática a cargo de operadores de serviços essenciais e de prestadores de serviços digitais protegem igualmente os consumidores. A Diretiva 2016/1148[15]

[14] Transpõe para o direito interno a Diretiva n.º 2000/31/CE, do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno.

[15] Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Entretanto transposta Lei n.º 46/2018, de 13 de agosto (regime jurídico da segurança do ciberespaço).

Podemos também afirmar a segurança informática como um bem jurídico penal. O Código Penal prevê tipos legais de crime relacionados com a segurança informática, como a devassa da vida privada, em especial por meio de informática (artigos 192 e 193), e a burla informática e nas comunicações (artigo 221). Além disso, a Lei do Cibercrime (aprovada pela Lei 109/2009, de 15 de setembro, que transpõe para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa) erige a segurança informática à dignidade de bem jurídico-penal, prevendo os seguintes tipos legais de crime (cibercrimes): a falsidade informática, o dano relativo a programa ou outros dados informáticos, a sabotagem infor-

estabelece obrigações de segurança face ao "papel vital" das redes e da informação na sociedade e na economia e ao potencial lesivo dos incidentes de segurança. Cria uma Rede de equipas de resposta a incidentes de segurança informática («rede de CSIRT») e um Grupo de Cooperação, incluindo os Estados-Membros, a agência europeia ENISA e a Comissão Europeia. Nos incidentes de segurança estão em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, e dos serviços utilizados.

Os deveres de segurança recaem sobre os operadores de serviços essenciais, categoria que abrange as empresas de energia, transportes, banca e bolsas, hospitais e clínicas privadas, fornecedores de água potável, e infraestruturas digitais (anexo II). Os deveres de segurança valem igualmente para os prestadores de serviços digitais, incluindo mercados em linha, motores de pesquisa em linha, e serviços de computação em nuvem (anexo III). De fora ficam as empresas que oferecem redes de comunicações públicas ou serviços de comunicações eletrónicas acessíveis ao público, na aceção da Diretiva 2002/21/CE, e os prestadores de serviços de confiança na aceção do Regulamento 910/2014[16], uma vez que tanto estes como aquelas

mática, o acesso ilegítimo, e a interceção ilegítima. É a ainda previsto o crime de reprodução ilegítima de programa protegido, o qual, todavia, transcende a lógica estrita da cibersegurança.

[16] Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (eIDAS) (e no direito interno o Decreto-Lei n.º 290-D/99, de 2 de agosto, com alterações posteriores).

ficam sujeitos aos requisitos de segurança estabelecidos nos respetivos diplomas.[17]

O preâmbulo da Dir. 2016/1148 esclarece no considerando 22 que a prestação de serviços essenciais pode não corresponder a toda a atividade da empresa, ficando esta sujeita aos deveres de segurança apenas no que respeita aos serviços essenciais:

"Por exemplo, no setor do transporte aéreo, os aeroportos prestam serviços que podem ser considerados essenciais por um Estado-Membro, tais como a gestão das pistas, mas também uma série de serviços que podem ser considerados não essenciais, como a disponibilização de áreas comerciais. / Os operadores de serviços essenciais deverão estar sujeitos aos requisitos de segurança específicos apenas no que respeita aos serviços considerados essenciais."

[17] Por exemplo, o Regulamento eIDAS estabelece como requisitos de segurança aplicáveis aos prestadores de serviços de confiança (1) a adoção de medidas para impedir ou reduzir ao mínimo o impacto dos incidentes de segurança e informar as partes interessadas dos efeitos adversos dos eventuais incidentes, e (2) o dever de notificação da autoridade nacional de segurança e da autoridade de proteção de dados de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo sobre o serviço de confiança prestado ou sobre os dados pessoais por ele conservados. Em caso de violação de segurança dos sistemas de ID, que prejudique a fiabilidade da autenticação transfronteiriça do sistema, o Estado-Membro notifica os outros Estados-Membros e a Comissão. Ao fim de 3 meses sem ter sido corrigida a falha o meio de ID é suprimido.

As medidas de controlo de segurança e gestão dos riscos de segurança na moeda eletrónica, em especial a notificação de incidentes, estão previstas na Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno (altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) 1093/2010, e revoga a Diretiva 2007/64/CE).

Os Estados-Membros devem identificar os *operadores de serviços essenciais* nos setores da *energia* (eletricidade, petróleo, gás, incluindo empresas de comercialização, de distribuição, de transporte, operadores de rede, operadores de instalações de refinamento, tratamento ou armazenamento), *dos transportes* (aéreo, ferroviário, marítimo e fluvial, rodoviário — por ex., entidades gestoras aeroportuárias, aeroportos, operadores de controlo da gestão do tráfego aéreo, gestores de infraestruturas e empresas rodoviárias, empresas de transporte e entidades gestores dos portos, operadores de serviços de tráfego marítimo, autoridades rodoviárias e operadores de sistemas de transporte inteligentes), no *setor bancário* (instituições de crédito e infraestruturas do mercado financeiro, incluindo operadores de plataformas de negociação (bolsas) e contrapartes centrais), no *setor da saúde* (incluindo instalações de prestação de saúde, nomeadamente hospitais e clínicas privadas), no *setor do fornecimento e distribuição de água potável para consumo humano*, e *no setor das infraestruturas digitais* (incluindo pontos de troca de tráfego, prestadores de serviços e registos de DNS).

Nos termos do artigo 6 da Dir. 2016/1148, a identificação dos operadores de serviços essenciais faz-se segundo determinados critérios, tais como, por exemplo, saber se a entidade presta um serviço essencial para a manutenção de atividades societais e/ou económicas cruciais, se a prestação desse serviço depende de redes e sistemas de informação, e se um incidente pode ter efeitos perturbadores importantes na prestação desse serviço, tendo em conta: a) O número de utilizadores que dependem dos serviços prestados pela entidade em causa; b) A dependência de outros setores essenciais em relação ao serviço prestado por essa entidade; c) O possível impacto dos incidentes, em termos de intensidade e duração, sobre as atividades económicas e societais ou a segurança pública; d) A quota de mercado dessa entidade; e) A distribuição geográfica, no que se refere à zona que pode ser afetada por um incidente; f) A importância da entidade para a manutenção de um nível suficiente do serviço, tendo em conta a disponibilidade de meios alternativos para a prestação desse serviço.

São ainda previstos fatores específicos por setor tais como a quantidade ou a percentagem de energia nacional gerada, para os fornecedores de energia, o volume diário, para os fornecedores de petróleo, e a sua importância sistémica com base nos ativos totais ou no rácio ativos totais/PIB, para os serviços bancários ou as infraestruturas do mercado financeiro.

Os operadores de serviços essenciais devem adotar *medidas técnicas e organizativas* adequadas e proporcionadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações e para reduzir ao mínimo o seu impacto, a fim de assegurar a continuidade desses serviços.[18]

As políticas de segurança dos operadores de serviços essenciais estão sujeitas a avaliação devendo para o efeito apresentar a respetiva documentação e provas da sua aplicação efetiva, tais como os resultados de uma *auditoria de segurança* efetuada pela autoridade competente ou por um auditor qualificado e que, no último caso, facultem os resultados dessa auditoria, incluindo os elementos de prova subjacentes, à autoridade competente. Se detetarem deficiências nas políticas de segurança ou na sua implementação, as autoridades com-

[18] Uma norma técnica standard de segurança é, atualmente, a ISO 27001 <https://www.27001.pt/>

petentes podem emitir instruções vinculativas dirigidas aos operadores de serviços essenciais, para que estes corrijam as deficiências detetadas (artigo 15 da Dir. 2016/1148).

Por seu turno, os *prestadores de serviços digitais* são obrigados a garantir um nível de segurança proporcional ao grau de risco para a segurança dos serviços digitais que fornecem, dada a importância dos seus serviços para as operações de outras empresas na União.

Os serviços digitais abrangem os mercados em linha, os motores de pesquisa em linha e os serviços de computação em nuvem (art. 4/5, anexo III). Nos termos do artigo 4/17-19 da Dir. 2016/1148: a) o *mercado em linha* permite a consumidores e/ou a comerciantes a celebração de contratos de venda ou de prestação serviços, quer no sítio do mercado em linha quer no sítio web do comerciante que utiliza os serviços de computação do mercado em linha (por ex. Amazon); b) o *motor de pesquisa em linha* disponibiliza aos seus utilizadores a consulta de todos os sítios web disponíveis "numa determinada língua com base numa pesquisa sobre qualquer assunto, sob a forma de uma palavra-chave, de uma frase ou de outros dados, e que responde fornecendo ligações onde podem ser encontradas informações relacionadas com o conteúdo solicitado" (por ex., Google); c) o serviço de computação em nuvem faculta o "acesso a um conjunto modulável e adaptável de recursos computacionais partilháveis".

Entende-se que os requisitos de segurança aplicáveis aos prestadores de serviços digitais podem ser menos exigentes já que, na prática, o seu grau de risco é inferior ao grau de risco a que estão sujeitos os operadores de serviços essenciais. Assim, por exemplo, a autoridade competente não tem uma obrigação

geral de supervisionar os prestadores de serviços digitais (considerandos 49 e 60 da Dir. 2016/1148).[19]

Dever de notificação dos incidentes de segurança

As entidades sujeitas a deveres de segurança têm um dever de notificar incidentes, i.e., eventos com um efeito adverso real na segurança das redes e da informação (artigo 14/3 da Dir. 2016/1148). As notificações de incidentes devem ser recebidas pelas autoridades competentes ou pelas equipas de resposta a incidentes de segurança informática (CSIRT).

Para determinar a importância do impacto de um incidente são estabelecidos alguns parâmetros como (1) o número de utilizadores afetados pela perturbação do serviço essencial, (2) a duração do incidente, e (3) a distribuição geográfica, no que se refere à zona afetada pelo incidente (artigo 14/4 da Dir. 2016/1148).

Os prestadores de serviços digitais não estabelecidos na União que ofereçam serviços na União devem designar obrigatoriamente um representante. Segundo o considerando 65 da Dir. 2016/1148: "A fim de determinar se esses prestadores oferecem ou não serviços na União, haverá que apurar se é evidente a sua intenção de oferecer serviços a pessoas num ou mais Estados-Membros. O mero facto de estar acessível na União um

[19] O artigo 16/11 da Dir. Dir. 2016/1148 isenta dos referidos deveres de segurança as microempresas e as pequenas empresas, tal como definidas na Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, de modo a não a ficarem sujeitas a encargos financeiros e administrativos desproporcionados (considerando 53).

sítio web do fornecedor de serviços digitais ou de um intermediário ou um endereço eletrónico ou outro tipo de contactos ou de ser utilizada uma língua de uso corrente no país terceiro em que o fornecedor de serviços digitais se encontra estabelecido não é suficiente para determinar essa intenção. Contudo, há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar serviços nessa outra língua, ou a referência a clientes ou utilizadores na União, que podem ser reveladores de que o fornecedor de serviços digitais tenciona oferecer serviços na União."[20]

[20] Para efeitos de determinação do foro competente nos termos do Regulamento Bruxelas I (Regulamento (UE) n.º 1215/2012 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2012, relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial (revogou e substituiu o Regulamento 44/2001)], o Tribunal de Justiça clarificou a noção de atividades dirigidas no contexto da Internet nos acórdãos *Alpenhof* e *Pammer*, de 7 de dezembro de 2010 (procs. C-144/09 e C-585/08, Colet., p. I-12527). Para determinar se um sítio profissional dirige a sua atividade ao EM do domicílio do consumidor deve ter-se em conta se, antes da celebração de qualquer contrato, resultava desse sítio e da sua atividade em geral que procurava oportunidades de negócio nesse EM. A mera acessibilidade do profissional no EM de domicílio do consumidor é insuficiente para estabelecer a conexão. O Tribunal de Justiça apresenta uma lista não exaustiva de tópicos, tais como: a) a natureza internacional da atividade, b) a referência a itinerários a partir de outros EM para ir ao local de estabelecimento do profissional, c) a utilização de línguas ou de moedas para além das que são geralmente aceites no seu EM de estabelecimento, d) a menção a números de telefone com código internacional, e) recurso a serviços pagos de indexação de resultados de pesquisa para facilitar acesso ao seu sítio por parte de consumidores domiciliados em outros EM, etc.

Conclusão

A promoção do comércio eletrónico depende em larga medida da proteção dos dados pessoais e da segurança das redes e da informação, aí se alicerçando a confiança dos consumidores. O consumidor, enquanto pessoa singular, é titular de dados pessoais protegidos pelo Regulamento Geral de Proteção de Dados. Por outro lado, enquanto utilizador de serviços essenciais e de serviços digitais beneficia do regime da segurança das redes e da informação.

O consumidor tem direito nomeadamente à confidencialidade e à segurança do tratamento dos seus dados pessoais, ficando as empresas que tratam os dados pessoais dos consumidores sujeitas às sanções especialmente gravosas previstas no RGPD. As empresas que pratiquem comércio eletrónico, sem cumprir as exigências de dados pessoais dos consumidores e de segurança informática das redes e da informação, ficam igualmente sujeitas a medidas cautelares de cessação, suspensão ou interdição de fornecimentos, nos termos do artigo. 21/2-d) da LDC.

Relativamente a empresas não estabelecidas em Portugal, mas que dirigem as suas atividades para o mercado português, a segurança informática do consumidor justificará a adoção de medidas restritivas, incluindo providências concretas contra um prestador de serviços, à circulação de um determinado serviço da sociedade da informação proveniente de outro Estado membro da União Europeia na medida em que possa lesar ou ameaçar gravemente os consumidores, nos termos do diploma do comércio eletrónico.