REVISTA FOCO e-issn: 1981-223X
Journal of Business Studies and Law

A SEGURANÇA NA PROTEÇÃO DE DADOS: ENTRE O RGPD EUROPEU E A LGPD BRASILEIRA

SECURITY IN DATA PROTECTION: BETWEEN THE EUROPEAN GDPR AND THE BRAZILIAN LGPD

Manuel David Masseno[1]
Guilherme Magalhães Martins[2]
José Luiz de Moura Faleiros Júnior[3]

Resumo: Este artigo expõe, criticamente, cada uma das principais questões relativas à segurança intrínseca no tratamento de dados resultantes da Lei Geral de Proteção de Dados Pessoais, do Brasil, mas desde uma perspectiva externa, a do Regulamento Geral sobre a Proteção de Dados, da União Europeia, o qual tem sido considerado como sua matriz. Assim, o presente estudo aprecia os pontos de contato entre o RGPD europeu, sob o olhar da experiência de Portugal, e da LGPD brasileira. Com efeito, a partir do método comparativo, serão apresentados os principais dispositivos normativos que cuidam da segurança de dados – tema eleito para o recorte proposto nesta análise –, sempre com aportes doutrinários pertinentes aos itens de maior relevância à análise em questão. Ao final, uma conclusão será apresentada com o intuito de confirmar a hipótese de pesquisa. Atendendo à proximidade juscultural, as referências se baseiam na Doutrina portuguesa especializada.
Palavras-chave: Brasil; dados pessoais; regulação; segurança; União Europeia.

Abstract: This article critically presents each of the main issues related to intrinsic security in the treatment of personal data as a result of the General Law for the Protection of Personal Data, in Brazil, but from an external perspective, that of the European Union's General Data Protection Regulation, which has been considered as its matrix. Thus, the present study appreciates the points of contact between the European GDPR, from the specific perspective of the Portuguese experience, in contrast to the Brazilian law. In effect, from the comparative method, the main normative frameworks that concern data security will be presented - theme chosen for the object selected for this analysis -, always with doctrinal contributions pertinent to the items of greatest relevance to the investigation in question. At the end, a

[1] Professor Adjunto e Encarregado da Proteção de Dados do IPBeja – Instituto Politécnico de Beja, em Portugal, onde também integra as Coordenações do Laboratório UbiNET – Segurança Informática e Cibercrime e do MESI – Mestrado em Engenharia de Segurança Informática. Pertence à EDEN Rede de Especialistas em Proteção de Dados da Europol Agência Europeia de Polícia e ainda ao Grupo de Missão "Privacidade e Segurança" da APDSI – Associação para a Promoção e Desenvolvimento da Sociedade da Informação. No Brasil, pertence ao Grupo de Trabalho de Direito Digital e *Compliance* da FIESP – Federação das Indústrias do Estado de São Paulo, às Comissões de Direito Digital da Seção de Santa Catarina e da Subseção de Campinas, assim como à Comissão de Inovação, Gestão e Tecnologia da Subseção de Guarulhos, todas da Ordem dos Advogados do Brasil. https://orcid.org/0000-0001-8861-0337 / masseno@ipbeja.pt

[2] Promotor de Justiça titular da 5ª Promotoria de Tutela Coletiva do Consumidor da Capital, do Ministério Público do Estado do Rio de Janeiro – MPRJ. Professor associado de Direito Civil da Faculdade Nacional de Direito da Universidade Federal do Rio de Janeiro – UFRJ. Professor permanente do Doutorado em Direito, Instituições e Negócios da Universidade Federal Fluminense – UFF. Doutor e Mestre em Direito Civil pela Faculdade de Direito da Universidade do Estado do Rio de Janeiro – UERJ. Ex-professor visitante do Mestrado em Direito da Faculdade de Direito da UERJ. Membro honorário do Instituto dos Advogados Brasileiros, junto à Comissão de Direito do Consumidor. Professor adjunto (licenciado) de Direito Civil da Universidade Cândido Mendes – Centro. Professor dos cursos de pós-graduação lato sensu da UERJ, PUC-RIO, EMERJ, INSPER, Damásio de Jesus, Universidade Cândido Mendes, UFRGS e UFJF. 2º Vice-Presidente do Instituto Brasileiro de Política e Direito do Consumidor – BRASILCON. https://orcid.org/0000-0003-3082-656X

[3] Mestre em Direito pela Universidade Federal de Uberlândia (UFU). Especialista em Direito Processual Civil, Direito Civil e Empresarial, Direito Digital e *Compliance*. Bacharel em Direito pela Universidade Federal de Uberlândia (UFU). Associado Fundador do Instituto Avançado de Proteção de Dados (IAPD). Membro do Instituto Brasileiro de Estudos de Responsabilidade Civil (IBERC). Advogado. http://orcid.org/0000-0002-0192-2336

conclusion will be presented in order to confirm the research hypothesis. In view of the cultural proximity, the references are based on the specialized Portuguese Doctrine.
Keywords: Brazil; personal data; regulation; safety; European Union.

Introdução

O presente estudo pretende analisar, comparativa e sistematicamente, os regimes jurídicos correspondentes à segurança no tratamento dos dados pessoais nos Ordenamentos da União Europeia e do Brasil, agora que a vigência da Lei n.º 13.709, de 14 de agosto de 2018 (a Lei Geral de Proteção de Dados – *LGPD*), está iminente, tendo em vista que, após uma inesperada discussão legislativa, nos dias 26 e 27 de agosto de 2020, a alteração consolidada na votação de conversão da Medida Provisória nº 959, de 29 de abril de 2020, definiu a imediata vigência dos dispositivos da LGPD, à exceção dos artigos 52 a 54 (que cuidam das sanções). Embora pendente a sanção presidencial, este se tornou um novo capítulo na complexa trama sobre a vigência da lei, amplificado, também no dia 26 de agosto de 2020, com a publicação do Decreto nº 10.474, que criou a estrutura administrativa da Agência Nacional de Proteção de Dados.

Efetivamente, a *LGPD* tem sido reiteradamente exposta como sendo uma "espécie de projeção" do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares [físicas] no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados), o *RGPD*, na terra de Vera Cruz.

Aliás, até a própria *occasio legis* seria suscetível de o demonstrar, pela coincidência da entrada em vigor do *RGPD*, no final de maio de 2018, com a aceleração do processo legislativo no Congresso brasileiro, depois de anos de hesitações na opção entre o "modelo norte-americano", de fragmentação legislativa vertical e aplicação judiciária *a posteriori*, e o "modelo europeu", prevalecente, com uma disciplina geral e uma implementação também feita através de autoridades administrativas independentes.

Porém, pode-se anotar que a proximidade é mais aparente do que real, sendo identificável um padrão comum: o da menor consideração dos interesses – e dos correspondentes direitos – das pessoas físicas, relativamente aos das organizações, mormente em se tratando de Instituições Públicas. Frente a esse problema, a hipótese de pesquisa cuida de indicar que, a despeito de algumas

similitudes, ainda há entre as duas normativas pontos de distanciamento cruciais para a efetiva aplicação da norma brasileira, particularmente quanto à segurança de dados.

Assim, o presente estudo aprecia os pontos de contato entre o *RGPD* europeu, sob o olhar da experiência de Portugal, e da *LGPD* brasileira. Com efeito, a partir do método comparativo, serão apresentados os principais dispositivos normativos que cuidam da segurança de dados – tema eleito para o recorte proposto nesta análise –, sempre com aportes doutrinários pertinentes aos itens de maior relevância à análise em questão. Ao final, uma conclusão será apresentada com o intuito de confirmar a hipótese de pesquisa.

1 Um objetivo comum entre a *LGPD* brasileira e o *RGPD* europeu: a segurança no tratamento dos dados pessoais

Por ocasião da promulgação da *LGPD*, no Brasil já vigorava o "Marco Civil da Internet", aprovado pela Lei n.º 12.965, 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil[4], incluindo diversas questões relativas à proteção de dados pessoais (arts. 3º, II e II; 7º, VII, VIII e X, 11 e 14), regulamentado pelo Decreto n.º 8.771, de 11 de maio de 2016, pelo que, tecnicamente, o "Marco Civil" até será uma Lei Geral perante a *LGPD*, no que se refere aos tratamentos de dados realizados na Internet, enquanto nos demais casos será aplicável por analogia.[5]

No entanto, a Constituição Federal, de 1988, apenas trata da matéria de um modo fragmentário e indireto. Além do *habeas data* (Art.º 5º, LXXII), só consta o direito ao respeito pela vida privada (Art.º 5º, X)[6].

---

[4] Maiores detalhes podem ser obtidos da leitura do estudo realizado por João Victor Rozatti Longhi (Marco Civil da Internet no Brasil: breves considerações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.). **Direito digital**: direito privado e internet. 3. ed. Indaiatuba: Foco, 2020, pp. 115-144), em especial quanto a seus fundamentos, princípios e ao regime de responsabilidade civil estabelecido.

[5] O microssistema em questão é composto, dentre outras normas, pela Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), pela Lei nº 12.965, de 23 de abril de 2014 (o chamado "Marco Civil da Internet"), pelo Decreto nº 8.771/2016, que a regulamentou; ainda, pela Lei nº 13.709, de 14 de agosto de 2018 (a chamada "Lei Geral de Proteção de Dados Pessoais"), posteriormente alterada pela Medida Provisória nº 869, de 27 de dezembro de 2018, que se consolidou pelo texto da Lei nº 13.853, de 08 de julho de 2019. Outras iniciativas de destaque são a Lei nº 12.527, de 18 de novembro de 2011 ("Lei de Acesso à Informação"), e a Lei nº 13.874, de 20 de setembro de 2019 ("Declaração de Direitos de Liberdade Econômica"). Além, é claro, do Código Civil (Lei nº 10.406/2002) e da própria Constituição da República. Nuantes específicas da incidência dessas normas podem ser colhidas dos escritos de Bruno Miragem (A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, São Paulo, v. 1009, p. 173-222, nov. 2019) e de Laura Schertel Mendes e Danilo Doneda (Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo: Revista dos Tribunais, v. 120, p. 468-486, nov./dez. 2018).

[6] O tema, inclusive, já foi objeto de investigações, especialmente quanto à distinção entre o direito fundamental à privacidade e um direito fundamental à proteção de dados pessoais. O tema pode ser explorado em: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 221-322; MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 161-190. Entretanto, em 2 de julho de 2019, foi aprovada, em segunda votação, pelo Senado Federal a

Quanto à disciplina da Segurança dos Dados, pode-se antecipar um padrão que revela maior consideração dos interesses das organizações, públicas ou privadas, em detrimento dos direitos dos cidadãos, enquanto titulares dos dados.[7] Mas, para que se possa entender as diferenças entre o *RGPD* e a *LGPD*, é preciso ter presente que os mesmos resultam de tradições diversas no que se refere à proteção de dados pessoais, apenas agora convergentes.

No que se refere às Fontes gerais europeias, o percurso já é de décadas, desde a Convenção do Conselho da Europa n.º 108, de 28 de janeiro de 1981, sobre a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, passando pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares [físicas] no que diz respeito ao tratamento de dados pessoais e à livre circulação

---

Proposta de Emenda à Constituição 17/2019, a qual acrescenta ao Art. 5º o inciso XII-A, estabelecendo que "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais".

[7] Um dos exemplos mais claros de uma tal escolha de Política Legislativa está na legitimação dada às organizações para criarem "perfis comportamentais", através de ferramentas técnicas próprias da Inteligência Artificial, aceitando a viabilidade de ocorrerem processos decisionais sem revisão humana (arts. 12, §2º, e 20, por força da Medida Provisória n.º 869, de 27 de dezembro de 2018, não revertida pela Lei n.º 13.853, de 8 de julho de 2019), bem como a previsão de um "uso compartilhado" por "órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados" (arts. 5º, XVI; 7º, III; 9º, V; 18, VII; e 26), este já regulamentado pelo Decreto n.º 10.046, de 9 de outubro de 2019, no que se refere à administração pública federal, o que autoriza o monitoramento permanente dos cidadãos, inclusive antecipando seus comportamentos futuros, e permite o seu condicionamento por tais organizações. Sobte o tema, valiosa a leitura dos escritos de José Luiz de Moura Faleiros Júnior (**Administração Pública digital**: proposições para o aperfeiçoamento do Regime Jurídico Administrativo na sociedade da informação. Indaiatuba: Foco, 2020, p. 118-124), de Daniela Copetti Cravo (Portabilidade de dados no poder público? **Jota**, 15 ago. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/portabilidade-de-dados-no-poder-publico-15082020. Acesso em: 29 de agosto de 2020) e, ademais, de Roberta Volpato Hanoff e Thiago Henrique Nielsen (A Lei Geral de Proteção de Dados Pessoais na administração pública brasileira: é possível implementar governança de dados antes de se implementar a governança em gestão? *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020, pp. 391-406). O que está em forte contrate com o disposto em matéria de "decisões individuais automatizadas, incluindo definição de perfis" (Art.ºs 22.º, *maxime* n.º 3 in *fine*, e 4.º 4), mas também e designadamente quanto às avaliações de impacto em proteção de dados (Art.º 35.º n.ºs 1 e 3 a), sobre estas questões, além das "Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679", de 3 de outubro de 2017/6 de fevereiro de 2018, do Grupo de Trabalho do Artigo 29, são de atender as considerações sintéticas de Catarina Sarmento e Castro (A jurisprudência do Tribunal de Justiça da União Europeia: o regulamento geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa. *In:* **Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos**. Coimbra: Almedina, 2016, v. I, pp. 1047-1070) e de Maria Eduarda Gonçalves (The EU Data Protection Reform and the Challenges of Big Data: tensions in the relations between technology and the law. *In:* NETO, Luísa; RIBEIRO, Fernanda (Eds.). **IV Colóquio Luso-Brasileiro Direito e Informação - Atas**. Porto: Faculdade de Letras da Universidade do Porto, pp. 46-63, 2016), os desenvolvimentos de 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:* CORDEIRO, António Menezes, OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech**: Desafios da Tecnologia Financeira. Coimbra: Almedina, 2017, pp. 75-202) e de Beatriz Santiago Trindade (Two years in: Does the GDPR already need updates? A question brought by algorithmic decision-making. **Anuário da Proteção de Dados - 2020**, Lisboa, pp. 79-103, 2020), os estudos aplicados de Manuel David Masseno (On the relevance of big data for the formation of contracts regarding package tours or linked travel arrangements, according to the new package travel directive. **Comparazione e Diritto Civile**, Salerno, n. 4, pp. 2-13, 2016; e Como a União Europeia procura proteger os cidadãos-consumidores em tempos de *Big Data*. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 14, n. 3, pp. 1-27, 2019) e de Manuel David Masseno e Cristiana Teixeira Santos (Personalization and Profiling of Tourists in Smart Tourism Destinations – a Data Protection perspective. **Revista Argumentum**, Marília, v. 20 n. 3, pp. 1215-1240, 2019) e ainda as referências contextualizadas de Francisca Cardoso Resende Gomes (O conteúdo do direito fundamental à proteção de dados à luz do novo Regulamento Geral de Proteção de Dados: em especial, a problemática do controlo das decisões automatizadas. **Anuário da Proteção de Dados - 2020**, Lisboa, pp. 105-119, 2020), designadamente.

desses dados, até à respetiva constitucionalização pelo Tratado sobre o Funcionamento da União Europeia (Art.º 16.º) e a Carta dos Direitos Fundamentais da União Europeia (Art.º 8.º), desde o Tratado de Lisboa (2007 – 2009), ambos os instrumentos com o mesmo valor formal que o Tratado da União Europeia (*ex vi* Art.º 6.º)[8], sem esquecer a Jurisprudência do Tribunal de Justiça da União Europeia, nomeadamente o Acórdão *Google Spain* (Processo C-131/12, de 13 de maio de 2014), proferido durante o processo legislativo que conduziu ao *RGPD* e teve uma grande importância para o prosseguimento do mesmo e seu conteúdo final[9].

Com efeito, no *RGPD* começa por ser enunciado um dever geral de "segurança no tratamento", o qual se projeta logo como um dos "princípios relativos ao tratamento de dados pessoais", o da "integridade e confidencialidade", pois os 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. (Art.º 5.º n.º 1 alínea f)."

Consequentemente, desde a concepção e por defeito (omissão), com ênfase na pseudonimização (Art.º 25.º n.º 1)[10]:

---

[8] Para uma melhor compreensão quanto à origem e à relevância destas Fontes, são sobretudo de atender os trabalhos de Maria Eduarda Gonçalves (**Direito da Informação**: novos direitos e formas de regulação na sociedade da informação. 2. ed. Coimbra: Almedina, 2003, pp. 88-97), e de Catarina Sarmento e Castro (**Direito da informática, privacidade e dados pessoais**. Coimbra, Almedina, 2005, p. 39-45) e, bem assim, de Alexandre Sousa Pinheiro (**Privacy e protecção de dados pessoais**: a construção dogmática do direito à identidade informacional. Lisboa: AAFD, 2015, pp. 528-546 e 573-661) e Alessandra Silveira e João Marques (Do direito a estar só ao direito ao esquecimento. Considerações sobre a proteção de dados pessoais informatizados no Direito da União Europeia: sentido, evolução e reforma legislativa. **Revista da Faculdade de Direito da UFPR**. Curitiba, v. 61, n. 3, pp. 91-118, 2016); além dos comentários aos referidos preceitos do Tratado sobre o Funcionamento da União Europeia, de Luís Neto Galvão (Comentário ao artigo 16.º do TFUE. *In:* PORTO, Manuel Lopes; ANASTÁCIO, Gonçalo (Eds.). **Tratado de Lisboa Anotado e Comentado**. Coimbra: Almedina, 2012, pp. 252-256), e da Carta dos Direitos Fundamentais da União Europeia, por Catarina Sarmento e Castro (Comentário ao artigo 8º. *In:* SILVEIRA, Alessandra; CANOTILHO, Mariana (Eds.). **Carta dos Direitos Fundamentais da União Europeia Comentada**. Coimbra: Almedina, 2013, pp. 120-128).

[9] Sobre este Acórdão, cuja importância não poderá nunca ser desvalorizada, tem-se as reflexões de Sofia Vasconcelos Casimiro (O direito a ser esquecido pelos motores de busca: o Acórdão Costeja. **Revista de Direito Intelectual**, Coimbra, n. 2, pp. 307-353, 2014), a que se juntaram os estudos de Filipa Urbano Calvão (A protecção de dados pessoais na internet: desenvolvimentos recentes. **Revista de Direito Intelectual**, Coimbra, n. 2, pp. 67-84, 2015), de João Marques (Direito ao Esquecimento – A Aplicação do Acórdão Google pela CNPD. **Fórum de Proteção de Dados**, Lisboa, n. 3, pp. 44-55, 2016) e de Catarina Sarmento e Castro (A jurisprudência do Tribunal de Justiça da União Europeia: o regulamento geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa. *In:* **Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos**. Coimbra: Almedina, 2016, v. I, pp. 1047-1070), assim como as considerações mais recentes de Catarina Santos Botelho (Novo Ou Velho Direito? – o direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global. **Ab Instantia**, Coimbra, n. 7, pp. 49-71, 2017), de Maria de Fátima Galante (A Internet e o Direito ao Esquecimento: Análise jurisprudencial. **Data Venia - Revista Jurídica Digital**, [S.l.], n. 9, pp. 223-250, 2018) e ainda de Rui P. Coutinho de Mascarenhas Ataíde (Direito ao esquecimento. **Cyberlaw by CIJIC**, Lisboa, n. 6, 2019.).

[10] Daí resulta que "A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento [controlador], ou o subcontratante [operador], deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Essas medidas deverão assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos 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); em termos gerais, são de referir as considerações breves de Alexandre L. Dias

> Tendo 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 [físicas], o responsável pelo tratamento [controlador] e o subcontratante [operador] aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco […], (Art.º 32.º n.º 1)

O qual se articula explicitamente com o princípio da "responsabilidade", dado que "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo" (Art.º 5.º n.º 2), e, por isso mesmo,

> Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares [físicas], cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades. (Art.º 24.º n.º 1).

Designadamente e em relação ao presente objeto de estudo, este princípio tem como corolários os regimes da responsabilidade (civil[11], Art.º 82.º, contraordenacional [administrativa][12],

---

Pereira (A Proteção de Dados Pessoais e o Direito à Segurança Informática no Comércio Eletrónico. **Banca, Bolsa e Seguros**, Coimbra, n.º 3, pp. 303-329, 2018), de Teresa Vale Lopes (Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. **Anuário da Proteção de Dados - 2018**, Lisboa, pp. 45-69, 2018), de Joana Mota (Proteção de dados desde a conceção e por defeito. Avaliação de impacto e segurança. *In:* CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech II**: Novos Estudos sobre Tecnologia Financeira. Coimbra: Almedina, 2019, pp. 129-146) e, sobretudo, de A. Barreto Menezes Cordeiro (**Direito da proteção de dados**. Coimbra: Almedina, 2020, pp. 326-335 e 346-347).

[11] A propósito da mesma, são de referir os estudos de Mafalda Miranda Barbosa (Protecção de Dados e Direitos de Personalidade: Uma Relação de Interioridade Constitutiva. Os Benefícios da Protecção e a Responsabilidade Civil. **Estudos de Direito do Consumidor**, Coimbra, n. 12, pp. 75-131, 2017), de A. Barreto Menezes Cordeiro (**Direito da proteção de dados**. Coimbra: Almedina, 2020, pp. 381-396), e de Tiago Branco da Costa (A responsabilidade civil decorrente da violação do Regulamento Geral sobre a Proteção de Dados. *In:* SILVEIRA, Alessandra; ABREU, Joana R. S. Covelo; COELHO, Larissa (Eds.). **UNIO Ebook Interop 2019**: O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: Pensamento Sábio - Associação para o conhecimento e inovação / Universidade do Minho - Escola de Direito, pp. 68-77, 2019), além das referências de Marco Alexandre Saias (Reforço da responsabilização dos responsáveis pelo tratamento de dados. **Revista Luso-Brasileira de Direito do Consumo**, Curitiba, n. 27, pp. 72-90, 2017) e do comentário de Cristina Pimenta Coelho (Artigo 82.º - Direito de indemnização e responsabilidade. *In:* PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, pp. 633-637).

[12] Quanto a estas, entretanto densificadas através das Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679, adotadas em 3 de outubro de 2017 pelo GT 29, tem-se as referências prospectivas de Catarina Sarmento e Castro (A jurisprudência do Tribunal de Justiça da União Europeia: o regulamento geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa. *In:* **Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos**. Coimbra: Almedina, 2016, v. I, pp. 1047-1070), assim como as iniciais de Marco Alexandre Saias (Reforço da responsabilização dos responsáveis pelo tratamento de dados. **Revista Luso-Brasileira de Direito do Consumo**, Curitiba, n. 27, pp. 72-90, 2017), além da análise de José Lobo Moutinho e David Silva Ramalho (Notas sobre o regime sancionatório da proposta de regulamento geral sobre a protecção de dados do Parlamento Europeu e do Conselho. **Fórum de proteção de dados**. Lisboa, n. 1, pp. 18-33, 2015), depois retomada por José Lobo Moutinho (Legislador português precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral sobre Protecção de Dados (Regulamento (UE) 2016/679). **Fórum de proteção de dados**. Lisboa, n. 4, pp. 40-57, 2017) e ainda as considerações de Pedro Miguel Freitas (The General Data Protection Regulation: an overview of the

Art.º 83.º, e, se os Estados-membros assim o decidirem, também penal, (Art.º 84.º), assim como a aplicação das regras e medidas de segurança que serão mencionadas em seguida.

Em termos análogos, da *LGPD* consta o princípio da segurança, o qual exige a "[…] utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (Art.º 6.º, VII). Pelo que, "[o]s sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares" (Art.º 49.º). E, por isso mesmo, "[o]s agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga[m]-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término" (Art.º 47.º).[13]

Este mesmo critério foi retomado e explicitado, até com alguma especificação, ao enunciar a Lei que

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (Art.º 46)

Tal como no *RGPD*, este princípio está articulado com o da responsabilização e prestação de contas, consistente na "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (Art.º 6.º, X).

Não obstante, a *LGPD* vai um pouco mais longe, prevendo que "[a] autoridade nacional poderá […] sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público" (Art.º 32.º). De igual modo e além de nas regras e medidas de segurança, este princípio tem uma especial importância no concernente às matérias "Da Responsabilidade e do Ressarcimento de Danos" (Art.ºs 42.º a 44.º) e das "Sanções Administrativas" (Art.ºs 52.º a 54.º).

2 As regras de segurança

---

penalties' provisions from a Portuguese standpoint. **UNIO - EU Law Review**, Braga, v. 4, n. 2, pp. 99-104, 2018), sem esquecer o comentário breve de Cristina Pimenta Coelho (Artigo 83.º - Condições gerais para a aplicação de coimas. *In:* PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, pp. 637-647).

[13] Veja-se, por todos, o estudo de Guilherme Magalhães Martins e José Luiz de Moura Faleiros Júnior (Segurança, boas práticas, governança e compliance. *In:* LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020, pp. 349-372).

Enquanto ponto de partida, resulta que do *RGPD* não consta a previsão de serem estabelecidas normas de segurança "vinculativas", a aprovar e/ou a auditar pela Comissão Europeia, pelos Estados-membros, pelas Autoridades nacionais ou mesmo pelo CEPD – Comité Europeu para a Proteção de Dados. Assim, apenas são indicados padrões genéricos, referidos como "medidas técnicas e organizativas adequadas", as quais deverão ser determinadas em função de critérios casuísticos, resultantes de análises de risco (Art.ºs 25.º n.ºs 1 e 2 e 32.º n.º 1)[14], ou de avaliações de impacto (Art.º 35.º), se estiverem reunidos os correspondentes pressupostos[15].

O que afasta esta disciplina da prevista pela Diretiva *ePrivacy*[16], remetendo explicitamente para esquemas autorregulatórios, consistentes em códigos de conduta (Art.ºs 40.º e 41.º) ou em instrumentos de certificação (Art.ºs 42.º e 43.º)[17].

Porém, se o respetivo acatamento "pode ser utilizado como elemento para demonstrar o cumprimento das obrigações" (Art.º 32.º n.º 3), o certo é que não exime de eventuais responsabilidades, apenas as podendo graduar (Art.º 83.º n.º 1 alínea d).

---

[14] Pois, "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." (Considerando 26). Sobre estas análises, numa perspetiva técnica, tem interesse o estudo de Luísa A. Inácio Varandas dos Santos e Mário R. Monteiro Marques (Gestão de Risco Aplicada à Segurança da Informação. **Cyberlaw by CIJIC – Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**. Lisboa, n. 7, 2019), e, desde uma perspetiva jurídica, as considerações de Teresa Vale Lopes (Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. **Anuário da Proteção de Dados - 2018**, Lisboa, pp. 45-69, 2018), Joana Mota (Proteção de dados desde a conceção e por defeito. Avaliação de impacto e segurança. *In:* CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech II**: Novos Estudos sobre Tecnologia Financeira. Coimbra: Almedina, 2019, pp. 129-146) e, ainda, de estudo de A. Barreto Menezes Cordeiro (**Direito da proteção de dados**. Coimbra: Almedina, 2020, pp. 317-322).

[15] Além de seguir as "Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679 (Revistas e adotadas pela última vez em 4 de outubro de 2017), do Comité Europeu para a Proteção de Dados, a este propósito e em geral, são de assinalar as referências breves de Luís Pica (As Avaliações de Impacto, o Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais. **Cyberlaw by CIJIC - Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**, Lisboa, n. 5, 2018) e as considerações de Teresa Vale Lopes (Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. **Anuário da Proteção de Dados - 2018**, Lisboa, pp. 45-69, 2018) e Joana Mota (Proteção de dados desde a conceção e por defeito. Avaliação de impacto e segurança. *In:* CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech II**: Novos Estudos sobre Tecnologia Financeira. Coimbra: Almedina, 2019, pp. 129-146), bem como e sobretudo o estudo de Bruno Pereira e João Orvalho (Avaliação de Impacto sobre a Protecção de Dados. **Cyberlaw by CIJIC - Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**. Lisboa, n. 7, 2019).

[16] Precisamente, no Art.º 4.º n.ºs 1-A, 4 e 5 da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), a propósito das "orientações" e das "medidas técnicas de execução" relativas à "segurança no processamento".

[17] Neste particular, tem-se já as das Orientações 1/2018 relativas à "certificação e à definição de critérios de certificação de acordo com os artigos 42.º e 43.º do Regulamento (Versão 3.0, de 4 de junho de 2019), adotadas pelo CEPD, e, embora em termos genéricos, são de lembrar os apontamentos de Luís Pica (As Avaliações de Impacto, o Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais. **Cyberlaw by CIJIC - Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**, Lisboa, n. 5, 2018) e de Teresa Vale Lopes (Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. **Anuário da Proteção de Dados - 2018**, Lisboa, pp. 45-69, 2018).

Mas, sendo o caso, também serão de observar as regras em matéria de Cibersegurança, cujos regimes jurídicos se sobrepõem. Antes de mais, relevam as presentes na Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, 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 [Diretiva *NIS* / *SRI*][18], já que

> Os Estados-Membros asseguram que os operadores de serviços essenciais tomem as 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. Essas medidas devem garantir um nível de segurança das redes e dos sistemas de informação adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes. (Art.º 14.º n.º 1)

Ainda neste âmbito e como referência, tem-se o Regulamento de Execução (UE) 2018/151, da Comissão, de 30 de janeiro de 2018, que estabelece normas de execução da Diretiva (UE) 2016/1148 "[…] no respeitante à especificação pormenorizada dos elementos a ter em conta pelos prestadores de serviços digitais[19] na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação […]".

E pode ainda vir a ser viável recorrer às normas constantes de um "sistema europeu de certificação de cibersegurança" (Art.ºs 51.º e 52.º do Regulamento (UE) 2019/881, de 17 de abril de 2019, relativo […] à certificação da cibersegurança das tecnologias da informação e comunicação [Regulamento Cibersegurança])[20].

Em síntese, o Legislador europeu teve sempre por referência as normas internacionais relevantes no que se refere à Segurança da Informação, designadamente a Norma ISO 27001, na medida em que esta se ajusta à proteção de dados pessoais[21].

Por sua vez, na *LGPD* a abordagem é simétrica, pois se "[o]s sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de

---

[18] A propósito desta disciplina, são de indicar as referências de: PEREIRA, Alexandre L. Dias. A Proteção de Dados Pessoais e o Direito à Segurança Informática no Comércio Eletrónico. **Banca, Bolsa e Seguros**, Coimbra, n.º 3, pp. 303-329, 2018.

[19] Enquanto "serviços digitais" são considerados os "1. Mercados em linha. [os] 2. Motores de pesquisa em linha. [e os] 3. Serviços de computação em nuvem", Art.º 4.º c) e Anexo III da Diretiva *NIS* / *SRI*.

[20] Estas questões têm escapado ao interesse da nossa Doutrina jurídica, mas sempre é de apontar o estudo de: CARRAPIÇO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. **European Politics and Society**, Londres, v. 19, n. 3, pp. 299-303, 2018.

[21] Sobre a Norma ISO 27001 (Por extenso, ISO/IEC 27001 - Tecnologia da informação - técnicas de segurança - sistemas de gestão da segurança da informação – requisitos) e sua implementação no contexto do *RGPD*, são de atender os Modelos propostos, ainda que desde a perspetiva da Segurança da Informação, por José C. Lourenço Martins *et al*. (Modelo Integrado de Atividades para a Gestão da Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais. **Cyberlaw by CIJIC - Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**, Lisboa, n. 5, 2018) e, ainda mais recentemente, por José C. Lourenço Martins (Método de Design, Implementação e Operação de um Sistema de Gestão de Segurança da Informação (V1.0). **Proelium – Revista Científica da Academia Militar**, Lisboa, A. VIII, n. 4, 2019), este tendo já em atenção a respetiva articulação com a Norma ISO/IEC 27701:2019, cujo Anexo D estabelece os correspondentes critérios.

segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. (Art.º 49)"

Da mesma resulta que, proativamente,

> A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* [corpo] deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* [corpo] do art. 6º desta Lei. (Art.º 46, § 1º)

E, também,

> […] editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei. (Art.º 55-J, XII)

Deste modo, apenas em termos complementares,

> Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. (Art.º 50) [22]

Sendo que "[a] autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais" (Art.º 51) e "[a]s regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional." (Art.º 50.º, § 3.º)

[22] Maiores detalhes acerca do tema, na forma como está apresentado pela LGPD, podem ser colhidos do estudo realizado por Guilherme Magalhães Martins e José Luiz de Moura Faleiros Júnior (Segurança, boas práticas, governança e compliance. *In:* LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020, p. 368): "A delimitação de deveres relacionados à segurança da informação denota uma preocupação profunda do legislador pátrio com a consolidação de parâmetros preventivos que correspondam à legítima expectativa do titular de dados de que os processos de coleta, tratamento e armazenagem aos quais está submetido serão hígidos e adequados. Trabalha-se, desse ponto de vista, com a ideia de governança (ou *compliance*) para além de uma responsabilidade acessória do agente de tratamento, muito embora a lei faça expressa menção ao seu implemento como uma faculdade (vide o emprego do verbo "poder", em lugar de "dever" no *caput* [corpo] do artigo 50). Isso porque a cláusula inserida no artigo 46, atrelada aos regramentos contidos ao longo de todo o texto da LGPD, reafirma a preocupação com a efetividade da proteção de dados pessoais. É insofismável a relevância deste capítulo da lei para a sua ampla compreensão, sendo certa, ademais, a importância destacada que os programas de governança corporativa representarão para todo aquele que opere com dados pessoais." Acerca dos impactos do tema para a responsabilidade civil, conferir, ainda: MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Compliance digital e responsabilidade civil na Lei Geral de Proteção de Dados. *In:* MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coords.). **Responsabilidade civil e novas tecnologias**. Indaiatuba: Foco, 2020, pp. 263-297.

3 Os dados pessoais e a limitação do seu tratamento

Se, nos termos do *RGPD*, é considerado como "dado pessoal" toda

> […] informação relativa a uma pessoa singular [física] identificada ou identificável («titular dos dados»)é considerada identificável uma pessoa singular [física] 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 [física] (Art.º 4.º 1)[23].

[23] O que incluí os quase-identificadores e os metadados, como os registros de conexão [no Brasil, definidos pelo Marco Civil como "o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (Art. 5º, VIII)], merecendo consulta, para maior aprofundamento, os escritos de Fabio Nori (A guarda dos registros de conexão e dos registros de acesso às aplicações no Marco Civil. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coords.). **Direito & Internet III**: Marco Civil da Internet (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. II, pp. 169-190)e de Antonia Espíndola Longoni Klee em coautoria com Guilherme Magalhães Martins (A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei nº 12.965/2014). *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coords.). **Direito & Internet III**: Marco Civil da Internet (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. I, pp. 291-368). A esse respeito, aliás, válido o destaque ao recente pronunciamento do Superior Tribunal de Justiça, por ocasião do julgamento do REsp nº 1.784.156/SP, que decidiu de forma a ampliar o referido conceito, impondo o fornecimento, além do endereço IP, também da porta lógica. Quanto ao tema, maiores informações podem ser colhidas do escrito de Guilherme Magalhães Martins, João Victor R. Longhi e José Luiz de Moura Faleiros Júnior (Porta lógica, IP e os registros de acesso a aplicações da Internet: Uma leitura ampliativa do art. 5º, VIII do Marco Civil da Internet. **Jota**, 26 dez. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/porta-logica-ip-e-os-registros-de-acesso-a-aplicacoes-da-internet-26122019. Acesso em: 29 de agosto de 2020). Ademais, cumpre salientar que "[a]s pessoas singulares [físicas] podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (*cookie*) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares [físicas]." (Considerando 30 do *RGPD*). Nesta matéria, há ainda que atender ao conteúdo do Parecer 4/2007 sobre o "conceito de dados pessoais", de 20 de junho de 2007, do GT 29, assim como à Jurisprudência do Tribunal de Justiça da União Europeia, a qual culminou no Acórdão proferido no Processo C-582/14, Patrick Breyer, de 19 de outubro de 2016. Na Doutrina, são de atender as considerações de Filipa Urbano Calvão (A protecção de dados pessoais na internet: desenvolvimentos recentes. **Revista de Direito Intelectual**, Coimbra, n. 2, pp. 67-84, 2015), esta ainda durante as negociações do Regulamento Geral, e de Mafalda Miranda Barbosa (Protecção de Dados e Direitos de Personalidade: Uma Relação de Interioridade Constitutiva. Os Benefícios da Protecção e a Responsabilidade Civil. **Estudos de Direito do Consumidor**, Coimbra, n. 12, pp. 75-131, 2017), tal como o estudo de A. Barreto Menezes Cordeiro (Dados pessoais: conceito, extensão e limites. **Revista de Direito Civil**, Coimbra, v. 3 n. 2, pp. 297-321, 2018), cujas conclusões são retomadas em A. Barreto Menezes Cordeiro (**Direito da proteção de dados**. Coimbra: Almedina, 2020, pp. 107-131), e de Augusto César Torbay (A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia. **Anuário da Proteção de Dados - 2020**, Lisboa, pp. 49-78, 2020), assim como as referências de Francisca Cardoso Resende Gomes (O conteúdo do direito fundamental à proteção de dados à luz do novo Regulamento Geral de Proteção de Dados: em especial, a problemática do controlo das decisões automatizadas. **Anuário da Proteção de Dados - 2020**, Lisboa, pp. 105-119, 2020) ademais do comentário à definição por parte de Alexandre Sousa Pinheiro (Artigo 4.º - Definições. *In:* PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, pp. 115-204).

Em contrapartida, da *LGPD* apenas consta uma definição muito sintética de "dado pessoal", como a "informação relacionada a pessoa natural identificada ou identificável", sem indicação de identificadores (Art.º 5.º, I).

Mas, a mesma deve ser integrada com a de

> dado pessoal sensível: [que é o] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Art.º 5º, II)

E "[p]oderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles [dados] utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada" (Art.º 12.º, § 2.º). A delimitando, negativamente, pelo conceito de "dado anonimizado: [enquanto] dado relativo a titular que não possa ser identificado […]" (Art.º 5.º, III). Isto, sem esquecer o Regulamento do Marco Civil da Internet, o qual, complementarmente, o define como o "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (Art.º 14.º, I).

Por sua vez, embora tenha por objetivo primeiro o da garantia dos direitos dos titulares dos dados, a limitação do respetivo tratamento desempenha também uma função relevante no que se refere à segurança, estando subjacente às correspondentes disciplinas. Isto, tanto por reduzir os riscos em casos de incidentes, quanto por dificultar, ou até mesmo impossibilitar, a utilização de ferramentas analíticas de *Big Data*, melhor dizendo de "megadados".[24]

[24] Quanto às implicações do tratamento destes "megadados", a Autoridade Europeia para a Proteção de Dados tem sido bastante assertiva, desde o Parecer preliminar "Privacidade e competitividade na era dos grandes volumes de dados: a articulação entre a proteção de dados, a lei da concorrência e a proteção do consumidor na Economia Digital", de 14 de março de 2014, reforçado pelo Parecer 4/2015 "Rumo a uma nova ética digital: dados, dignidade e tecnologia", de 11 de setembro de 2015, logo seguido do Parecer 7/2015 "Corresponder aos desafios dos Grandes Volumes de Dados: Um apelo à transparência, controlo do utilizador, proteção de dados desde a conceção e responsabilidade", de 19 de novembro do mesmo ano, entretanto atualizado pelo Parecer 8/2016 "Aplicação efetiva da legislação na economia digital", de 23 de setembro de 2016. Por sua vez, o Grupo de Trabalho do Artigo 29.º, que enfrentara estes problemas, pela primeira vez, no seu Parecer 2/2010, sobre "a publicidade comportamental em-linha", voltou a abordá-los com o Parecer 5/2012, sobre a "Computação em Nuvem", de 1 de julho de 2012, e pelo Parecer 3/2013, sobre "limitação de finalidade", antes referido, bem como e sobretudo pela "Declaração do Grupo do Artigo 29.º sobre o impacto do desenvolvimento da *Big Data* na proteção das pessoas relativamente ao tratamento dos seus dados pessoais na UE", de 16 de setembro de 2016. A este propósito e em termos gerais, tem-se as referências de Catarina Sarmento e Castro (A jurisprudência do Tribunal de Justiça da União Europeia: o regulamento geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa. *In:* **Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos**. Coimbra: Almedina, 2016, v. I, pp. 1047-1070), assim como o estudo de Manuel David Masseno (On the relevance of big data for the formation of contracts regarding package tours or linked travel arrangements, according to the new package travel directive. **Comparazione e Diritto Civile**, Salerno, n. 4, pp. 2-13, 2016), no âmbito do Direito Privado, e o de Maria Eduarda Gonçalves (The EU Data Protection Reform and the Challenges of Big Data: tensions in the relations between technology and the law. *In:* NETO, Luísa; RIBEIRO, Fernanda (Eds.). **IV Colóquio Luso-Brasileiro Direito e Informação - Atas**. Porto: Faculdade de Letras da Universidade do Porto, pp. 46-63, 2016), no do Público, seguidos do de 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:* CORDEIRO,

Assim, no *RGPD* é enunciado o princípio da «minimização dos dados», já que estes devem ser "[a]dequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados" (Art.º 5.º n.º 1 alínea c). O que tem também uma dimensão temporal, que o articula com o princípio da «limitação da conservação», sendo aqueles "[c]onservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados […]" (Art.º 5.º n.º 1 alínea d)[25].

Consequentemente,

> […] o responsável pelo tratamento [controlador] aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas […] destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização. (Art.º 25.º n.º 1).

O que é depois especificado, dado que

> O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito [por omissão], 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 [físicas]. (Art.º 25 n.º 2).

O mesmo princípio releva, ainda, a propósito das "regras vinculativas aplicáveis às empresas" nas transferências de dados pessoais para países terceiros ou organizações internacionais (Art.º 47.º n.º 1 alínea d) ou do "tratamento para fins de arquivo de interesse público ou para fins de investigação científica ou histórica ou para fins estatísticos" (Art.º 89.º n.º 1).

Por sua vez, na *LGPD* é enunciado o "princípio da necessidade", consistindo este na "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (Art.º 6º, III), tendo também limites temporais, nomeadamente com a "verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada" (Art.º 15.º, I).

António Menezes, OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech**: Desafios da Tecnologia Financeira. Coimbra: Almedina, 2017, pp. 75-202).

[25] Sobre o conteúdos deste(s) princípio(s) são de indicar as referências breves de Alexandre Sousa Pinheiro (Artigo 4.º - Definições. *In:* PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, pp. 115-204) e de A. Barreto Menezes Cordeiro (**Direito da proteção de dados**. Coimbra: Almedina, 2020, pp. 158-131) e ainda as do estudo de Manuel David Masseno com Cristiana Teixeira Santos (Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations. **MediaLaws – Rivista di Diritto dei Media**, Milão, n. 2, pp. 251-266, 2018).

4 A anonimização e a pseudonimização

Antes de tudo o mais e no que concerne ao *RGPD*, é necessário afirmar que a "anonimização", enquanto técnica destinada a garantir a segurança dos dados pessoais, nem sequer é referida no seu articulado. Por isso,

> […] 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. (Considerando 26, *in fine*)

Mais explícito ainda é o Regulamento (UE) 2018/1807, de 14 de novembro de 2018, relativo a um regime para o livre fluxo de dados não pessoais na União Europeia, o qual complementa o *RGPD*. Este, além de distinguir "dados pessoais" de "dados não pessoais" e de restringir a sua aplicação a estes, incluindo as situações em que ambos "estejam indissociavelmente ligados", reitera a imperatividade dos regimes de proteção dos dados pessoais (Art.ºs 2.º n.º 2 e 3.º 1).

E, mais ainda, deixa em evidência que

> A internet das coisas, a inteligência artificial e a aprendizagem automática, que estão em expansão, representam grandes fontes de dados não pessoais, por exemplo, em consequência da sua utilização em processos automatizados de produção industrial. [Concluindo que] Se os progressos tecnológicos permitirem transformar dados anonimizados em dados pessoais, esses dados devem ser tratados como dados pessoais, e o Regulamento (UE) 2016/679 deve ser aplicado em conformidade.[26-27].

[26] Ao que acresce o explicitado pela Comissão Europeia na sua Comunicação, interpretativa, "Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia" (COM(2019) 250 final, de 25 de maio de 2019), com referências específicas e desenvolvidas quanto a esta questão, concluindo que "[…] se determinados dados não pessoais puderem ser associados a uma pessoa de qualquer forma, tornando-os direta ou indiretamente identificáveis, devem ser considerados dados pessoais. [e, do mesmo modo] Aplicam-se as mesmas regras [as relativas ao tratamento de dados pessoais] quando a evolução da tecnologia e da análise de dados torna possível a conversão de dados anonimizados em dados pessoais."

[27] Nesta matéria, é fundamental o Parecer n.º 5/2014, sobre "técnicas de anonimização", de 10 de abril, do GT 29, e, sobre a mesma, começámos por dispor das considerações de Catarina Sarmento e Castro (A jurisprudência do Tribunal de Justiça da União Europeia: o regulamento geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa. *In:* **Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos**. Coimbra: Almedina, 2016, v. I, pp. 1047-1070), sendo que, logo após a publicação do *RGPD*, esta questão foi identificada e analisada por 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:* CORDEIRO, António Menezes, OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech**: Desafios da Tecnologia Financeira. Coimbra: Almedina, 2017, pp. 75-202), a propósito das implicações da *Big Data*, entretanto, a questão foi enfrentada por A. Barreto Menezes Cordeiro (Dados pessoais: conceito, extensão e limites. **Revista de Direito Civil**, Coimbra, v. 3 n. 2, pp. 297-321, 2018), a propósito dos limites da "identificabilidade", retomando-a A. Barreto Menezes Cordeiro (**Direito da proteção de dados**. Coimbra: Almedina, 2020, pp. 126-131) , assim como por Augusto César

Isto, porque a identificação a partir de dados anónimos, ou a re-identificação de dados anonimizados, passaram a ser tecnicamente viáveis, designadamente com base nas analíticas de *Big Data*[28].

O que nos permite concluir que, na União Europeia, vigora um limite móvel entre os "dados pessoais" e os "dados não pessoais", com uma tendência expansiva dos primeiros, à medida que a tecnologia o permita. O que exige uma atitude de prevenção e de precaução permanentes por parte de quem assume beneficiar do respetivo tratamento, com os inerentes riscos e sem exclusão das respectivas responsabilidades, retomando o antigo brocardo *cuius commoda eius et incommoda*.

Diferentemente do que sucede com a "anonimização", a "pseudonimização" é definida pelo *RGPD*, 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. (Art.º 4.º 5)

E além de ser fortemente sugerida[29], surge qualificada como constituindo uma "medida técnica adequada para assegurar um nível de segurança adequado ao risco" (Art.º 32 n.º 1 alínea c). Mais ainda, constitui o "exemplo" de "medidas técnicas adequadas (…) destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento", no contexto da proteção de dados desde a concepção (Art.º 25.º n.º 1),

---

Torbay (A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia. **Anuário da Proteção de Dados - 2020**, Lisboa, pp. 49-78, 2020); ademais, tem-se o estudo de Manuel David Masseno (Na borda: dados pessoais e não pessoais nos dois Regulamentos da União Europeia. **Cyberlaw by CIJIC - Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**, Lisboa, n. 9, 2020) sobre os limites entre ambos os Regulamentos referidos.

[28] Neste mesmo sentido, com uma assertividade crescente, foi-se pronunciando o GT 29, designadamente, no Parecer n.º 7/2003, de 12 de dezembro, sobre a "reutilização de informações do setor público e a proteção dos dados pessoais", no Parecer n.º 6/2013, de 5 de junho, sobre "dados abertos e reutilização de informações do setor público (ISP)", de 5 de junho, e, sobretudo, de um modo muito detalhado, no Parecer sobre as "técnicas de anonimização", antes referido.

[29] Designadamente, no Considerando 26, segundo o qual, "[o]s 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 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.", mas também no Considerando 28, "A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento [controladores] e os seus subcontratantes [operadores] a cumprir as suas obrigações de proteção de dados. A introdução explícita da «pseudonimização» no presente regulamento não se destina a excluir eventuais outras medidas de proteção de dados". A este propósito, são interessantes as considerações recentes de Augusto César Torbay (A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia. **Anuário da Proteção de Dados - 2020**, Lisboa, pp. 49-78, 2020), embora a sua não distinção clara entre as referências do Considerando à pseudonimização e a anonimização o conduza a conclusões muito diferentes.

com a sua especificação a dever constar dos "códigos de conduta" (Art.º 40.º n.º 2 alínea d) ou a ser usada para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos (Art.º 89.º n.º 1).

Porém, o problema está em a re-identificação dos titulares dos dados pessoais ser ainda mais fácil tecnicamente que com a anonimização, não o só com base nas analíticas de *Big Data*, mas também por outras vias (*v.g.*, por correlações, ou por notícias de jornal, ou por dados de utilização de celulares ou de cartões de crédito ou ainda por reversão de pseudónimos através de "força bruta"), o que é assumido no próprio *RGPD*[30].

Daí a preocupação manifesta com os riscos inerentes à "inversão não autorizada da pseudonimização"[31]. O que torna necessária, ou muito aconselhável, uma "pseudonimização forte", incluindo os quase-identificadores, já próxima das técnicas de cifragem, *v.g.*, com uma atribuição aleatória de códigos, desligados dos dados originais, e não reversível com a mesma tecnologia.

Em contraponto, a *LGPD* toma a "anonimização" como uma referência técnica destinada a garantir a segurança do tratamento de dados pessoais[32] e define-a como a "utilização de meios

[30] Para começar, se é certo que "[a] aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento [controladores] e os seus subcontratantes [operadores] a cumprir as suas obrigações de proteção de dados." (Considerando 28) e, "A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento [controlador] quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento e a conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico", como explicita o Considerando 29. Aliás, estas mesmas limitações constam do Parecer do GT 29 sobre as "técnicas de anonimização", já referido.

[31] Pois "[o] risco para os direitos e liberdades das pessoas singulares [físicas], cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social;", Considerando 75, e "[s]e não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares [físicas], como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares [físicas]", Considerando 85.

[32] O tema foi análisado, quanto à experiência brasileira, por Guilherme Magalhães Martins e José Luiz de Moura Faleiros Júnior (A anonimização de dados pessoais: consequências jurídicas do processo de reversão, a importância da entropia e sua tutela à luz da Lei Geral de Proteção de Dados. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coords.). **Direito & Internet IV**: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019, p. 77): "Analisou-se em maiores minúcias como diversos preceitos que inspiraram a edição desses marcos regulatórios estão conectados à segurança jurídica e à transparência na coleta, no tratamento e na armazenagem de dados pessoais, de modo que a definição de alguns temas adquiriu especial relevância, e é nesse ponto que centro de investigação abordado se insere: com o intuito de retirar dos dados pessoais coletados quaisquer informações que permitam identificar e, evidentemente, expor a pessoa à qual dizem respeito, alguns processos técnicos prometem viabilizar o uso desses dados sem risco de violações, colocando os dados anonimizados noutro polo em relação ao dos dados pessoais. Questionando a confiabilidade de tais mecanismos, destacou-se que a heurística computacional surge como um passo inicial a ser exigido dos operadores de dados, causando reflexos no que diz respeito aos modais de tutela jurídica adequados ao tema, uma vez que a lei brasileira, por exemplo, se limitou a trabalhar com um filtro de razoabilidade que, embora conceituado no corpo do texto normativo, depende muito mais de atualizações constantes à luz das melhores técnicas da matemática e da ciência da computação. Nesse sentido, a prática denominada *entropia* passa a se coadunar com a expectativa não apenas de boas práticas na anonimização de dados para

técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (Art.º 5º, XI).

Depois, é referida a propósito da legitimidade "para a realização de estudos por órgão de pesquisa" (Art.º 7º, IV), mesmo no que se refere ao tratamento de dados sensíveis (Art.º 11.º, II, c), desde que indispensável, assim como "na realização de estudos em saúde pública", neste último caso a par da pseudonimização (Art.º 13.º).

Adicionalmente, também justifica a conservação dos dados anonimizados, "após o término do seu tratamento", desde que "para finalidades [de] de estudo por órgão de pesquisa" (Art.º 16, II).

Além de poder ser exigida, pelo titular dos dados, ao controlador, "a qualquer momento e mediante requisição", a anonimização dos "dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei" (Art.º 18.º, IV), ficando ainda excluída a portabilidade dos dados anonimizados (Art.º 18.º, § 7-º).

Porém e, afastando-se do regime europeu, as suas limitações intrínsecas e temporais são assumidas *ab initio* pelo Legislador, por o critério indicado para a qualificação dos "dados anonimizados" ter por referência os "meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (Art.º 5.º, III), o mesmo valendo para a "anonimização" enquanto processo.

Mas, sendo certo que

> Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios [*i.e.*, não de ou por terceiros], ou quando, com esforços razoáveis, puder ser revertido. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. (Art.º 12.º)

O que tem uma especial relevância em termos de responsabilidade civil, pois se "Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano" (Art.º 44.º, parágrafo único).

A aplicação dos "meios técnicos razoáveis e disponíveis no momento do tratamento" afastará a correspondente ilicitude (Art.º 43.º, III), não tornando sequer irregular o tratamento desses dados "[…] quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais [III] as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado." (Art.º 44.º).

---

fins de proteção da privacidade, mas também como uma "régua" que conduz à aferição – a partir de parâmetros mais objetivos – do potencial de reversão de um determinado método empregado para anonimizar dados."

O mesmo vale para as sanções administrativas, sendo critério de apreciação da respetiva conduta "[…] a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei" (Art.º 52.º, § 1.º, VIII).

Em termos substancialmente análogos aos do *RGPD*, a "pseudonimização" é identificada como "[…] o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (Art.º 13.º § 4.º).

No entanto, a mesma apenas surge a propósito da "realização de estudos em saúde pública, [para os quais] os órgãos de pesquisa poderão ter acesso a bases de dados pessoais", como uma alternativa, menos exigente, à "anonimização" (Art.º 13.º, corpo). Apesar disso, é uma das possíveis "[…] medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (Art.º 6.º, VII). Ou, mais especificamente, uma das "[…] medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (Art.º 46.º).

Porém, ao não existir uma previsão análoga à "anonimização", no que se relativa à determinação de regras técnicas de segurança pela autoridade nacional (Art.º 12.º, § 3.º), apenas releva o poder genérico de esta dispor "padrões técnicos mínimos", também a este propósito (§ 1.º do Art.º 46.º). Consequentemente, fica mais difícil afastar a ilicitude em caso de incidente de segurança, no que se refere à responsabilidade civil e às sanções administrativas.

5 A cifragem

Esta é referida quase a medo pelo *RGPD*, o qual não a define, surgindo sempre a par da "pseudonimização", a propósito dos tratamentos que não tenham por base o consentimento dos titulares dos dados (Art.º 7.º n.º 4 alínea e), da segurança no tratamento (Art..º 32.º n.º 1 alínea a) e, sobretudo, da isenção de responsabilidades no caso de ocorrerem incidentes de segurança (Art.º 34.º n.º 3 alínea a), sempre que

> O responsável pelo tratamento [controlador] tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas 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.

Não obstante, deve-se ter presente que a "cifragem dos dados pessoais", só por si, não baste (Art.º 32.º n.º 1 alínea a), por a mesma apenas poder garantir a confidencialidade dos dados, não as respectivas integridade e disponibilidade[33]. O que em especial a aconselha perante "grandes riscos", designadamente perante o tratamento de "categorias especiais de dados pessoais" [dados sensíveis] (Art.º 9.º), na sequência de avaliações de impacto (Art.º 35.º). Ainda assim, a cifragem, e mesmo uma cifragem "forte", sem acesso por quaisquer terceiros, inclusive com autorização judicial, tem vindo a ser proposta ou defendida institucionalmente na União Europeia ainda que no plano da *Soft Law*.

Já na *LGPD*, a despeito dos alertas da doutrina[34], a cifragem não é, sequer, mencionada, embora esteja implícita quando refere que "[n]o juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. (Art.º 48.º, § 3.º)."

Pelo que estará só entre as "[…] medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (Art.º 46.º)"

Embora, tal como no *RGPD*, também não baste, só por si, para afastar a responsabilidade civil ou sanções administrativas, pois pode não ser viável reverter ou mitigar os efeitos do incidente de segurança (Art.º 48.º, § 1.º, VI, e § 2.º, II), por sua natureza, a cifragem é a técnica mais pertinente para prevenir danos maiores, tal como se verifica no *RGPD*.

Conclusão

Inegavelmente, diversas coincidências podem levar o intérprete a visualizar a *LGPD* brasileira como substrato inspirado na experiência europeia e, particularmente, no *RGPD*. Entretanto, quando se perquire as minúcias das duas legislações, observa-se que ainda há lacunas e,

[33] Daí, o caráter cumulativo das medidas de segurança (Art.º 32.º n.º 1), ou seja, "A capacidade de assegurar [não só] a confidencialidade, [mas também a] integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento" (b), "A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico" (c) e ainda "Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento." (d).

[34] Recomenda-se a leitura dos trabalhos de Fabiano Menke (A criptografia e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). *In:* DONEDA, Danilo; MACHADO, Diego (Coord.). **A criptografia no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 123-136) e do estudo realizado por Diego Machado em coautoria com Danilo Doneda (Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *In:* DONEDA, Danilo; MACHADO, Diego (Coords.). **A criptografia no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, pp. 137-164).

especialmente no que concerne à segurança da informação para o tratamento de dados pessoais, alguns temas revelam a necessidade de aprimoramentos.

Como se viu, para além de definir os objetos de incidência de seus ditames (os dados pessoais), a *LGPD* os distinguiu dos dados anonimizados, em conceituação que não levou em consideração, com a clareza esperada, a diferença entre "anonimização" e "pseudonimização", da qual poderia se beneficiar para produzir melhores conclusões, a nível de responsabilidade civil, quando apresenta causa excludente do nexo de causalidade (Art.º 43.º, II) representativa da nebulosa e ainda incerta "razoabilidade" quanto à implementação de mecanismos de segurança (Art.ºs. 12.º, § 1.º, 44.º, I a III, 46.º e 50.º).

Ponto confuso é, outrossim, a questão da cifragem de dados, que poderia ter sido devidamente conceituada na lei para, em conjugação com a leitura que se faz do conceito de "dado anonimizado" e para os fins da delimitação dos parâmetros de segurança da informação adequados à aferição dos esforços suficientes para a mitigação ou eliminação do nexo causal, permitir o adequado reforço à segurança jurídica que a lei pretensamente explicita.

Enfim, se ainda há muitas controvérsias quanto à futura efetividade da *LGPD*, é certo que a experiência europeia – e, neste particular, a doutrina portuguesa tem apresentado forte repositório doutrinário para a ampla compreensão do tema – atenderá aos propósitos que são inerentes ao estudo comparado. Mais do que nunca, o intercâmbio de experiências trará ao Brasil imprescindível reforço dogmático rumo à concretização do *telos* essencial da segurança de dados, especialmente frente aos acinzentados meandros em que sua aplicação se faz necessária.

Referências

ABREU, Carlos Pinto de. Breves notas sobre segurança da informação, acesso a dados e privacidade. **C&R - Revista de Regulação e Concorrência**, Lisboa, n. 35, pp. 49-78, 2018. Disponível em: http://www.concorrencia.pt/vPT/Estudos_e_Publicacoes/Revista_CR/Documents/Revista_ReC_35.pdf. Acesso em: 29 de agosto de 2020.

ATAÍDE, Rui P. Coutinho de Mascarenhas. Direito ao esquecimento. **Cyberlaw by CIJIC**, Lisboa, n. 6, 2019. Disponível em: https://www.cijic.org/wp-content/uploads/2019/05/Rui-Ata%C3%ADde_Direito-esquecimento.pdf. Acesso em: 29 de agosto de 2020.

BARBOSA, Mafalda Miranda. Protecção de Dados e Direitos de Personalidade: Uma Relação de Interioridade Constitutiva. Os Benefícios da Protecção e a Responsabilidade Civil. **Estudos de Direito do Consumidor**, Coimbra, n. 12, pp. 75-131, 2017. Disponível em: https://www.fd.uc.pt/cdc/pdfs/rev_12_completo.pdf. Acesso em: 29 de agosto de 2020.

BARBOSA, Mafalda Miranda. *Data controllers* e *data processors*: da responsabilidade pelo tratamento de dados à responsabilidade civil. **Revista de Direito Comercial**, Lisboa, n. 2, pp. 424-

494, 2018. Disponível em: https://www.revistadedireitocomercial.com/data-controllers-e-data-processors. Acesso em: 29 de agosto de 2020.

BOTELHO, Catarina Santos. Novo Ou Velho Direito? – o direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global. **Ab Instantia**, Coimbra, n. 7, pp. 49-71, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130258. Acesso em: 29 de agosto de 2020.

CALVÃO, Filipa Urbano. A protecção de dados pessoais na internet: desenvolvimentos recentes. **Revista de Direito Intelectual**, Coimbra, n. 2, pp. 67-84, 2015.

CARRAPIÇO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. **European Politics and Society**, Londres, v. 19, n. 3, pp. 299-303, 2018.

CASIMIRO, Sofia Vasconcelos. O direito a ser esquecido pelos motores de busca: o Acórdão Costeja. **Revista de Direito Intelectual**, Coimbra, n. 2, pp. 307-353, 2014.

CASTRO, Catarina Sarmento e. A jurisprudência do Tribunal de Justiça da União Europeia: o regulamento geral sobre a proteção de dados pessoais e as novas perspetivas para o direito ao esquecimento na Europa. *In:* **Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos**. Coimbra: Almedina, 2016, v. I, pp. 1047-1070.

CASTRO, Catarina Sarmento e. Comentário ao artigo 8º. *In:* SILVEIRA, Alessandra; CANOTILHO, Mariana (Eds.). **Carta dos Direitos Fundamentais da União Europeia Comentada**. Coimbra: Almedina, 2013, pp. 120-128.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra, Almedina, 2005.

COELHO, Cristina Pimenta. Artigo 82.º - Direito de indemnização e responsabilidade. *In:* PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, pp. 633-637.

COELHO, Cristina Pimenta. Artigo 83.º - Condições gerais para a aplicação de coimas. *In:* PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, pp. 637-647.

CORDEIRO, A. Barreto Menezes. Dados pessoais: conceito, extensão e limites. **Revista de Direito Civil**, Coimbra, v. 3 n. 2, pp. 297-321, 2018.

CORDEIRO, A. Barreto Menezes. **Direito da proteção de dados**. Coimbra: Almedina, 2020.

COSTA, Tiago Branco da. A responsabilidade civil decorrente da violação do Regulamento Geral sobre a Proteção de Dados. *In:* SILVEIRA, Alessandra; ABREU, Joana R. S. Covelo; COELHO, Larissa (Eds.). **UNIO Ebook Interop 2019**: O Mercado Único Digital da União Europeia como desígnio político: a interoperabilidade como o caminho a seguir. Braga: Pensamento Sábio - Associação para o conhecimento e inovação / Universidade do Minho - Escola de Direito, pp. 68-77, 2019. Disponível em: http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf . Acesso em: 29 de agosto de 2020.

CRAVO, Daniela Copetti. Portabilidade de dados no poder público? **Jota**, 15 ago. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/portabilidade-de-dados-no-poder-publico-15082020. Acesso em: 29 de agosto de 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FALEIROS JÚNIOR, José Luiz de Moura. **Administração Pública digital**: proposições para o aperfeiçoamento do Regime Jurídico Administrativo na sociedade da informação. Indaiatuba: Foco, 2020.

FREITAS, Pedro Miguel. The General Data Protection Regulation: an overview of the penalties' provisions from a Portuguese standpoint. **UNIO - EU Law Review**, Braga, v. 4, n. 2, pp. 99-104, 2018. Disponível em: https://revistas.uminho.pt/index.php/unio/article/view/24/56. Acesso em: 29 de agosto de 2020.

GALANTE, Maria de Fátima. A Internet e o Direito ao Esquecimento: Análise jurisprudencial. **Data Venia - Revista Jurídica Digital**, [S.l.], n. 9, pp. 223-250, 2018. http://datavenia.pt/ficheiros/edicao09/datavenia09_p223_250.pdf. Acesso em: 29 de agosto de 2020.

GALVÃO, Luís Neto. Comentário ao artigo 16.º do TFUE. *In:* PORTO, Manuel Lopes; ANASTÁCIO, Gonçalo (Eds.). **Tratado de Lisboa Anotado e Comentado**. Coimbra: Almedina, 2012, pp. 252-256.

GOMES, Francisca Cardoso Resende. O conteúdo do direito fundamental à proteção de dados à luz do novo Regulamento Geral de Proteção de Dados: em especial, a problemática do controlo das decisões automatizadas. **Anuário da Proteção de Dados - 2020**, Lisboa, pp. 105-119, 2020. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2020/07/ANUARIO-2020-Eletronico-compressed.pdf. Acesso em: 29 de agosto de 2020.

GONÇALVES, Maria Eduarda. **Direito da Informação**: novos direitos e formas de regulação na sociedade da informação. 2. ed. Coimbra: Almedina, 2003.

GONÇALVES, Maria Eduarda. The EU Data Protection Reform and the Challenges of Big Data: tensions in the relations between technology and the law. *In:* NETO, Luísa; RIBEIRO, Fernanda (Eds.). **IV Colóquio Luso-Brasileiro Direito e Informação - Atas**. Porto: Faculdade de Letras da Universidade do Porto, pp. 46-63, 2016. Disponível em: https://view.joomag.com/direito-e-informa%c3%a7%c3%a3o-na-sociedade-em-rede-atas-direito-e-informa%c3%a7%c3%a3o-na-sociedade-em-rede-atas/0242499001470686892. Acesso em: 29 de agosto de 2020.

HANOFF, Roberta Volpato; NIELSEN, Thiago Henrique. A Lei Geral de Proteção de Dados Pessoais na administração pública brasileira: é possível implementar governança de dados antes de se implementar a governança em gestão? *In:* DAL POZZO, Augusto Neves; MARTINS, Ricardo Marcondes (Coords.). **LGPD & Administração Pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020, pp. 391-406.

KLEE, Antonia Espíndola Longoni; MARTINS, Guilherme Magalhães. A privacidade, a proteção dos dados e dos registros pessoais e a liberdade de expressão: algumas reflexões sobre o Marco Civil da Internet no Brasil (Lei nº 12.965/2014). *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coords.). **Direito & Internet III**: Marco Civil da Internet (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. I, pp. 291-368

LEAL, Ana Alves. 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:* CORDEIRO, António Menezes, OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech**: Desafios da Tecnologia Financeira. Coimbra: Almedina, 2017, pp. 75-202.

LONGHI, João Victor Rozatti. Marco Civil da Internet no Brasil: breves considerações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.). **Direito digital**: direito privado e internet. 3. ed. Indaiatuba: Foco, 2020, pp. 115-144.

LOPES, Teresa Vale. Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. **Anuário da Proteção de Dados - 2018**, Lisboa, pp. 45-69, 2018. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf. Acesso em: 29 de agosto de 2020.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *In:* DONEDA, Danilo; MACHADO, Diego (Coords.). **A criptografia no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, pp. 137-164.

MARQUES, João. Direito ao Esquecimento – A Aplicação do Acórdão Google pela CNPD. **Fórum de Proteção de Dados**, Lisboa, n. 3, pp. 44-55, 2016. Disponível em: https://www.cnpd.pt/bin/revistaforum/forum2016_3/files/assets/basic-html/page-48.html. Acesso em: 29 de agosto de 2020.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. A anonimização de dados pessoais: consequências jurídicas do processo de reversão, a importância da entropia e sua tutela à luz da Lei Geral de Proteção de Dados. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (Coords.). **Direito & Internet IV**: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019, pp. 51-80.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Compliance digital e responsabilidade civil na Lei Geral de Proteção de Dados. *In:* MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coords.). **Responsabilidade civil e novas tecnologias**. Indaiatuba: Foco, 2020, pp. 263-297.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Segurança, boas práticas, governança e compliance. *In:* LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020, pp. 349-372.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura. Porta lógica, IP e os registros de acesso a aplicações da Internet: Uma leitura ampliativa do art. 5º, VIII do Marco Civil da Internet. **Jota**, 26 dez. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/porta-logica-ip-e-os-registros-de-acesso-a-aplicacoes-da-internet-26122019. Acesso em: 29 de agosto de 2020.

MARTINS, José C. Lourenço. Método de Design, Implementação e Operação de um Sistema de Gestão de Segurança da Informação (V1.0). **Proelium – Revista Científica da Academia Militar**, Lisboa, A. VIII, n. 4, 2019. Disponível em: https://www.academia.edu/40439061/M%C3%A9todo_de_Design_Implementa%C3%A7%C3%A3

o_e_Opera%C3%A7%C3%A3o_de_um_Sistema_de_Gest%C3%A3o_de_Seguran%C3%A7a_da_Informa%C3%A7%C3%A3o_V1_0_. Acesso em: 29 de agosto de 2020.

MARTINS, José C. Lourenço [*et al*.]. Modelo Integrado de Atividades para a Gestão da Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais. **Cyberlaw by CIJIC - Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**, Lisboa, n. 5, 2018. Disponível em: https://www.cijic.org/wp-content/uploads/2018/03/MODELO-INTEGRADO-DE-ATIVIDADES-PARA-A-GEST%C3%83O-DE-SEGURANCA-DA-INFORMACAO-CIBERSEGURANCA-E-PROTECCAO-DE-DADOS.pdf. Acesso em: 29 de agosto de 2020.

MASSENO, Manuel David. On the relevance of big data for the formation of contracts regarding package tours or linked travel arrangements, according to the new package travel directive. **Comparazione e Diritto Civile**, Salerno, n. 4, pp. 2-13, 2016. Disponível em: http://www.comparazionedirittocivile.it/download/volumi/201604.pdf. Acesso em: 29 de agosto de 2020.

MASSENO, Manuel David. Como a União Europeia procura proteger os cidadãos-consumidores em tempos de *Big Data*. **Revista Eletrônica do Curso de Direito da UFSM**, Santa Maria, v. 14, n. 3, pp. 1-27, 2019. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/41708. Acesso em: 29 de agosto de 2020.

MASSENO, Manuel David. Na borda: dados pessoais e não pessoais nos dois Regulamentos da União Europeia. **Cyberlaw by CIJIC - Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**, Lisboa, n. 9, 2020. Disponível em: https://www.cijic.org/wp-content/uploads/2020/04/II_Na-Borda_Dados-Pessoais-e-nao-Pessoais-nos-2-regulamentos-da-UE_MDMasseno.pdf. Acesso em: 29 de agosto de 2020.

MASSENO, Manuel David; SANTOS, Cristiana Teixeira. Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations. **MediaLaws – Rivista di Diritto dei Media**, Milão, n. 2, pp. 251-266, 2018. Disponível em: http://www.medialaws.eu/rivista/assuring-privacy-and-data-protection-within-the-framework-of-smart-tourism-destinations/. Acesso em: 29 de agosto de 2020.

MASSENO, Manuel David; SANTOS, Cristiana Teixeira. Personalization and Profiling of Tourists in Smart Tourism Destinations – a Data Protection perspective. **Revista Argumentum**, Marília, v. 20 n. 3, pp. 1215-1240, 2019. Disponível em: http://ojs.unimar.br/index.php/revistaargumentum/article/view/1243. Acesso em 29 de agosto de 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo: Revista dos Tribunais, v. 120, p. 468-486, nov./dez. 2018.

MENKE, Fabiano. A criptografia e a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). *In:* DONEDA, Danilo; MACHADO, Diego (Coord.). **A criptografia no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019, p. 123-136.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, São Paulo, v. 1009, p. 173-222, nov. 2019.

MOTA, Joana. Proteção de dados desde a conceção e por defeito. Avaliação de impacto e segurança. *In:* CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). **FinTech II**: Novos Estudos sobre Tecnologia Financeira. Coimbra: Almedina, 2019, pp. 129-146.

MOUTINHO, José Lobo. Legislador português precisa-se. Algumas notas sobre o regime sancionatório no Regulamento Geral sobre Protecção de Dados (Regulamento (UE) 2016/679). **Fórum de proteção de dados**. Lisboa, n. 4, pp. 40-57, 2017. Disponível em: https://www.cnpd.pt/bin/revistaforum/forum2017_1/files/assets/basic-html/page-40.html. Acesso em: 29 de agosto de 2020.

MOUTINHO, José Lobo; RAMALHO, David Silva. Notas sobre o regime sancionatório da proposta de regulamento geral sobre a protecção de dados do Parlamento Europeu e do Conselho. **Fórum de proteção de dados**. Lisboa, n. 1, pp. 18-33, 2015. Disponível em: https://www.cnpd.pt/bin/revistaforum/forum2015_1/files/assets/basic-html/page-20.html. Acesso em: 29 de agosto de 2020.

NORI, Fabio. A guarda dos registros de conexão e dos registros de acesso às aplicações no Marco Civil. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coords.). **Direito & Internet III**: Marco Civil da Internet (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015, t. II, pp. 169-190.

PEREIRA, Alexandre L. Dias. A Proteção de Dados Pessoais e o Direito à Segurança Informática no Comércio Eletrónico. **Banca, Bolsa e Seguros**, Coimbra, n.º 3, pp. 303-329, 2018. Disponível em: https://www.fd.uc.pt/bbs/wp-content/uploads/2019/01/bbs3_final_2p.pdf. Acesso em: 29 de agosto de 2020.

PEREIRA, Bruno; ORVALHO, João. Avaliação de Impacto sobre a Protecção de Dados. **Cyberlaw by CIJIC - Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**. Lisboa, n. 7, 2019. Disponível em: https://www.cijic.org/wp-content/uploads/2019/05/Bruno-Pereira-e-Joao-Orvalho_RGPD_Avalia%C3%A7%C3%A3o-de-Impacto-sobre-a-Prote%C3%A7%C3%A3o-de-Dados.pdf. Acesso em: 29 de agosto de 2020.

PICA, Luís. As Avaliações de Impacto, o Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais. **Cyberlaw by CIJIC - Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**, Lisboa, n. 5, 2018. Disponível em: https://www.cijic.org/wp-content/uploads/2018/03/3_AS-AVALIA%C3%87%C3%95ES-DE-IMPACTO-O-ENCARREGADO-DE-DADOS-PESSOAIS-E-A-CERTIFICA%C3%87%C3%83O-NO-NOVO-REGULAMENTO-EUROPEU-DE-PROTE%C3%87%C3%83O-DE-DADOS-PESSOAIS.pdf. Acesso em: 29 de agosto de 2020.

PINHEIRO, Alexandre Sousa. **Privacy e protecção de dados pessoais**: a construção dogmática do direito à identidade informacional. Lisboa: AAFD, 2015.

PINHEIRO, Alexandre Sousa. Apresentação do Regulamento (UE) 216/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 – Regulamento Geral de Proteção de Dados (RGPD). **Revista do Centro de Estudos Judiciários**, Lisboa, n. 1 pp. 303-327, 2018.

PINHEIRO, Alexandre Sousa. Artigo 4.º - Definições. *In:* PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados**. Coimbra: Almedina, 2018, pp. 115-204.

PINHEIRO, Alexandre Sousa; GONÇALVES, Carlos Jorge. Artigo 22.º - Decisões automatizadas, incluindo definição de perfis. *In:* PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados.** Coimbra: Almedina, 2018, pp. 386-390.

PINHEIRO, Alexandre Sousa; GONÇALVES, Carlos Jorge. Artigo 45.º - Transferências com base numa decisão de adequação. *In:* PINHEIRO, Alexandre Sousa (Ed.). **Comentário ao Regulamento Geral de Proteção de Dados.** Coimbra: Almedina, 2018, pp. 504-512.

SAIAS, Marco Alexandre. Reforço da responsabilização dos responsáveis pelo tratamento de dados. **Revista Luso-Brasileira de Direito do Consumo**, Curitiba, n. 27, pp. 72-90, 2017.

SANTOS, Luísa A. Inácio Varandas dos; MARQUES, Mário R. Monteiro. Gestão de Risco Aplicada à Segurança da Informação. **Cyberlaw by CIJIC – Revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa**. Lisboa, n. 7, 2019. Disponível em: https://www.cijic.org/wp-content/uploads/2019/05/Luisa-Santos-e-Mario-Marques_GEST%C3%83O-DE-RISCO-APLICADA-%C3%80-SEGURAN%C3%87A-DA-INFORMA%C3%87%C3%83O.pdf. Acesso em: 29 de agosto de 2020.

SILVEIRA, Alessandra; MARQUES, João. Do direito a estar só ao direito ao esquecimento. Considerações sobre a proteção de dados pessoais informatizados no Direito da União Europeia: sentido, evolução e reforma legislativa. **Revista da Faculdade de Direito da UFPR**. Curitiba, v. 61, n. 3, pp. 91-118, 2016. Disponível em: https://revistas.ufpr.br/direito/article/view/48085/29828. Acesso em: 29 de agosto de 2020.

TORBAY, Augusto César. A anonimização enquanto mecanismo de proteção de dados pessoais à luz da atual conjuntura legislativa europeia. **Anuário da Proteção de Dados - 2020**, Lisboa, pp. 49-78, 2020. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2020/07/ANUARIO-2020-Eletronico-compressed.pdf. Acesso em: 29 de agosto de 2020.

TRINDADE, Beatriz Santiago. Two years in: Does the GDPR already need updates? A question brought by algorithmic decision-making. **Anuário da Proteção de Dados - 2020**, Lisboa, pp. 79-103, 2020. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2020/07/ANUARIO-2020-Eletronico-compressed.pdf. Acesso em: 29 de agosto de 2020.