CATÓLICA LAW REVIEW

Identidade e autodeterminação informacional no novo Regulamento Geral de Proteção de Dados:

a inevitável privatização dos deveres estaduais de proteção

Guilherme da Fonseca Teixeira*

Mestrando da Escola de Lisboa da Faculdade de Direito
da Universidade Católica Portuguesa

SUMÁRIO

---

* Licenciado em Direito pela Faculdade de Direito da Universidade de Lisboa. Mestrando em Direito Administrativo na Faculdade de Direito da Universidade Católica Portuguesa – Escola de Lisboa, encontra-se atualmente a elaborar a dissertação de natureza científica. O presente artigo corresponde, com algumas alterações, ao relatório final apresentado na cadeira de Proteção Administrativa de Direitos Fundamentais, lecionada pelo Professor Doutor Jorge Pereira da Silva. *E-mail*: guilhermefonsecateixeira@gmail.com.

1. Introdução

Na sociedade atual, em que se inscreve a democratização das tecnologias de informação, os cidadãos vêm-se confrontados, embora de forma silente na «penumbra» da legalidade que lhes é cognoscível, com uma tensão dialética entre o fenómeno de recolha, armazenamento, tratamento e transmissão de dados de carácter pessoal[1] e o seu próprio estatuto jurídico-cívico.

De facto, o desenvolvimento tecnológico exponencial no domínio do controlo, vigilância e segurança na transmissão de dados informatizados[2], registado nas últimas décadas do século XX, ficou marcado, de forma paradigmática, por: *i*) novas tecnologias com elevada capacidade de processamento, de transmissão e de armazenamento de dados; *ii*) redes interconectadas de partilha de informação; e *iii*) tecnologias de localização geográfica em tempo real.

Ora, afigura-se problemático, do ponto de vista da tutela dos bens jusfundamentais dos cidadãos, reconhecer que lhes é, em certa medida, desconhecido que a recorrente disponibilização a terceiros de múltiplos dados pessoais (*v.g.*, nome, género, filiação, origem étnica, morada, profissão, elementos clínicos, dados genéticos, crenças religiosas, ideologias políticas, gostos literários e musicais, opções de consumo), pese embora se insira num momento quotidianamente determinado ou determinável e com um fim aparentemente específico ou concretamente delimitável, se tornou uma constante ineliminável da sociedade atual[3], que pode, inclusivamente, permitir aos detentores materiais dos seus dados um uso indistinto, ilegítimo e indiscriminado dos mesmos e, *in extremis*, culminar na elaboração de bancos de ficheiros consolidados, contendo um perfil detalhado sobre cada indivíduo, numa ou em diversões dimensões suas.

1 Neste sentido, Rosa Matacán, Maria, 2011, *Protección de Datos Persónales en la Sociedad de la Información y la Vigilancia*, La Ley, Madrid, p. 15. Considera-se que o grau de perceção do risco tecnológico influencia decisivamente a tomada de decisão pública (em especial, legislativa e administrativa), sendo os sujeitos relevantes na perceção do risco quanto à problemática da proteção de dados os seguintes: *i*) público em geral e comunidades locais; *ii*) autoridades públicas; *iii*) profissionais do sector; *iv*) trabalhadores; *v*) peritos; *vi*) comunicação social.

2 Cfr. Graham, Stephen, 1988, *Spaces of surveillant simulation: New Technologies, digital representations and material geographies*, Environment and Planning D: Society and Space, pp. 483 e ss.

3 Neste sentido, Teixeira, Maria Leonor da Silva, 2013, «A União Europeia e a protecção de dados pessoais: "Uma visão futurista"?», in *Revista do Ministério Público*, n.º 135, p. 66, afirma que «A evolução científica, o desenvolvimento dos meios de comunicação e das tecnologias informáticas permitem a dispersão quase imediata e incontrolável dos dados pessoais recolhidos […] torna-se, pois, essencial dotar o cidadão de meios que lhe permitam controlar, em cada momento, quem, como, onde e por que razão circulam ou são conhecidas quaisquer informações sobre parcelas da sua vida mais ou menos íntima, mais ou menos privada».

Verifica-se, portanto, a pouco e pouco, um fenómeno de crescente *captura silenciosa* da identidade pessoal de cada um, com um potencial lesivo, direto ou indireto, quase ilimitado do bloco de direitos fundamentais constitucionalmente reconhecido aos particulares.

Ainda que se tome como indispensável ou, de certo modo, inevitável algum grau de renúncia à intimidade e privacidade nos tempos modernos (*v.g.*, no acesso e no desempenho de determinados cargos profissionais, na simples atuação enquanto operador económico do mercado ou mero consumidor), tendo em vista as exigências que decorrem, nos casos de atividades jurídico-administrativas exercidas por entidades públicas ou entidades privadas no exercício de prerrogativas ou de poderes públicos, dos princípios da transparência, da imparcialidade, da boa administração e dos demais ditames e princípios gerais da atividade administrativa, também se há de reconhecer que o potencial lesivo subjacente sobre os direitos fundamentais dos particulares é bastante considerável, sobretudo no âmbito das suas esferas pessoal, familiar e profissional.

Na verdade, revelando os dados disponibilizados uma «imagem» da pessoa (nas suas várias dimensões), tais informações podem vir a ser utilizadas para fins contrários ao princípio da dignidade da pessoa humana[4], instrumentalizando o titular dos dados num contexto de situações verdadeiramente patológicas que, por isso, justificam forte prevenção e repressão jurídica, moral e ética, não apenas em sede de atuação das entidades públicas, mas também de entes privados no exercício de funções públicas[5].

A tensão entre as diferentes valorações em colisão afigura-se manifesta no contexto atual: se, por um lado, se exige a construção de uma esfera de liberdade dos cidadãos enquanto indivíduos com capacidade de autodeterminação pessoal, sem ingerência estatal ou privada de modo arbitrário ou autoritário quanto aos fragmentos da sua individualidade que a recolha, tratamento, armazenamento e utilização ilegítima dos seus dados pessoais constitui; por outro,

4 Cfr. Novais, Jorge Reis, 2015, *A Dignidade da Pessoa Humana*, vol. I, Almedina, pp. 58 e ss., afirma que a dignidade da pessoa humana se identifica com «a ideia de um valor próprio, supremo e inalienável atribuído à pessoa só pelo facto de o ser, por simples facto da sua humanidade; a ideia de respeito, de igual consideração dos interesses de cada pessoa, da sua vida, da sua autonomia, liberdade e bem-estar; a ideia da pessoa como fim e não como mero meio ou instrumento de outros; a ideia de que é a pessoa individualmente considerada, e não qualquer realidade transpersonalista, que justifica a existência do Estado e do poder político organizado da comunidade», concretizando a «fórmula do objeto» que teve, historicamente, origem na jurisprudência do Tribunal Constitucional Alemão. Importa, neste âmbito, impedir o fenómeno de transformação do cidadão em mero objeto de informações para o Estado ou entidades privadas, sem qualquer poder de controlo sobre si ou sobre os seus dados pessoais.

5 Afirma-se como característica inegável da globalização a fuga ao controlo democrático das atuações de recolha, tratamento e utilização de dados pessoais efetuados por entidades privadas, uma vez que, não estando sujeitas ao escrutínio público (razão pela qual carecem de legitimidade democrática ou de uma verdadeira *public accountability*), dão azo a novos perigos para os direitos fundamentais dos indivíduos.

o valor da segurança[6], que norteia o sistema jurídico, também exige a dotação prévia dos entes que se relacionam com os particulares nesta sede de certas capacidades intrusivas nos seus direitos e liberdades, sobretudo através de instrumentos que permitam o acesso a determinados tipos de informação, a fim de tutelar, de forma reflexa, bens jusfundamentais de terceiros e da comunidade.

Na senda das considerações apresentadas, o presente artigo demandará uma análise sobre o fundamento constitucional do direito à proteção de dados pessoais *(Datenschutz)* e sobre as suas fontes normativas de maior relevo, assim como um excurso sobre a recente revisão operada pelo legislador europeu do quadro normativo relativo à proteção de dados.

Abordar-se-á, em particular, o novo Regulamento Geral de Proteção de Dados, que lança novos problemas e desafios, num campo paradigmático da atual sociedade de risco (mormente, de risco tecnológico[7]), sobre o atual entendimento relativo ao escopo de proteção dos direitos, liberdades e garantias dos cidadãos[8].

---

6 Cfr. Canaris, Claus-Wilhem, 1989, *Pensamento sistemático e conceito de sistema na Ciência do Direito*, Lisboa, pp. 9 e ss. A segurança, sendo inseparável da noção de Estado de Direito Democrático e Social, transcende a dimensão constitucional para se afirmar como valor imanente e enformador do próprio sistema jurídico, ao fixar as finalidades axiológicas pelas quais o mesmo se deve orientar. Ora, considerando que a norma, enquanto critério de decisão do caso concreto que exprime um «dever ser» (seja norma-regra ou norma-princípio), «representa um momento necessário do processo de integração fático-axiológica, ordenando factos sociais sob o influxo de valores» (Cfr. Reale, Miguel, 2005, *Filosofia do Direito*, II, n.º 207, in Ascensão, Oliveira, *O Direito – Introdução e Teoria Geral*, Almedina, p. 215, de acordo com a teoria tridimensional do Direito que é propugnada pelo autor), impõe-se concluir que o valor da segurança se encontra, por esta via, necessária e normativamente positivado nos diversos ordenamentos jurídicos, ainda que, considerando determinados fatores (*v.g.*, contexto histórico-cultural, político e sociológico), se revele sob formas distintas. No ordenamento jurídico nacional, e considerando a temática do presente escrito, o valor em causa revela-se na conformação do conteúdo do direito fundamental à proteção de dados, previsto no artigo 35.º da Constituição da República Portuguesa, e no correspondente conjunto de restrições constitucionais e legais que se consideram admissíveis ao mesmo.

7 Cfr. Terrinha, Luís Heleno, *Direito e contingência: com e para além de Ulrich Beck*, *In Memoriam Ulrich Beck*, Atas do colóquio promovido pelo ICJP e pelo CIDP em 22 de outubro de 2015, disponível em https://www.icjp.pt/sites/default/files/publicacoes/files/ebook_ulrichbeck_0.pdf, p. 21, afirma que a conceptualização da sociedade de risco constitui «uma sugestiva construção semântica através da qual descobrir ou representar uma certa unidade da sociedade (daí, também, a sua força atrativa num contexto de complexidade), unidade essa que é reconduzida aos riscos ameaçadores que resultam do progresso técnico e tecnológico da humanidade e à inevitabilidade de o preço a pagar pelas vantagens que esse progresso nos traz se traduzir na necessidade de aceitar determinadas consequências negativas laterais».

8 Cfr. Brito, Miguel Nogueira de, *O admirável novo constitucionalismo da Sociedade de Risco*, *In Memoriam Ulrich Beck*, Atas do colóquio promovido pelo ICJP e pelo CIDP em 22 de outubro de 2015, disponível em https://www.icjp.pt/sites/default/files/publicacoes/files/ebook_ulrichbeck_0.pdf, pp. 54 e ss. É inegável que a sociedade atual se confronta com tendências securitárias que, muitas vezes, surgem encapotadas de políticas de justiça de prevenção e repressão da criminalidade altamente organizada ou terrorismo, que fazem perigar a efetividade dos direitos, liberdades e garantias constitucionais dos cidadãos. Recentemente, a aprovação do *Investigatory Powers Act* pelo Parlamento do Reino Unido, em 29 de novembro de 2016 (que entrou em vigor em 30 de dezembro do mesmo ano), também designado por «*The Snooper's Charter*», constituirá certamente um marco histórico, porquanto o diploma expande os poderes investigatórios e de vigilância das forças policiais e de inteligência britânicas ao ponto de permitir o

2. Da jusfundamentalidade do direito à proteção de dados

O direito fundamental à proteção de dados surge, originariamente, consagrado no artigo 35.º da Constituição da República Portuguesa[9] (doravante, «CRP»), constituindo uma opção legislativa inovadora em face das soluções adotadas pelas suas congéneres ao nível europeu e internacional. A sua consagração, *ab initio*, no texto fundamental pelo legislador constituinte é de salutar, sobretudo pela sua particular proatividade em função do exponencial desenvolvimento tecnológico, associado aos riscos para os direitos fundamentais dos cidadãos que lhe são inerentes, que se veio a verificar na Sociedade da Informação nos anos que se seguiriam.

O dispositivo em causa, note-se, apresenta uma natureza compreensiva, na medida em que se desdobra em diversos corolários específicos consoante a dimensão sobre a qual recai o perigo concreto de instrumentalização do direito.

No plano da sua função garantística[10], o preceito positiva, nomeadamente, as seguintes vertentes do direito à proteção de dados pessoais: *i*) o direito de

recurso a técnicas de *hacking* e similares de forma a aceder aos dados pessoais de quaisquer sujeitos que sejam alvo de investigação. A aprovação do diploma em causa simboliza uma opção clara do Legislador britânico pela «legalização» de atividades que, na prática, foram recorrentemente exercidas, ao longo dos últimos anos, em evidente violação do direito à proteção de dados pessoais e do direito à privacidade dos cidadãos, simultaneamente, como o demonstra a decisão do *Investigatory Powers Tribunal* – a única jurisdição com competência para julgar ações interpostas contra o *MI5*, o *MI6* e o *GCHQ* –, de 4 de novembro de 2015, que condenou as agências de segurança britânicas pela recolha – através de técnicas de vigilância da atividade telefónica e informática – e armazenamento ilegais de quantidades maciças de dados pessoais dos cidadãos (*Bulk Communications Data* – BCD), incluindo informação financeira, fiscal, comercial, médica e do foro pessoal e familiar, durante os últimos 17 anos (!) (1998-2015), em violação do disposto no artigo 8.º da Convenção Europeia dos Direitos do Homem, que consagra, *lato sensu*, o direito à privacidade.

9 A Constituição Portuguesa foi o primeiro texto constitucional a consagrar a proteção de dados pessoais como um direito fundamental autónomo em face do direito à reserva da intimidade da vida privada. Embora o artigo 35.º tenha sido introduzido na constituição originária de 1976, o seu conteúdo atual resulta, em grande medida, da quarta revisão constitucional, de 1997, que visou compatibilizar o dispositivo com o que se preceituava na Diretiva n.º 95/46/CE. Neste sentido, Lopes, Joaquim de Seabra, 2016, *O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível*, in Fórum de Proteção de Dados, n.º 2, pp. 15 e ss., associando a sua introdução no ordenamento jurídico nacional como uma reação à Lei n.º 2/73, de 10 de fevereiro, que instituía o registo nacional de identificação através da atribuição de um número de identificação único a todos os cidadãos, e Pinheiro, Alexandre Sousa, 2015, *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, Lisboa, pp. 695 e ss.

10 Neste sentido, Canotilho, Gomes / Moreira, Vital, 2017, *Constituição da República Portuguesa Anotada*, vol. I, Coimbra Editora, pp. 551 e ss., consideram que a operatividade do direito à proteção de dados, nomeadamente do direito de acesso e conhecimento dos dados pessoais registados, se encontra na dependência do correto desempenho da função hermenêutica e orientadora de um conjunto de princípios-quadro e de *guidelines* neste âmbito: *i*) publicidade; *ii*) justificação social (sujeição das atividades de recolha, tratamento e utilização de dados a um «objetivo geral e usos específicos socialmente aceites»); *iii*) transparência; *iv*) especificação de finalidades; *v*) limitação da recolha, de acordo com os ditames e

acesso, alteração, atualização, retificação e eliminação dos registos informáticos do titular do direito (n.º 1, 1.ª parte); *ii*) o direito de informação sobre as finalidades a que se destinam os dados informatizados, assim como da identidade dos responsáveis pelo tratamento de dados (n.º 1, 2.ª parte); *iii*) a imposição de que a fiscalização do cumprimento das diretrizes constitucionais e legais quanto à recolha, armazenamento, tratamento e utilização de dados pessoais seja da competência de uma entidade administrativa independente, não sujeita aos poderes de direção, superintendência e tutela da Administração direta do Estado, nomeadamente do Governo e restante aparelho da Administração Central, de modo a evitar «tentações» sobre utilizações ilegítimas e/ou discriminatórias com fins político-partidários (n.º 2); *iv*) o direito ao não tratamento informático de certos tipos de dados pessoais que, historicamente, fundaram atos discriminatórios atentatórios da dignidade da pessoa humana, salvo consentimento expresso do titular, autorização legal com garantias de não discriminação ou processamento de dados para fins meramente estatísticos não individualmente identificáveis (n.º 3); *v*) o direito ao sigilo em relação aos responsáveis pelos ficheiros informatizados e a terceiros, incluindo o direito à não interconexão de dados fora dos casos legalmente previstos, proibindo-se a criação de um perfil completo e detalhado da pessoa contendo dados de diversa natureza (n.os 4 e 5); *vi*) o direito de acesso às redes informáticas de uso público (n.º 6); *vii*) a extensão da proteção aos dados pessoais constantes de ficheiros manuais ou não informatizados (n.º 7).

De notar, a este propósito, que as dimensões enunciadas possuem, necessariamente, diferentes graus de intensidade de controlo[11], a ser aferidas perante a violação concreta da específica vertente em causa, no que constitui um parâmetro essencial de conformação da atuação estadual no âmbito da restrição de

corolários do princípio da proporcionalidade; *vi*) princípio da fidelidade; *vii*) limitação da utilização; *viii*) garantias de segurança; *ix*) responsabilidade legal, ética e deontológica; *x*) princípio da política de abertura; *xi*) princípio de limitação de tempo.

A dimensão garantística do direito fundamental à proteção de dados projeta-se no escopo de proteção dos demais direitos fundamentais dos cidadãos, funcionando como um mecanismo de proteção reflexa dos direitos sobre os quais a natureza da informação recai. De facto, se, *v.g.*, uma empresa detentora dos registos de pesquisa na Internet de determinado cidadão tiver elaborado um perfil de saúde médica do sujeito com base na compilação de um conjunto de pesquisas sobre determinado tipo de doença e, posteriormente, «disponibilizar» (mais corretamente, «alienar») esse perfil a determinada empresa farmacêutica, que passa a assumir práticas constantes de envio de propaganda e publicidade não solicitada ao indivíduo em causa sobre os medicamentos ou tratamentos recomendados para a doença específica – bens ou serviços esses que ela própria comercializa –, então não estará em causa apenas uma violação do direito à proteção de dados (que ocorre num primeiro momento, com a disponibilização da empresa detentora do motor de busca dos dados e com o acesso ilegítimo da farmacêutica aos mesmos), mas também, eventualmente, uma violação do direito à privacidade (na dimensão de *right to be let alone* e de intimidade privada e familiar), à saúde e à autodeterminação pessoal.

11 *Cfr*. Alexandrino, José Melo, 2014, «Jurisprudência da Crise. Das questões Prévias às Perplexidades», *O Tribunal Constitucional e a Crise – Ensaios Críticos*, p. 67.

direitos fundamentais dos particulares[12], consoante a estrutura normativa concreta em que as vertentes referidas se encontrem constitucional e legalmente consagradas[13].

No sentido de dar cumprimento ao impulso legiferante[14] que consta da 1.ª parte do n.º 2 do artigo 35.º da CRP, o legislador ordinário veio densificar o conceito de «dados pessoais»[15], nos termos do artigo 3.º, al. *a*), da Lei n.º 67/98, de 26 de outubro, ou Lei de Proteção de Dados Pessoais[16], considerando-se como tal «qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ["titular dos dados"]», sendo «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».

Foram, ainda, aprovados um conjunto de diplomas que estabelecem o regime quanto à recolha, armazenamento, tratamento, utilização e circulação de dados pessoais, impondo determinadas condicionantes e restrições em nome da salvaguarda dos direitos, liberdades e garantias do titular dos dados.

No quadro do bloco de legalidade ordinária que se impõe à função administrativa sobre proteção de dados pessoais, deve realçar-se que – pese embora o Código do Procedimento Administrativo de 1991 (aprovado pelo Decreto-Lei n.º 442/91, de 15 de novembro) não contemplasse qualquer dispositivo que, de forma expressa e inequívoca, tutelasse a proteção de dados dos particulares – era pacífico na doutrina e na jurisprudência que, em face da consagração constitucional do direito no artigo 35.º da Constituição e do restante bloco de

12 Neste sentido, Novais, Jorge Reis, 2010, *As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*, 2.ª ed., Coimbra Editora, p. 799.

13 Neste sentido, Egídio, Mariana Melo, 2010, «Análise da estrutura das normas atributivas de direitos fundamentais. A ponderação e a tese ampla da previsão, in *Estudos em Homenagem ao Prof. Doutor Sérvulo Correia*», vol. I, Faculdade de Direito da Universidade de Lisboa, pp. 626 e ss., defendendo que «com o recurso à ponderação, pode frequentemente estabelecer-se um resultado racional, através da limitação da mencionada operação discricionária pelo recurso, nomeadamente, a metaprincípios, sem significar que tal operação conduza sempre a um único resultado».

14 Neste sentido, Miranda, Jorge / Medeiros, Rui, 2017, *Constituição Portuguesa Anotada*, tomo I, 2.ª edição revista, Universidade Católica Editora, e o acórdão do Tribunal Constitucional n.º 182/89, disponível em http://www.dgsi.pt.

15 Para uma perspetiva histórica da controvérsia associada à delimitação do conceito de «dados pessoais» no ordenamento nacional, veja-se Nicolau, Tatiana Duarte, 2015, *O armazenamento de amostras de ADN e as bases de dados de perfis genéticos*, Comissão Nacional de Proteção de Dados, pp. 32 e 33.

16 A Lei n.º 67/98 transpõe para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, relativa à proteção de pessoas singulares no que concerne ao tratamento de dados pessoais e à livre circulação desses dados.

legislação vigente[17], ao direito fundamental em causa sempre foi reconhecida força vinculativa imediata no âmbito do procedimento administrativo, independentemente de a competência para a sua realização ser atribuída a entidades públicas ou a entidades privadas no exercício de funções públicas.

Atualmente, com a revisão do CPA operada pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, consagrou-se expressamente o princípio da proteção de dados pessoais, no artigo 18.º, numa opção de positivização na legislação jusprocedimental administrativa com uma notória função pedagógico-preventiva dirigida aos serviços da administração pública[18].

Feito este breve excurso, cumpre destacar que se afigura da maior relevância a opção pela autonomização do direito à proteção de dados enquanto bem jusfundamental autónomo, em face do direito fundamental à reserva da intimidade da vida privada, previsto no artigo 26.º da CRP, o que não constitui, de todo, uma solução consensual do ponto de vista legislativo, doutrinário e jurisprudencial no direito comparado, identificando-se sistemas nos quais se seguiu a via da autonomização do direito à proteção de dados[19] e sistemas nos

17 Para este efeito, e no âmbito da economia do presente artigo, importa realçar a já referida Lei de Proteção de Dados, a Lei n.º 41/2004, de 18 de agosto (que regula a proteção de dados pessoais nas comunicações eletrónicas), e a Lei n.º 26/2016, de 22 de agosto (que regula o acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos), enquanto diplomas basilares que consagram o regime de proteção de dados pessoais que se impõe aos órgãos e serviços da Administração.
Para uma visão histórica sobre os diplomas internacionais de relevo na proteção de dados, Teixeira, Maria Leonor da Silva, 2013, «A União Europeia e a protecção de dados pessoais: "Uma visão futurista"?», in *Revista do Ministério Público*, n.º 135, 2013, pp. 77 e 78, salientando-se a Convenção n.º 108 do Conselho da Europa, de 28 de janeiro de 1981, que pretendia «tutelar a intimidade e garantir o funcionamento do mercado interior e a livre circulação de dados pessoais entre os Estados aderentes».

18 Sustentando que da inter-relação e dos nexos intrasistemáticos que se podem estabelecer entre o princípio da proteção de dados e o princípio da administração aberta, consagrado no artigo 17.º, se deduzem «importantes inovações na forma como a proteção de dados se relaciona quer com o acesso a informação procedimental quer com a transparência administrativa», Pinheiro, Alexandre Sousa, 2015, «A proteção de dados no novo Código do Procedimento Administrativo», in *Comentários ao Novo Código do Procedimento Administrativo*, 2.ª edição, AAFDL Editora, pp. 253 e ss.

19 Neste sentido, Serrano Pérez, Maria, 2013, *El Derecho Fundamental a la protección de datos. Derecho español y comparado*, Civitas, Madrid, p. 72. A Constituição Espanhola, no artigo 18.º, n.º 4, acabou por seguir a mesma orientação que a Constituição Portuguesa ao consagrar o direito fundamental à proteção de dados pessoais, tendo em conta a orientação interpretativa da jurisprudência do Tribunal Constitucional Espanhol, nas sentenças n.os 290/2000 e 292/2000, de 30 de novembro.
Quanto ao ordenamento alemão, embora a Constituição Alemã não autonomize o direito em causa, a jurisprudência do Tribunal Constitucional Alemão, afirmando-se, neste âmbito, como marco histórico a sentença de 15 de dezembro de 1983, considera que a proteção do indivíduo contra a recolha, armazenamento, utilização e transmissão de dados ilegítima se pode retirar do disposto no artigo 2.º, n.º 1, da Constituição, que consagra um direito geral de personalidade dos indivíduos em nome do princípio da dignidade da pessoa humana, sob pena de «coisificação» do indivíduo enquanto mero objeto da atuação estadual («fórmula do objeto»).
Sendo certo que a Convenção Europeia dos Direitos do Homem também não autonomiza expressamente o direito à proteção de dados pessoais, a jurisprudência do Tribunal Europeu dos Direitos do Homem tem

quais o direito em causa se considera como uma mera manifestação do direito à privacidade[20].

---

entendido que este se terá, forçosamente, de retirar do artigo 8.º da mesma, que consagra a proteção da vida privada e familiar do domicílio e das comunicações. Nos acórdãos *Leander v. Suécia*, de 26 de março de 1987, e *Gaskin v. Reino Unido*, de 7 de julho de 1989, o tribunal reconheceu um direito de acesso às informações pessoais armazenadas do titular dos dados, mesmo que lhes seja atribuído carácter sigiloso pela entidade pública detentora dos mesmos, violando o disposto no artigo 8.º a recusa de facultar aos particulares acesso aos seus dados ou o seu tratamento ilegítimo.
No Direito da União Europeia, a autonomização do direito à proteção de dados pessoais, nos artigos 16.º do Tratado sobre o Funcionamento da União Europeia e 8.º da Carta dos Direitos Fundamentais da União Europeia em face do artigo 7.º da Carta, que consagra o direito à reserva da intimidade da vida privada. Ao nível do regime, que consta dos n.os 2 e 3 do artigo 8.º, consagram-se: *i*) condicionantes ou restrições à recolha, utilização e tratamento de dados, que deverão assentar no consentimento válido do titular (consentimento expresso, livre e esclarecido) ou em justificação bastante que legitime a desnecessidade de consentimento para as ações referidas, num elemento funcional (os dados devem ser recolhidos e armazenados apenas para determinados fins concretos, sendo ilegítima uma apropriação excessiva de dados pessoais em função do fim visado pela recolha de dados ou uma utilização para fins diversos dos que são informados ao titular ou permitidos legalmente) e observar os ditames do princípio da lealdade (nomeadamente, as imposições de transparência e imparcialidade que decorrem do mesmo); *ii*) o direito de acesso e de retificação dos dados recolhidos; *iii*) sujeição à fiscalização de uma autoridade independente do cumprimento das disposições – no plano comunitário, a Autoridade Europeia de Proteção de Dados, criada pelo Regulamento n.º 45/2001, de 18 de dezembro, e, no ordenamento nacional, a Comissão Nacional de Proteção de Dados (CNPD), criada pela Lei n.º 43/2004, de 18 de agosto.
A jurisprudência do Tribunal de Justiça da União Europeia afirmou, nos casos *Volker und Markus Schecke GbR* (C-92/09) e *Hartmut Eifert* (C-93/09) v. *Land Hessen*, de 9 de novembro de 2010, que o direito à proteção de dados não é absoluto, antes deve ser sujeito a uma reserva de ponderação que considere a sua função na sociedade.

20 Em diversos ordenamentos jurídicos não se considera necessária a autonomização, nos elencos constitucionais de bens jusfundamentais e na jurisprudência dos respetivos tribunais constitucionais, do direito fundamental à proteção de dados pessoais, mesmo que no confronto com os avanços tecnológicos e digitais registados e com a universalização do uso da informática por entidades públicas e privadas no exercício da função administrativa, com fundamento na agilização e economia dos procedimentos em nome dos princípios da eficiência, eficácia e boa administração. É o caso da Constituição Italiana, da Constituição Francesa (que, numa opção que pode ser alvo de críticas imediatas dada a desatualização do normativo em causa, se continua a reger pelos direitos e princípios consagrados na Declaração Universal dos Direitos do Homem e do Cidadão, de 1789), e do *Human Rights Act* inglês, de 1998.
Ora, o entendimento que subjaz a estes ordenamentos na opção de não autonomização do direito fundamental à proteção de dados é o de que o seu conteúdo normativo se encontra abrangido pelo direito à reserva da intimidade da vida privada, não se identificando um recorte dogmático próprio.
No entanto, parece ser uma solução dogmaticamente criticável dada a fluidez com que, no Direito Comparado dos Estados-membros da UE, o direito à proteção da intimidade da vida privada é concebido, por diversas vezes confundido com o direito à autodeterminação pessoal – vejam-se as críticas, julgo que infundadas, que são assacadas ao acórdão *A*, *B and C v Ireland* do Tribunal Europeu dos Direitos do Homem, de 2010, que considerou, de forma acertada, que do direito à reserva da intimidade da vida privada não se pode retirar um «direito ao aborto» ao abrigo do artigo 8.º da CEDH, por Goold, Imogen, 2015, «A, B and C v Ireland [2010]», in *Landmark Cases in Medical Law*, Hart Publishing, pp. 335 e ss., considerando que se trata de uma decisão conservadora, com o efeito útil de impor aos Estados uma obrigação de criar legislação clara e precisa sobre os critérios de permissibilidade ou proibitividade de realização de aborto, tendo preferido uma orientação decisória semelhante à que tem sido seguida na jurisprudência firmada no sistema legal norte-americano, em especial após o caso *Roe vs Wade*, de 1973, do *Supreme Court*, no qual se reconheceu um «direito ao aborto» adveniente do direito à privacidade.
No Direito norte-americano, o direito à privacidade *(privacy)* é concebido de modo amplíssimo (cfr. Warren, Samuel / Brandeis, Louis, 1995, *El derecho a la intimidad*, Madrid: Civitas), não apenas na doutrina mas

Na verdade, talvez visando, apenas, introduzir medidas de segurança no domínio informático, o legislador constitucional acabou por consagrar o direito à proteção de dados enquanto direito à identidade e autodeterminação informativa[21], que assume uma vertente ativa de titularidade do poder de controlo sobre os seus próprios dados pessoais[22], que se afigura absolutamente essencial no cumprimento do escopo da norma em causa, no sentido da tutela efetiva da dignidade da pessoa humana em face da sociedade atual de reconhecido risco tecnológico, o que não se coaduna com a limitada vertente (historicamente) passiva como é concebido o direito à privacidade[23], que meramente habilita o

também na jurisprudência (como o caso *Roe vs Wade* demonstra), sendo, usualmente, identificadas quatro dimensões nucleares (cfr. Nicolau, Tatiana Duarte, 2015, *O armazenamento de amostras de ADN e as bases de dados de perfis genéticos*, Comissão Nacional de Proteção de Dados, pp. 27 e 28): *i*) direito a estar sozinho *(right to be alone)*; *ii*) direito à intimidade da vida privada e familiar; *iii*) direito ao anonimato; *iv*) direito à não intervenção de terceiros *(right to be let alone)*.

21 Neste sentido, Ferreira, Pedro, 2006, *A protecção de dados pessoais na sociedade de comunicação – Dados de Tráfego, Dados de Localização e Testemunhos de Conexão*, O Espírito das Leis, pp. 144 e ss. Em sentido diverso, considerando que o direito à proteção de dados pessoais é uma mera garantia constitucional do direito à privacidade e reserva da intimidade da vida privada, Moniz, Helena, «Os problemas jurídico-penais da criação de uma base de dados genéticos para fins criminais», 2002, *Revista Portuguesa de Ciência Criminal*, n.º 2, pp. 246 e ss. Partindo do mesmo entendimento que esta autora, a jurisprudência do Tribunal Constitucional tem sediado a fundamentação das suas decisões quanto ao tratamento informatizado de dados pessoais no direito à reserva da intimidade da vida privada, nos termos do artigo 26.º da CRP, não fazendo uso da autonomia constitucionalmente concedida ao direito à proteção de dados no artigo 35.º da CRP, num entendimento que, pelas críticas que já lhe foram dirigidas, não se afigura o mais correto do ponto de vista dogmático ou, sequer, o mais idóneo à proteção dos direitos, liberdades e garantias dos cidadãos. Vejam-se, nomeadamente, os acórdãos n.os 355/1997, 255/2002 e 386/2002, pesquisáveis em http://www.dgsi.pt.

22 Quanto à titularidade do direito, é discutível se o direito à proteção de dados pessoais se estende às pessoas coletivas, dada a sua íntima conexão com a esfera privada e de identidade pessoal do indivíduo. Sobre esta discussão, no direito comparado, cfr. Pollman, Elizabeth, 2014, «A Corporate Right to Privacy», in Minnesota Law Review, vol. 99, pp. 32 e 88, considerando que «*most corporations in most circumstances should not have a constitutional right to privacy. There is simply no natural person, or persons, associated in a corporation with a privacy interest at stake and a need for the corporation to vindicate it*», embora «*Certain corporations (which) reflect an associational dynamic, with tightly connected individuals pursuing activity, social, political or religious in nature, that has long been valued in fostering our societal goals of liberty and democracy*», incluindo organizações sem fins lucrativos, possam justificar a extensão, *mutatis mutandis*, do direito à proteção de dados.

23 A jurisprudência do Tribunal Constitucional Alemão densificou o direito à reserva da intimidade da vida privada através da tradicional «teoria das esferas», segundo a qual se identificam três níveis concêntricos de proteção diferenciada: a esfera privada *(Privatsphäre)*, que, por se encontrar dentro do núcleo essencial do direito fundamental na proteção da vida pessoal e familiar mais íntima, não admite qualquer ingerência; a esfera íntima *(Inthimsphäre)*, que admite ingerências de terceiros sob reserva de ponderação, caso o interesse público ou privado for preponderante para justificar a restrição do direito; a esfera individual *(Individualsphäre)*, que simboliza uma área periférica do conteúdo normativo do direito, representando a exteriorização de certos aspetos de personalidade na comunidade, como o nome e a imagem, que admitem uma maior ingerência. Note-se que a evolução da jurisprudência constitucional alemã acabou por abandonar a aplicação da «teoria das esferas» na conformação do direito à proteção de dados pessoais, construindo o seu recorte dogmático a partir do princípio da dignidade da pessoa humana e do direito geral de personalidade constitucionalmente consagrado.

titular do direito a excluir terceiros, sejam entidades privadas ou públicas, da sua esfera de intimidade.

Por conseguinte, é possível identificar no direito à proteção de dados pessoais um recorte dogmático ou âmbito de tutela autónomo que, mais do que procurar garantir uma tutela dos dados pessoais dos cidadãos, consoante a maior ou menor proximidade das informações em causa com a esfera íntima, privada ou individual/social do sujeito (*maxime*, ao núcleo íntimo da pessoa), procura conferir ao titular dos dados o poder de manter na sua disponibilidade a gestão dos mesmos, configurando-se como o direito do indivíduo a controlar a obtenção, detenção, tratamento e transmissão de dados pessoais, autorizando a sua recolha, armazenamento, e utilização, conhecendo onde estão armazenados, a identidade dos responsáveis pelo seu tratamento e quais as suas finalidades, acedendo aos mesmos ou inclusivamente exigindo a sua alteração, retificação ou eliminação *(habeas data)*.

3. Revisão do quadro normativo de proteção de dados pessoais: alterações, inovações e desafios

Ao nível europeu, a União Europeia e o Mercado Interno Comum surgem como uma plataforma jurídica privilegiada de circulação e tratamento de dados pessoais, quer ao nível das instituições e órgãos da União Europeia quer das entidades públicas e privadas dos Estados-membros. Como já se referiu, o artigo 16.º do TFUE e o artigo 8.º da CDFUE contêm a positivização expressa do direito à proteção de dados pessoais e a sua regulamentação basilar, excluindo-se do âmbito de aplicação deste regime as matérias de Política Externa e Segurança Comum (PESC), às quais se aplica o disposto no artigo 39.º do TUE.

No entanto, dado o carácter marcadamente programático e incipiente da regulação do direito à proteção de dados nos dispositivos referidos, por um lado, e as disparidades observadas nos direitos nacionais dos Estados-membros quanto à proteção efetiva do bem jusfundamental em causa, por outro, cedo emergiu a necessidade de regulação da presente matéria, de modo mais densificado, em instrumentos jurídicos comunitários derivados, visando assegurar uma uniformização e harmonização jurídica ao nível da União, em nome dos princípios da equivalência e da efetividade[24] enquanto princípios gerais do Direito da UE.

24 Cfr. Casos *Rewe-Zentralfinanz eG and Rewe-Zentral AG v. Landwirtschaftskammer für das Saarland* (C-33/76), *Express Dairy Foods Ltd. v International Board of Agricultural Produce* (C-130/79), *Factortame I* (C-213/89), *Francovich* (C-6/90 e 9/90) e *Palmisani* (C-261/95), da jurisprudência do TJUE.

Em face do quadro enunciado, foi aprovada a Diretiva 95/46/CE, relativa à proteção do tratamento e circulação dos dados pessoais, que fixa o princípio da livre circulação de dados entre os Estados-membros e estabelece o regime jurídico concretamente aplicável. Uma vez que a referida Diretiva assumia uma linha genérica de regulação da proteção de dados, houve a necessidade de enveredar por uma regulação sectorial da recolha, armazenamento, tratamento e utilização de dados em áreas de atuação com um potencial lesivo elevado dos direitos, liberdades e garantias dos cidadãos, em face das características específicas das respetivas atividades e dos segmentos de mercado em causa. Foi, neste sentido, aprovada a Diretiva 2002/58/CE *(ePrivacy Directive)*, de 12 de julho de 2002, relativa ao tratamento de dados e à proteção da privacidade no sector das telecomunicações.

Volvidas quase duas décadas da entrada em vigor da Diretiva 95/46/CE, a significativa evolução tecnológica registada, a crescente assunção por parte de operadores económicos privados – dotados de um grande poder de influência nos mercados em que atuam e de elementos de transnacionalidade assinalável, dificultando sobremaneira a regulação e fiscalização da sua atividade – de um papel de relevo no âmbito da recolha, tratamento, utilização e circulação de dados e, bem assim, a identificação de algumas lacunas e/ou soluções menos eficazes na Diretiva levaram o legislador europeu a tomar a consciência da necessidade de revisão e de atualização do quadro normativo vigente em matéria de proteção de dados.

Assim, em 25 de janeiro de 2012, o Parlamento e a Comissão Europeia apresentaram uma Proposta de Regulamento relativo à proteção das pessoas singulares quanto ao tratamento de dados pessoais e à livre circulação dos mesmos, no âmbito da competência que lhes é atribuída no artigo 16.º, n.º 2, do TFUE.

Em 27 de abril de 2016, foi aprovado o Regulamento Geral sobre Proteção de Dados[25], que visou atualizar, reforçar e uniformizar a proteção conferida ao direito à proteção de dados, assim como incentivar a consolidação do Mercado Interno da União, em face das novas realidades empresariais e tecnológicas, estabelecendo um conjunto de normas e princípios gerais para a proteção de dados e para o tratamento transfronteiriço dos mesmos.

25 Regulamento n.º 2016/679/UE, que entrará em vigor em 25 de maio de 2018, nos termos do artigo 99.º, n.º 2, do Regulamento, e que revoga a Diretiva 95/46/CE. Foram também aprovadas a Diretiva n.º 2016/680/UE (relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados) e a Diretiva n.º 2016/681/UE (relativa à utilização dos dados dos registos de identificação dos passageiros [PNR] para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave) que, pela economia do presente escrito e pelas razões *supra* aduzidas, não serão consideradas na análise do direito fundamental à proteção de dados pessoais.

Quanto às alterações e inovações que constam do Regulamento, cabe sinalizar e analisar as soluções que assumem um maior relevo na realização do escopo do direito à proteção de dados, que são as que de seguida se apresentam[26]:

i) *autonomia do direito fundamental à proteção de dados* (artigo 1.º, n.º 2, do Regulamento): abandonou-se a solução prevista no artigo 1.º, n.º 1, da Diretiva 95/46/CE, que considerava o direito à proteção de dados pessoais como uma manifestação do direito à reserva da intimidade da vida privada, na senda do que o artigo 8.º da CDFUE preconiza. Trata-se, no confronto com a posição anteriormente assumida, de uma solução dogmaticamente mais ajustada a uma efetiva realização do escopo de proteção do direito, no sentido de reconhecer a titularidade de um poder de controlo do titular dos dados sobre as suas próprias informações, independentemente do maior ou menor grau de proximidade à esfera íntima que a natureza e o conteúdo das concretas informações possa revestir;

ii) *pseudoanonimização do tratamento de dados* (artigo 4.º, n.º 5, do Regulamento[27]): o diploma envereda por um tratamento desenvolvido da pseudoanonimização enquanto garantia essencial da efetividade do direito à proteção de dados, quer nos casos de tratamento que não tenham exigido identificação do titular dos dados (artigo 11.º do Regulamento), quer na fixação das condições de segurança do tratamento dos dados aplicáveis à generalidade dos procedimentos [artigo 32.º, n.º 1, al. *a*)], quer na aprovação de códigos de conduta pelas associações e outros organismos representantes de categorias de responsáveis pelo tratamento de dados que prevejam a pseudoanonimização [artigo 40.º, n.º 2, al. *d*), do Regulamento];

26 Pronunciando-se sobre algumas das soluções da Proposta do Regulamento que transitaram para o diploma final, ou sobre o Regulamento em si mesmo, cfr. Lopes, Joaquim de Seabra, 2016, «O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível», in *Fórum de Proteção de Dados*, n.º 2, pp. 15 e ss., Calvão, Filipa Urbano, 2015, «Modelo de supervisão e tratamento de dados pessoais na União Europeia: da atual Diretiva ao futuro Regulamento», in *Fórum de Proteção de Dados*, Lisboa, n.º 1, pp. 34 e ss., Teixeira, Maria Leonor da Silva, 2013, «A União Europeia e a protecção de dados pessoais: "Uma visão futurista"?», in *Revista do Ministério Público*, n.º 135, pp. 91 e ss., Ramalho, David Silva, 2016, *O novo Regulamento Geral sobre a Proteção de Dados e o Data Protection Officer*, disponível em http://www.servulo.com/xms/files/00_SITE_NOVO/01_CONHECIMENTO/01_PUBLICACOES_SERVULO/2016/Updates/Update_PI__PD_e_TI_DSR_O_Novo_Regulamento_Geral_sobre_a_Protecao_de_Dados.pdf.

27 Que define a «pseudonimização» como «o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável».

iii) *consagração dos princípios da transparência e da proporcionalidade*[28] ou da «*minimização dos danos*» [artigo 5.º, n.º 1, alíneas *a*) e *c*), do Regulamento]: visou-se, deste modo, garantir que a informação disponibilizada ao titular dos dados é clara, acessível, simples e percetível, pugnando-se por uma recolha e tratamento de dados subordinado a um elemento funcional, ou seja, que os dados sejam adequados e limitados ao que é necessário para as finalidades a que se destinam. A sua consagração assume uma importante função pedagógica, uma vez que, enquanto princípio geral de Direito, o princípio da proporcionalidade já tinha imediata aplicabilidade no campo da proteção de dados, enquanto parâmetro de controlo das concretas atuações administrativas das entidades públicas ou privadas no exercício de poderes públicos, bem como no domínio das relações entre cidadãos e entidades privadas enquanto tais (sem se encontrarem no exercício de funções públicas);

iv) *tutela dos direitos dos menores* (artigo 8.º do Regulamento): pese embora a opção por sujeitar o consentimento fornecido por menores a alguns condicionalismos seja louvável (*maxime*, ao consentimento do progenitor ou do titular da guarda com responsabilidades parentais), dada a «validade reduzida» do consentimento obtido de certos menores, sobretudo de baixa faixa etária, atento o nível de desenvolvimento psicológico e cognitivo para formar um consentimento esclarecido – que demonstre a plena consciência dos dados que se estão a disponibilizar, das suas implicações e consequências e do regime aplicável –, trata-se de um aspeto de regime criticável, na medida em que se deixa aos Estados-membros dispor, no seu Direito nacional, sobre qual a idade a partir da qual se sujeita o consentimento dos menores aos condicionalismos previstos, desde que essa idade não seja inferior a 13 anos. Se o propósito era de uniformização e tutela efetiva do direito, trata-se de um ponto de regime dissonante do espírito da revisão;

v) *proibição geral de tratamento de certas categorias de dados* (artigo 9.º do Regulamento): concretizando o princípio da não discriminação, o Regulamento prevê uma proibição de tratamento de certas categorias de dados que

28 Defendendo que o princípio da proporcionalidade é um princípio geral do Direito, Muller, Jorg Paul, 1983, *Éléments pour une théorie suisse des droits fondamentaux*, Berne. Atualmente, tem-se vindo a defender a superação da trilogia clássica alemã em que, tradicionalmente, é decomposto o princípio da proporcionalidade (adequação, necessidade e proporcionalidade em sentido restrito) devido às exigências acrescidas de controlo das leis e intervenções restritivas de direitos fundamentais, na sociedade atual, e às dificuldades de aplicação do «teste» da necessidade, Silva, Suzana Tavares da, 2012, «O *tetralemma* do controlo judicial da proporcionalidade no contexto da universalização do princípio: adequação, necessidade, ponderação e razoabilidade», *Boletim da Faculdade de Direito Coimbra*, n.º 2, pp. 668 e 678 (para uma visão sintética da controvérsia no direito comparado); Canotilho, Gomes, 2002, *Direito Constitucional e Teoria da Constituição*, Almedina, p. 272; Andrade, Vieira de, 2012, *Os direitos fundamentais na Constituição a República Portuguesa de 76*, Almedina, pp. 288 e ss.; e Novais, Jorge Reis, 2004, *Os Princípios Constitucionais Estruturantes da República Portuguesa*, Coimbra Editora, pp. 162 ss.

revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa;

vi) *direito ao esquecimento* (artigo 17.º do Regulamento): enquanto manifestação do direito à autodeterminação informativa, reconhece-se ao titular dos dados o direito a solicitar a eliminação dos seus dados pessoais, na senda da jurisprudência anterior do TJUE[29], visto que a perpetuação da acessibilidade a determinados dados pessoais tem um potencial lesivo enorme dos direitos, liberdades e garantias dos cidadãos, não só ao nível da privacidade, honra e bom nome, livre desenvolvimento da personalidade e autodeterminação, mas também da sua própria dignidade[30];

vii) *direito à portabilidade dos dados* (artigo 20.º do Regulamento): confere-se ao titular dos dados o direito de receber os dados que lhe digam respeito e que tenha fornecido a um responsável pelo seu tratamento, assim como o direito a que o responsável em causa os transmita a um diferente responsável pelo tratamento de dados, sem que o responsável pelo tratamento originário se possa opor, de forma a que lhe seja possível conhecer o exato conteúdo das informações que prestou e, em última análise, poder dispor das mesmas;

viii) *direito de oposição* (artigo 21.º do Regulamento): permite-se ao titular dos dados a faculdade de se opor ao tratamento de dados pessoais que lhe diga respeito, incluindo a definição de perfis, salvo se o responsável pelo tratamento apresentar «razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados». Ora, a opção do legislador europeu em causa afigura-se criticável porque configura uma «cláusula em branco», que faz apelo a conceitos indeterminados e fluidos,

---

29 Cfr. Àlvarez Rigaudias, Cecilia, 2014, «Sentencia Google Spain y derecho al olvido», in *Actualidad Jurídica Úria Menendez*, pp. 110 e ss., em ação interposta pela Agência Espanhola para a Proteção de Dados contra a Google, o TJUE, em sentença de 13 de maio de 2014 (acórdão Costeja), «*viene a reconocer el "derecho al olvido" en Internet, atribuyendo a los motores de búsqueda la responsabilidad de ponderar los intereses en juego en cada caso (y sin que se eliminen necesariamente los resultados en la web de origen), incluso si están sitos fuera de la Unión Europea, como es el caso de Google Inc*.».

Sobre o tema, veja-se Simón Castellano, Pere, 2013, «El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos», in *Libertad de expresión e información en Internet: amenazas y protección de los derechos personales*, Madrid: Centro de Estudios Políticos y Constitucionales. pp. 451 e ss., Álvarez Caro, María, 2014, «Reflexiones sobre la sentencia del TJUE en el asunto "Mario Costeja" (C-131/12) sobre derecho al olvido», in *Revista Española de Derecho Europeo*, n.º 51, pp. 165 e ss., Soriano García, Jose Eugenio, 2012, «Derecho al olvido y la creación de derechos», in *Revista de Economia e Direito*, Lisboa, vol. 17, n.º 1, pp. 207 e ss., e Lindsay, David, 2014, «The "right to be forgotten" in European data protection law», in *Emerging challenges in privacy law: comparative perspectives*, Cambridge University Press, pp. 290 e ss.

30 Neste sentido, Teixeira, Maria Leonor da Silva, 2013, «A União Europeia e a protecção de dados pessoais: "Uma visão futurista"?», in *Revista do Ministério Público*, n.º 135, p. 95.

não determinando nem a sua significância, nem elencando um conjunto de índices a partir dos quais o intérprete/aplicador poderá densificar o conceito de «razões imperiosas e legítimas prevalecentes». Assim sendo, cabe esperar pela jurisprudência do TJUE para clarificar esta matéria, embora se advogue, com razão, que este preceito pode dar azo, na prática, a um esvaziamento de conteúdo do direito de oposição ao tratamento de dados do titular, com severas implicações no escopo do direito à proteção de dados;

ix) *direito à não sujeição do titular dos dados a nenhuma decisão tomada exclusivamente com base no tratamento automatizado de dados*, incluindo a definição de perfis (artigo 22.º do Regulamento), salvo as restrições previstas no n.º 2 [que inclui, na alínea *c*), o consentimento do próprio titular, no âmbito da temática da disponibilidade e da renúncia a direitos fundamentais do titular]. Trata-se de um preceito de relevo em face da preferência crescente pela utilização de meios informáticos no âmbito do procedimento administrativo e restantes formas de atuação das Administrações dos Estados-membros (no ordenamento jurídico nacional, relevam os artigos 61.º a 64.º do CPA, estabelecendo-se que a preferência pela instrução dos procedimentos através da utilização de meios eletrónicos visa facilitar o exercício de direitos e o cumprimento de deveres, agilizar os procedimentos e garantir a sua maior economia e eficiência) com implicações na possibilidade de emissão de atos administrativos «eletrónicos» (decisões individuais e concretas automatizadas, sem intervenção humana, mediante o preenchimento de formulários informáticos que fixem os pressupostos sobre os quais assentará o dever de decisão do caso concreto, sobretudo nos casos de atos administrativos vinculados);

x) enfoque na *compliance* no âmbito do *regime do responsável pelo tratamento de dados* (artigos 4.º, parágrafo 7[31], 24.º e 26.º-31.º do Regulamento): o legislador europeu coloca a ênfase dos deveres de fiscalização e de verificação prévia do cumprimento das regras relativas a proteção de dados sobre o «responsável pelo tratamento de dados», desonerando as entidades administrativas independentes de uma acumulação excessiva de funções de fiscalização que gera ineficiências claras, num fenómeno de *privatização dos deveres estaduais de proteção*[32] que se tem vindo a verificar no domínio do Direito Administrativo. Nesta senda, o responsável pelo tratamento dos dados é incumbido de

31 Que dispõe que se considera como 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; 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».

32 Silva, Jorge Pereira da, 2015, *Deveres do Estado de Protecção de Direitos Fundamentais*, Universidade Católica Editora, pp. 729 e ss.

diversas tarefas, nomeadamente, a de fiscalizar a (in)observância dos princípios gerais sobre proteção de dados (artigo 5.º, n.º 2, do Regulamento); de verificar se o tratamento de dados recolhidos sem o consentimento do titular, ou com título habilitante em norma de Direito da União Europeia ou de Direito dos Estados-membros que cumpra com os ditames da proporcionalidade, é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos (artigo 6.º, n.º 4, do Regulamento); de poder demonstrar o consentimento do titular dos dados (artigo 7.º, n.º 1, do Regulamento); de disponibilizar informações ao titular, ao nível da finalidade do tratamento, período de conservação, possibilidade de retificação ou apagamento e direito de apresentar queixa (artigos 12.º-15.º, 18.º e 19.º do Regulamento); e, ainda, de implementar mecanismos eficazes de *compliance*, sob pena da aplicação de multas administrativas até 20 000 000,00 € ou, tratando-se de uma empresa, até 4% do seu volume de negócios anual a nível mundial[33];

xi) privacy by design e privacy by default (artigo 25.º do Regulamento): o legislador europeu, no sentido de reforçar a prossecução efetiva do escopo de proteção do direito à proteção de dados, considerou que devem ser aplicadas um conjunto de medidas técnicas e organizativas que permitam a tomada em devida linha de conta de aspetos relacionados com a proteção de dados, aquando da criação e desenvolvimento de cada novo serviço ou produto, por parte das entidades que possam deter dados pessoais de terceiros. Por outro lado, impõe-se que quando o serviço ou produto seja comercializado, deva sê-lo com a parametrização das definições automáticas no sentido de garantirem o maior nível de privacidade possível do próprio consumidor;

xii) *medidas de segurança no tratamento dos dados* (artigo 32.º do Regulamento): prevê-se, neste âmbito, um conjunto de medidas técnicas adequadas para assegurar um nível de segurança consoante o risco envolvido, seja pela natureza sensível das informações seja pela possibilidade de se lesar não apenas o titular dos dados, mas também de terceiros, entre as quais medidas que assegurem a confidencialidade, a cifragem e a disponibilidade dos dados, assim como a implementação de um processo que teste a eficácia das medidas;

33 Para uma análise crítica do regime sancionatório, Moutinho, José Lobo, / Ramalho, David Silva, 2015, *Notas sobre o regime sancionatório da Proposta de Regulamento Geral sobre a Protecção de Dados do Parlamento Europeu e do Conselho*, *in* Fórum de Proteção de Dados, Lisboa, n.º 1, pp. 25 e ss., considerando que o legislador europeu foi «demasiado ambicioso» e que a «tutela sancionatória carece de ser cuidadamente (re)pensada e (re)definida, tendo em atenção a natureza das infrações em causa. Com efeito, a tutela dos bens jurídicos subjacentes à proteção de dados não se cria pela imposição externa de sanções desproporcionais ao agente da infração, num pensamento, afinal, de uma prevenção geral entendida de forma bastante primária, devendo ser antes o fruto de um labor de sensibilização que faça brotar da consciência jurídica comum a compreensão dos referidos valores e a importância do seu respeito para a tutela da pessoa humana no que é a realidade da vida social e comunicacional dos nossos dias, unindo, assim, a comunidade em torno da sua preservação».

xiii) *avaliação de impacto sobre proteção de dados e consulta prévia* (artigos 35.º e 36.º do Regulamento): em casos de tratamentos de dados que impliquem a utilização de novas tecnologias ou que sejam suscetíveis de implicar um elevado risco para os direitos, liberdades e garantias dos titulares de dados, prevê-se a realização de uma avaliação de impacto e uma consulta prévia, enquanto garantias procedimentais das valorações materiais – de proteção dos dados e informações dos visados – que lhes subjazem;

xiv) *encarregado de proteção de dados* (artigos 37.º a 39.º do Regulamento): embora a previsão da figura não seja uma verdadeira inovação (visto que já se encontrava prevista genericamente e a título facultativo, nos artigos 18.º, n.º 2, e 20.º, n.º 2, da Diretiva 95/46/CE), a sua consagração a título obrigatório é uma medida significativa na realização do escopo do direito à proteção de dados.

Considerando que a futura entrada em vigor do Regulamento Geral sobre a Proteção de Dados, em 25 de maio de 2018, terá como consequência a revogação da Diretiva *ePrivacy*, nos termos do artigo 94.º do Regulamento, a Comissão Europeia publicou, em 10 de janeiro de 2017, a nova proposta de Regulamento relativo à proteção da privacidade e ao tratamento de dados pessoais no sector das comunicações eletrónicas, visando reforçar a segurança no mercado único digital[34].

A revisão do bloco de legalidade em matéria de proteção de dados, levada a cabo pelo legislador europeu, exigirá, para além da imediata compatibilização da legislação interna com as novas soluções consagradas no Regulamento, um esforço de adequação das estruturas institucionais e empresariais públicas e privadas com as novas diretrizes e, bem assim, o desempenhar de um papel mais ativo por parte da CNPD, no caso português, e das restantes entidades administrativas independentes, nos restantes Estados-membros, na fiscalização do cumprimento do bloco de regras e princípios aprovado[35].

No entanto, em face do carácter genérico ou programático que o novo Regulamento assume na regulação de determinadas matérias, também se considera necessária uma atividade de densificação e concretização, por via regulamentar ou através de comunicações interpretativas, das soluções constantes de diversos preceitos do Regulamento, em função das particularidades concretas de cada Estado-membro, nomeadamente ao nível da estrutura e funcionamento da Administração Pública.

34 Disponível em https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-andelectron ic-communications.

35 Aliás, seria, de todo em todo, benéfica a promoção de um conjunto de ações de sensibilização dos cidadãos para o acervo de direitos que lhes é, de forma inovatória, reconhecido no Regulamento.

Ora, pelo exposto, impõe-se concluir que, ao fixar uma regulamentação mais densa e uniforme no espaço europeu (*rectius*, mais exigente), o escopo do direito à proteção de dados sai, inequivocamente, reforçado com a aprovação e implementação do novo bloco de legalidade.

4. O encarregado de proteção de dados *(Data Protection Officer)* e a privatização dos deveres estaduais de proteção

De entre as diversas inovações introduzidas pelo Regulamento no domínio da proteção de dados, a imposição, a título obrigatório, da nomeação de um encarregado de proteção de dados (DPO) merece especial destaque.

Com efeito, no artigo 37.º, n.º 1, do Regulamento, prevê-se a obrigação de designar um encarregado de proteção de dados nos seguintes casos:

i) Quando o tratamento seja efetuado por uma autoridade ou um organismo público[36], com exceção dos tribunais;

ii) Quando as atividades principais do responsável pelo tratamento de dados ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala;

iii) Quando as atividades principais do responsável pelo tratamento de dados ou do subcontratante consistam em operações de tratamento, em grande escala, de categorias especiais de dados ou de dados relacionados com condenações e infrações penais.

Sobre o estatuto da pessoa concreta que pode ser nomeada como encarregado de proteção de dados, e sobre a sua posição jurídica no respetivo seio empresarial público ou privado, é possível enfatizar os seguintes elementos:

a) Trata-se de um trabalhador ou prestador de serviços, contratado pela entidade responsável pelo tratamento de dados ou pelo subcontratante, selecionado com base nas suas *qualidades profissionais* e *conhecimentos especializados* no domínio da proteção de dados, nos termos do artigo 37.º, n.os 5 e 6;

b) Estabelece-se um conjunto de *deveres de informação e de cooperação* dos responsáveis pelo tratamento de dados perante o encarregado de proteção de dados, facultando-lhe as informações e os meios necessários ao regular e

36 Permite-se, inclusivamente, nos termos do n.º 3 do artigo 37.º, que, dependendo da respetiva estrutura empresarial em termos de organização e dimensão, seja possível nomear um único encarregado de proteção de dados para várias entidades, em nome dos princípios da eficácia, eficiência e boa administração.

eficiente desempenho das suas funções[37], tal como se dispõe nos n.os 1 e 2 do artigo 38.º;

c) Garante-se um *estatuto de independência*, que permite ao encarregado de proteção de dados não estar vinculado às instruções do responsável do tratamento dos dados quanto ao exercício das suas funções, não podendo ser penalizado pela inobservância das mesmas; diga-se, aliás, que à luz do Direito Administrativo nacional, estabelece-se um verdadeiro *dever de desobediência* perante quaisquer ordens ou instruções provenientes do responsável pelo tratamento, que se afigurariam como atos nulos;

d) Consagram-se *deveres de sigilo e confidencialidade*, no que tange à natureza e conteúdo dos dados pessoais dos seus titulares, nos termos do artigo 38.º, n.º 5.

A obrigatoriedade de nomeação de um encarregado de proteção de dados, nos casos já referidos, exigirá uma adaptação por parte das entidades e empresas, quer sejam de natureza pública ou privada, ao nível da sua estrutura organizativa no sentido de promover a integração do encarregado de proteção de dados de acordo com os ditames do Regulamento, de modo a que possa exercer eficazmente as suas funções de garantia do direito fundamental à proteção de dados dos cidadãos.

Pese embora o exposto, deve notar-se que o Regulamento contém um regime genérico e lacunar em diversos aspetos quanto à figura do encarregado de proteção de dados, o que pode constituir fonte de insegurança e incerteza jurídica sobre os titulares de dados quanto à segurança e efetividade da proteção do seu direito, tal como nos próprios operadores económicos ao nível da adaptação das suas estruturas organizativas. O mesmo se pode afirmar relativamente ao âmbito das funções do encarregado de proteção de dados e às condicionantes e restrições existentes na dinâmica de relacionamento a

37 O artigo 39.º do Regulamento prevê, a título de mínimo (em conformidade com o que se dispõe no n.º 6 do artigo 38.º e do n.º 1 do artigo 39.º), que o âmbito das funções que estão adstritas ao encarregado da proteção de dados são: «*a*) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-membros; *b*) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes; *c*) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.º; *d*) Coopera com a autoridade de controlo; *e*) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.» No fundo, trata-se de avaliar e promover a implementação de mecanismos de cumprimento da legislação sobre proteção de dados e de prestar aconselhamento ao responsável pelo tratamento de dados, assim como de cooperar com a CNPD.

estabelecer entre o encarregado de proteção e a empresa ou entidade, com o intuito de se cumprir integralmente as obrigações legais a que se encontram adstritos.

Em princípio, dependendo da natureza pública ou privada da entidade na qual exercerá as suas funções, ao encarregado de proteção de dados será aplicado, subsidiária e respetivamente, a Lei Geral do Trabalho em Funções Públicas (Lei n.º 35/2014, de 20 de junho) ou o Código do Trabalho (Lei n.º 7/2009, de 12 de fevereiro), com as devidas adaptações.

Em face do quadro enunciado, afigura-se previsível e necessário que as entidades administrativas independentes dos Estados-membros incumbidas de regular o sector da proteção de dados, como é o caso da CNPD, venham a emitir um conjunto de regulamentos, orientações ou comunicações interpretativas que concretizem as normas que se extraem dos artigos 37.º a 39.º do Regulamento, de forma não só a colmatar as lacunas subsistentes como a adaptar o normativo às especificidades da realidade nacional.

Ora, atenta a necessidade de se empreender a tarefa de densificação do regime aplicável ao encarregado de proteção de dados, é possível identificar, desde já, dois aspetos que certamente serão alvo de debate e controvérsia aquando da futura conformação do bloco de legalidade ao novo Regulamento e, bem assim, da aplicação prática do mesmo:

i) Deve o acesso ao cargo de encarregado de proteção de dados ser restringido/limitado a pessoas que tenham conhecimentos jurídicos obtidos por via académica (*v.g.*, uma licenciatura em Direito ou uma pós-graduação/especialização em certa área jurídica)?

De facto, o Regulamento não prevê que categorias profissionais ou que condições académicas permitem o acesso ao cargo, apenas afirmando a necessidade de o profissional reunir as qualidades profissionais e conhecimentos técnicos especializados sobre a área enquanto requisitos.

Ora, se é verdade que a natureza das funções desempenhadas pelo DPO, sobretudo na vertente de garantia do direito à proteção de dados dos titulares e da responsabilidade pelo cumprimento das suas obrigações estatutárias, pode conduzir a uma ideia de maior «habilitação legal e técnica» no acesso ao cargo por profissionais ligados ao Direito, certo é que tal restrição representaria uma violação do princípio da igualdade, sem justificação bastante, nos termos do artigo 13.º da CRP, visto que não é demonstrável que apenas os profissionais com habilitações académicas na área do Direito possam desempenhar eficazmente as funções cometidas ao encarregado de proteção de dados.

Se pensarmos em certos conjuntos de categorias profissionais, *v.g.*, ligadas à engenharia informática, que possuem conhecimentos técnicos sobre o funcionamento dos sistemas de recolha, tratamento e utilização de dados, a situação

de desconformidade com o princípio da igualdade torna-se evidente, à qual, neste caso, necessariamente acresce que se trataria de uma restrição abusiva da liberdade de escolha de profissão e de acesso à função pública, nos termos do artigo 47.º da CRP, e da livre iniciativa económico-empresarial, tal como se dispõe no artigo 61.º da CRP.

ii) Pode a CNPD criar um processo de certificação direta de DPO – dada a assumida falta de especialistas no mercado nesta área e, por outro lado, o elevado número de entidades públicas e privadas que se encontram abrangidas pela obrigação de nomear um DPO – que se assuma como uma condição de legitimidade e de acesso ao exercício do cargo?

Mais uma vez, trata-se de uma questão discutível, sobretudo à luz do princípio da concorrência e do princípio da livre iniciativa económico-empresarial, na vertente de liberdade de organização e gestão da empresa enquanto direito institucional da empresa em si mesma.

No entanto, diga-se que também não é desejável que se entregue às entidades públicas e privadas discricionariedade total sobre a nomeação do seu encarregado de proteção de dados, considerando a exigência que consta do Regulamento de garantir as «qualidades profissionais» e os «conhecimentos especializados» do DPO, nos termos do n.º 5 do artigo 37.º do Regulamento.

Uma solução possível, de compromisso entre as diversas vertentes e valorações em ponderação, passaria pela implementação de um sistema de certificação indireta ou em escada, no qual a CNPD certificasse certas entidades que reunissem os requisitos necessários para tal (*v.g.*, caso de certas universidades ou de certos institutos públicos), como estando habilitadas a desenvolver, por sua vez, processos de habilitação e certificação legal dos candidatos, para que estes venham a exercer, futuramente, o cargo de encarregado de proteção de dados, afastando-se, desta forma, o obstáculo que uma intervenção direta da CNPD na livre iniciativa privada neste âmbito pode gerar.

Apesar de toda a incerteza que rodeia a figura do DPO, um elemento do regime revela-se bastante nítido: em face do disposto no n.º 4 do artigo 38.º [38], o encarregado de proteção de dados assume uma função de garantia não apenas da legalidade objetiva relativa à proteção de dados (cumprimento do conjunto de regras e princípios que formam o bloco de legalidade em causa, de um ponto de vista de ordem pública e valores de segurança e justiça), mas também de garantia da legalidade subjetiva, ou seja, de fiscalizar que a entidade detentora dos dados pessoais não viola o direito fundamental à proteção de dados do seu titular.

38 Que dispõe que «Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente regulamento».

Por conseguinte, tal como também se constata quando o Regulamento prevê certas obrigações para o responsável pelo tratamento de dados ou para o subcontratante[39], é possível verificar que a previsão da obrigatoriedade de nomeação de um encarregado de proteção de dados, com as funções que lhe são cometidas, é uma manifestação do fenómeno de *privatização de deveres estaduais de proteção*[40] que se tem vindo a verificar no Direito Administrativo, conferindo-se a particulares (no caso de se tratarem de estruturas empresarias de natureza privada que lidem com quantidades maciças de dados ou dados sensíveis) tarefas de fiscalização e verificação do cumprimento integral da legalidade que, *a priori*, estariam a cargo de entidades públicas, no âmbito da função administrativa do Estado – fenómeno ao qual certamente não serão alheias as considerações sobre o momento atual de crise de recursos financeiros que, inevitavelmente, influencia a capacidade do agir público[41].

A propósito da privatização dos serviços de correios e de telecomunicações que se verificou em Portugal, também se afirmou que da privatização dos deveres de proteção do Estado inerentes às áreas em causa (nomeadamente no que respeita ao sigilo da correspondência) não pode resultar qualquer diminuição de garantia dos bens jusfundamentais em causa, mantendo-se, pelo menos, o mesmo nível de proteção em face do que anteriormente existia.

Afirmou-se, nessa sede, que a «manutenção do *standard* de proteção do direito ao sigilo de correspondência continua a ser um dever do Estado, exigirá que os poderes públicos, através de normas adequadas (desde normas legislativas, até normas técnicas elaboradas por entidades ou autoridades independentes ou comissões técnicas), tem o dever de manter um nível de proteção elevado do segredo de correspondência», consagrando-se uma «responsabilidade estadual pelos resultados da privatização»[42].

---

39 Analisadas *supra*.

40 Cfr. Silva, Jorge Pereira da, 2015, *Deveres do Estado de Protecção de Direitos Fundamentais*, Universidade Católica Editora, p. 731, afirma que «os particulares são chamados a desempenhar funções de proteção de direitos fundamentais inseridos no âmbito de estruturas relacionais tetrapolares (ou multipolares), em que à relação triangular original se vem juntar um outro sujeito privado que – a par do Estado ou em sua substituição – é encarregado de zelar pela proteção dos bens jurídicos do titular sob ameaça».

41 Sobre o modo como a falta de recursos, associada à atual crise económico-financeira, influi sobre o agir da Administração e sobre a normatividade concreta à qual se lhe deve exigir o cumprimento, Ventas, Rosa María, Hernández, Ignacio [*et al.*], 2012, *La Administración en tiempo de crisis: presupuestación, cumplimiento de obligaciones y responsabilidades*, Thomson Reuters, Aranzadi, pp. 1071 e ss., para uma visão da problemática no Direito Espanhol.

42 Cfr. Canotilho, Gomes, 2008, *Estudos sobre Direitos Fundamentais*, Coimbra Editora, p. 164. Sendo certo que o autor parte da realidade existente no sector específico das telecomunicações e dos correios, na qual se verificou uma privatização não apenas dos deveres, mas também das próprias estruturas empresariais, é de considerar que o entendimento exposto pelo autor também revela a sua utilidade, *mutatis mutandis*, na compreensão dos casos de mera privatização dos deveres estaduais de proteção,

De resto, resulta do dispositivo constitucional, previsto no artigo 18.º, n.º 1, da Constituição, a vinculação imediata das entidades privadas ao cumprimento das dimensões garantísticas do direito fundamental à proteção de dados, enquanto posição jurídica subjetiva compreensiva, que se desdobra num conjunto de corolários relevantes na garantia da efetividade da proteção do direito.

Portanto, o DPO, ao desempenhar funções que tutelam, de um modo imediato – não só no contacto direto com os titulares de dados, mas também no contacto que, por via das obrigações de informação e cooperação, terá com a CNPD –, o direito fundamental à proteção de dados pessoais dos cidadãos, assumir-se-á como um funcionário público no exercício de poderes públicos e, mesmo nos casos de encarregados de proteção de dados que não sejam funcionários públicos (porque integrados em estruturas empresariais privadas) como um privado no exercício de funções públicas ou jurídico-administrativas[43], que, como tal, poderá vir a ser responsabilizado, em ambos os casos, nos termos dos artigos 1.º, n.º 5, e 7.º e ss. da Lei n.º 67/2007, de 31 de dezembro, ou Regime da Responsabilidade Civil Extracontratual do Estado.

5. Conclusão

A problemática da proteção de dados pessoais é uma questão incontornável da sociedade de risco tecnológico atual, ao introduzir novos perigos aos direitos, liberdades e garantias dos cidadãos que devem ser devidamente enquadrados e acautelados.

O reconhecimento de um recorte dogmático próprio ao direito à proteção de dados constitui um primeiro passo no reforço da efetividade do escopo do direito, aliado à elaboração de regimes legais que tutelem a posição do titular dos dados de forma adequada em face dos constantes avanços tecnológicos registados.

Neste sentido, sentiu-se a necessidade de rever o quadro normativo da UE ao nível da proteção de dados, aprovando-se o novo Regulamento Geral sobre Proteção de Dados que, certamente, irá desempenhar um papel essencial no seio do bloco de legalidade de proteção de dados dos diferentes Estados-membros.

---

assentes na entrega a entidades privadas de deveres de fiscalização e de verificação do cumprimento do bloco de legalidade (sobretudo, de funções de fiscalização prévia ou *ex ante*) que, originariamente, pertenciam à competência de entidades públicas.

43 Cfr. Otero, Paulo, 2001, «Coordenadas jurídicas da privatização da Administração Pública», in *Os caminhos da privatização da Administração Pública*, Coimbra, pp. 37 e ss.

Por fim, e ainda que se possa argumentar que o «tempo do direito» nunca conseguirá alcançar, de forma plena, o «tempo da tecnologia» neste campo (dada a maior morosidade e ponderação que é, em princípio, exigida a um processo legislativo do que a um processo de criação, desenvolvimento e comercialização de uma nova tecnologia ou de novas funcionalidade da mesma tecnologia), reservando-se *ad aeternum* um papel essencialmente reativo perante os avanços tecnológicos e os perigos ou lesões efetivas entretanto verificadas, sempre será possível afirmar que, para o exercício efetivo do direito fundamental à proteção de dados, o particular tem de se afirmar como o «pleno proprietário» dos seus próprios dados, sobretudo numa época em que «A "morte da privacidade" deve, assim, ser reinventada para reclamar antes a transparência dos procedimentos de restrição de direitos»[44].

6. Bibliografia

Alexandrino, José Melo, 2014, «Jurisprudência da Crise. Das questões Prévias às Perplexidades», *O Tribunal Constitucional e a Crise – Ensaios Críticos*, p. 67.

Álvarez Caro, María, 2014, «Reflexiones sobre la sentencia del TJUE en el asunto "Mario Costeja" (C-131/12) sobre derecho al olvido», *Revista Española de Derecho Europeo*, n.º 51, pp.165 e ss.

Andrade, Vieira de, 2012, *Os direitos fundamentais na Constituição a República Portuguesa de 76,* Almedina, pp. 288 e ss.

Ascenção, Oliveira, 2005, *O Direito – Introdução e Teoria Geral*, Almedina, p. 215.

Brito, Miguel Nogueira de, 2015, *O admirável novo constitucionalismo da Sociedade de Risco*, *In Memoriam Ulrich Beck*, Atas do colóquio promovido pelo ICJP e pelo CIDP, disponível em https://www.icjp.pt/sites/default/files/publicacoes/files/ebook_ulrichbeck_0.pdf, pp. 54 e ss.

Calvão, Filipa Urbano, 2015, *Modelo de supervisão e tratamento de dados pessoais na União Europeia: da atual Diretiva ao futuro Regulamento*, in Fórum de Proteção de Dados, Lisboa, n.º 1, pp. 34 e ss.

Canaris, Claus-Wilhem, 1989, *Pensamento sistemático e conceito de sistema na Ciência do Direito*, Lisboa, pp. 9 e ss.

Canotilho, Gomes, 2002, *Direito Constitucional e Teoria da Constituição*, Almedina, p. 272.

Canotilho, Gomes / Moreira, Vital, 2007, *Constituição da República Portuguesa Anotada*, vol. I, Coimbra Editora, pp. 551 e ss.

44 Cfr. Neto, Luísa, 2011, «Acórdãos do TC n.os 213/2008 e 486/2009: a prova numa sociedade transparente», in *Revista da Faculdade de Direito da Universidade do Porto*, p. 343.

Egídio, Mariana Melo, 2010, «Análise da estrutura das normas atributivas de direitos fundamentais. A ponderação e a tese ampla da previsão», in *Estudos em Homenagem ao Prof. Doutor Sérvulo Correia*, vol. I, Faculdade de Direito da Universidade de Lisboa, pp. 626 e ss.

Ferreira, Pedro, 2006, *A protecção de dados pessoais na sociedade de comunicação – Dados de Tráfego, Dados de Localização e Testemunhos de Conexão*, O Espírito das Leis, pp. 144 e ss.

Goold, Imogen, 2015, «A, B and C v Ireland [2010]», in *Landmark Cases in Medical Law*, Hart Publishing, pp. 335 e ss.

Graham, Stephen, 1998, *Spaces of surveillant simulation: New Technologies, digital representations and material geographies*, Environment and Planning D: Society and Space, pp. 483 e ss.

Lindsay, David, 2014, «The "right to be forgotten" in European data protection law», in *Emerging challenges in privacy law: comparative perspectives*, Cambridge University Press, pp. 290 e ss.

Lopes, Joaquim de Seabra, 2016, *O artigo 35.º da Constituição: da génese à atualidade e ao futuro previsível*, in Fórum de Proteção de Dados, n.º 2, pp. 15 e ss.

Luhmann, 1999, *Funktionem und Folgen formaler Organisation*, Berlim, pp. 304 e 305.

María Ventas, Rosa / Hernàndez, Ignacio [*et al.*], 2012, *La Administración en tiempo de crisis: presupuestación, cumplimiento de obligaciones y responsabilidades*, Thomson Reuters, Aranzadi, pp. 1071 e ss.

Miranda, Jorge / Medeiros, Rui, 2010, *Constituição Portuguesa Anotada*, tomo I, Coimbra Editora.

Moniz, Helena, 2002, «Os problemas jurídico-penais da criação de uma base de dados genéticos para fins criminais», in *Revista Portuguesa de Ciência Criminal*, n.º 2, pp. 246 e ss.

Moutinho, José Lobo / Ramalho, David Silva, 2015, *Notas sobre o regime sancionatório da Proposta de Regulamento Geral sobre a Protecção de Dados do Parlamento Europeu e do Conselho*, *in* Fórum de Proteção de Dados, Lisboa, n.º 1, pp. 25 e ss.

Muller, Jorg Paul, 1983, *Éléments pour une théorie suisse des droits fondamentaux*, Berne.

Neto, Luísa, 2011, «Acórdãos do TC n.os 213/2008 e 486/2009: a prova numa sociedade transparente», in *Revista da Faculdade de Direito da Universidade do Porto*, p. 343.

Nicolau, Tatiana Duarte, 2015, *O armazenamento de amostras de ADN e as bases de dados de perfis genéticos*, Comissão Nacional de Proteção de Dados, pp. 32 e 33.

Novais, Jorge Reis, 2004, *Os Princípios Constitucionais Estruturantes da República Portuguesa*, Coimbra Editora, pp. 162 e ss.

Novais, Jorge Reis, 2010, *As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*, 2.ª ed., Coimbra Editora, pp. 799 e ss.

Novais, Jorge Reis, 2015, *A Dignidade da Pessoa Humana*, vol. I, Almedina, pp. 58 e ss.

Otero, Paulo, 2001, «Coordenadas jurídicas da privatização da Administração Pública», in *Os caminhos da privatização da Administração Pública*, Coimbra, pp. 37 e ss.

Pinheiro, Alexandre Sousa, 2015, «A proteção de dados no novo Código do Procedimento Administrativo», in *Comentários ao Novo Código do Procedimento Administrativo*, 2.ª edição, AAFDL Editora, pp. 253 e ss.

Pinheiro, Alexandre Sousa, 2015, *Privacy e proteção de dados: a construção dogmática do direito à identidade informacional*, Lisboa, pp. 695 e ss.

Pollman, Elizabeth, 2014, «A Corporate Right to Privacy», in *Minnesota Law Review*, vol. 99, pp. 32 e 88.

Ramalho, David Silva, 2016, *O novo Regulamento Geral sobre a Proteção de Dados e o Data Protection Officer*, disponível em http://www.servulo.com/xms/files/00_SITE_NOVO/01_CONHECIMENTO/01_PUBLICACOES_SERVULO/2016/Updates/Update_PI__PD_e_TI_DSR_O_Novo_Regulamento_Geral _sobre_a_Protecao_de_Dados.pdf.

Rosa Matacán, Maria, 2011, *Protección de Datos Persónales en la Sociedad de la Información y la Vigilancia*, La Ley, Madrid.

Serrano, Rita, 2017, *Proposta de Regulamento do Parlamento Europeu e do Conselho, relativo à proteção da privacidade e ao tratamento de dados pessoais no sector das comunicações electrónicas («Proposal for na ePrivacy regulation»)*, disponível em http://www.servulo.com/xms/files/00_SITE_NOVO/01CONHECIMEN TO/01_PUBLICACOES_SERV ULO/2017/Updates/Update_Propriedade_Intelectual_RSO_01.02.2017_ePrivacy_Regulation.pdf.

Serrano Pérez, Maria, 2003, *El Derecho Fundamental a la protección de datos. Derecho español y comparado*, Civitas, Madrid, p. 72.

Silva, Jorge Pereira da, 2015, *Deveres do Estado de Protecção de Direitos Fundamentais*, Universidade Católica Editora, pp. 729 e ss.

Silva, Suzana Tavares da, 2012, «O tetralemma do controlo judicial da proporcionalidade no contexto da universalização do princípio: adequação, necessidade, ponderação e razoabilidade», in *Boletim da Faculdade de Direito Coimbra*, n.º 2, pp. 668 e 678.

Soriano García, Jose Eugenio, 2012, «Derecho al olvido y la creación de derechos», in *Revista de Economia e Direito*, Lisboa, vol. 17, n.º 1, pp. 207 e ss.

Teixeira, Maria Leonor da Silva, 2013, «A União Europeia e a protecção de dados pessoais: "Uma visão futurista"?», in *Revista do Ministério Público*, n.º 135, p. 66.

Terrinha, Luís Heleno, 2015, *Direito e contingência: com e para além de Ulrich Beck, In Memoriam Ulrich Beck, Atas do colóquio promovido pelo ICJP e pelo CIDP*, disponível em https://www.icjp.pt/sites/default/files/ publicacoes/files/ebook_ulrichbeck_0.pdf, p. 21.

Warren, Samuel / Brandeis, Louis, 1995, *El derecho a la intimidad*, Madrid: Civitas.