Revista do Direito

https://online.unisc.br/seer/index.php/direito/index
ISSN on-line: 1982 - 9957
DOI: 10.17058/rdunisc.v3i50.14819

A SEGURANÇA DOS DADOS NA LGPD, BRASILEIRA: UMA PERSPETIVA EUROPEIA, DESDE PORTUGAL

DATA SECURITY AT LGPD, BRAZILIAN: A EUROPEAN PERSPECTIVE, FROM PORTUGAL

Manuel David Masseno[1]

Recebido em: 02/03/ 2020
Aceito em: 15/07/2020

mdmasseno@gmail.com

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 perspetiva externa, a do Regulamento Geral sobre a Proteção de Dados, da União Europeia, o qual tem sido considerado como sua matriz. Atendendo à proximidade juscultural, as referências assentam na Doutrina portuguesa especializada.

Palavras-chave: Brasil. Dados Pessoais. Regulação. Segurança. União Europeia.

Abstract: This paper addresses, critically, each one of the main issues regarding the intrinsic security of data processing according to the Brazilian General Law on Personal Data Protection, from an external point of view, the General Data Protection Regulation, of the European Union, deemed to be its matrix. Having in mind the closeness of the Legal Cultures, the references are based on the Portuguese specialized Jurisprudence.
Keywords: Brazil. Personal data. Regulation. Safety. European Union.

1. INTRODUÇÃO - A LGPD e o RGPD – a modo de pré-entendimento… conclusivo

Como ponto de partida, não podemos deixar de constatar como a Lei n.º 13.709, de 14 de agosto de 2018, a Lei Geral sobre Proteção de Dados – LGPD, tem sido reiteradamente exposta como sendo uma espécie de projeção tropicalizada 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.2

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, sobretudo devida a uma muito forte pressão midiática. Assim, 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, com uma disciplina geral e uma implementação

[1] Instituto Politécnico de Beja – IPBeja - Beja – Baixo Alentejo – Portugal.

[2] Mesmo apenas em Portugal, os trabalhos dedicados ao *Regulamento* começam a somar-se. Assim e no que se refere a abordagens gerais, são de apontar desde os trabalhos iniciais de Catarina Sarmento e CASTRO (2016), de Angelina TEIXEIRA (2016), de Jorge Barros MENDES (2017) e de Mafalda Miranda BARBOSA (2017), até às sínteses de Sónia MOREIRA (2018) e de Alexandre Sousa PINHEIRO (2018 a), podendo também ter algum interesse o meu estudo com Cristiana Teixeira SANTOS (2018), assim como, e sobretudo, o *Comentário* coordenado por Alexandre Sousa PINHEIRO (2018) e ainda o recentíssimo *Manual* de A. Barreto Menezes Cordeiro (2020).

também feita através de autoridades administrativas independentes, o Brasil escolheu seguir o segundo.

Porém, se assim será em termos gerais, ao descermos ao nível do estudo de cada um dos institutos que enformam a LGPD, metaforicamente falando "do bosque para cada árvore", verificamos como a proximidade é mais aparente do que real. Inclusive é viável identificar um padrão comum, o da menor consideração dos interesses, e dos correspondentes direitos, das pessoas físicas, relativamente aos das organizações, mormente se tratando de Instituições Públicas.

A meu ver, 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 (Art.s 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" (Art.s 5 XVI, 7 III, 9 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.

A isto acresce a previsão de uma "Autoridade Nacional de Proteção de Dados - ANPD, enquanto órgão da administração pública federal, na esfera da Presidência da República" (Art. 55-A, mesmo após a referida Lei n.º 13.853), consequentemente, sem garantias de independência, apesar de ter ficado "assegurada [sua] autonomia técnica e decisória" (Art. 55-B, ainda segundo a mesma Lei).

Em ambos os institutos, verificamos que a LGPD se afasta tanto do regime aplicável às "decisões individuais automatizadas, incluindo [a] definição de perfis" (Art.ºs 4.º 4) e 22.º)3 quanto do estatuto garantido às "autoridades de controlo" (Art.ºs 51.º e 52.º)4, ao ponto de só a segunda

[3] Quanto a esta questão, uma das mais delicadas e controvertidas no que se refere ao emprego da Inteligência Artificial no domínio do tratamento de dados pessoais, são de atender as referências de Catarina Sarmento e CASTRO (2016), assim como os estudos de José Afonso FERREIRA (2018), de Gabriela CALDAS (2019) e de Madalena Perestrelo de OLIVEIRA (2019), bem como o comentário de Alexandre Sousa PINHEIRO e Carlos Jorge GONÇALVES (2018 a), e as referências de A. Barreto Menezes CORDEIRO (2020, pp. 148-149); e, especificamente, além da abordagem de Ana Alves LEAL (2017), esta centrada no Setor Financeiro, aponto a minha abordagem no que se refere às viagens (2016) e o meu trabalho com Cristiana Teixeira SANTOS (2019), a propósito da proteção dos turistas enquanto cidadãos e consumidores. Sobre estas questões, são ainda fundamentais as *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*, do Grupo de Trabalho do Artigo 29.º [GT 29, o qual antecedeu o atual CEPD – Comité Europeu para a Proteção de Dados], adotadas em 3 de outubro de 2017 (Com a última redação revista e adotada em 6 de fevereiro de 2018.

[4] A este propósito, mormente, relevam as considerações de Filipa Urbano CALVÃO (2015), ainda que proferidas antes da adoção do RGPD, assim como os comentários breves de Alexandre Sousa PINHEIRO (2018 c) e (2018 d), o apontamento contextualizado de João Ferreira PINTO (2018) e, ainda, a abordagem de A. Barreto Menezes CORDEIRO (2020, pp. 397-402).

discrepância ser suscetível de impedir a consideração do Brasil enquanto destino de dados pessoais tratados na União Europeia sem autorizações específicas (Art.ºs 44.º e 45.º, 1 e 2 alínea b)5.

Quanto à disciplina da Segurança dos Dados e desde já, podemos antecipar que este padrão se confirma, com uma maior consideração dos interesses das organizações, públicas ou privadas, em detrimento dos direitos dos cidadãos, enquanto titulares dos dados.

Mas, para podermos 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 carácter 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 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)6, 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 final7.

Enquanto a LGPD é uma novidade, ainda que relativa, se formos rigorosos. Com efeito, já vigorava o, dito, "Marco Civil da Internet", aprovado pela Lei n.º 12.965, 23 de abril de 2014, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil8, incluindo diversas questões relativas à proteção de dados pessoais (Art.s 3, II e II, 7, VII, VIII e X, 11, 14 e 14),

[5] Para estas matéria e em termos gerais, temos os estudos de Inês O. Andrade de JESUS (2018) e, sobretudo, de Ricardo Rodrigues de Oliveira (2018), assim como o comentário de Alexandre Sousa PINHEIRO e Carlos Jorge GONÇALVES (2018 b).

[6] Para uma melhor compreensão quanto à origem e à relevância destas Fontes, são sobretudo de atender os trabalhos de Maria Eduarda GONÇALVES (2003, pp. 88-97), e de Catarina Sarmento e CASTRO (2005, pp. 39-45) e, bem assim, de Alexandre Sousa PINHEIRO (2015, pp. 528-546 e 573-661) e Alessandra SILVEIRA e João MARQUES (2016); além dos comentários aos referidos preceitos do *Tratado sobre o Funcionamento da União Europeia*, de Luís Neto GALVÃO (2012), e da *Carta dos Direitos Fundamentais da União Europeia*, por Catarina Sarmento e CASTRO (2013).

[7] Sobre este Acórdão, cuja importância não poderá nunca ser desvalorizada, contamos com as reflexões, ainda "a quente", de Sofia Vasconcelos CASIMIRO (2014), a que se juntaram os estudos de Filipa Urbano CALVÃO (2015), de João MARQUES (2016) e de Catarina Sarmento e CASTRO (2016), assim como as considerações mais recentes de Catarina Santos BOTELHO (2017), de Maria de Fátima GALANTE (2018) e ainda de Rui P. Coutinho de Mascarenhas ATAÍDE (2019).

[8] Daí, no que se refere à proteção de dados, a correspondência será com a Diretiva relativa à privacidade e às comunicações eletrónicas (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, tal como alterada pela Diretiva 2009/136/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009), a qual está em vias de ser substituída pelo Regulamento relativo à privacidade e às comunicações eletrónicas (Proposta de Regulamento relativo ao respeito pela vida privada e à proteção dos dados pessoais, COM(2017) 10 final, de 10 de janeiro de 2017), sobre o qual aponto as referência presentes no meu estudo com Cristiana Teixeira SANTOS (2019).

regulamentado pela 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, legis ou iuris.

Adicionalmente, também o Código de Defesa do Consumidor, aprovado pela Lei n.º 8.078, de 11 de setembro de 1990, e a Lei de Acesso a Informações Públicas, resultante da Lei n.º 12.527, de 18 de novembro de 2011, contêm regras sobre dados pessoais, a serem articuladas sistematicamente com a LGPD e o "Marco Civil".

No entanto, a Constituição Federal, de 1988, apenas trata da matéria de um modo fragmentário e indireto, além do habeas data (Art. 5 LXXII), só consta o direito ao respeito pela vida privada (Art. 5 X)9.

Enquanto no que se refere à Jurisprudência, para ficarmos pelo assunto correspondente ao Acórdão Google Spain, há a apontar as decisões do Superior Tribunal de Justiça no Caso Xuxa (REsp n.º 1.316.921/RJ, de 26 de junho de 2012), que se consolidou também nos Tribunais de Justiça, salvo nos do Rio de Janeiro e de São Paulo, a qual foi superada quando a "alternativa europeia" se tornou prevalecente (REsp n.º 1.660.168/RJ, de 8 de maio), ao prevalecer o voto do Ministro Marco Aurélio Bellize sobre o da Ministra Fátima Nancy Andrighi.

2. UM OBJETIVO COMUM: A SEGURANÇA NO TRATAMENTO DOS DADOS PESSOAIS

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

[9] Entretanto, a 2 de julho de 2019, foi aprovada, em segunda votação, pelo Senado Federal a 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", cujo primeiro subscritor é o Senador Eduardo Gomes (MDB-TO).

[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

> "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)11.

Designadamente e em relação ao nosso objeto de estudo, este princípio tem como corolários os regimes da responsabilidade (civil12, Art.º 82.º, contraordenacional [administrativa]13, 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 abordaremos em seguida.

---

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 PEREIRA (2018), de Teresa Vale LOPES (2018), de Joana MOTA (2019) e, sobretudo, de A. Barreto Menezes CORDEIRO (2020, pp. 326-335 e 346-347).

[11] Consequentemente, "Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas. Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares [físicas]." (*Considerando* 74). Este princípio de *accountability* havia sido já objeto do Parecer 3/2010 do GT 29, sobre o "princípio da responsabilidade", adotado em 13 de julho de 2010, e, no que se refere ao seu conteúdo, podemos referir os estudos de Mafalda Miranda BARBOSA (2018) e de Teresa Vale LOPES (2018), assim como as considerações de Joana MOTA (2019) e de A. Barreto Menezes CORDEIRO (2020, pp. 161-163 e 323-325), além das Alexandre Sousa PINHEIRO (2018 b).

[12] A propósito da mesma, são de referir os estudos de Mafalda Miranda BARBOSA (2017), de A. Barreto MENEZES CORDEIRO (2018), retomadas em A. Barreto Menezes CORDEIRO (2020, pp. 381-396), e de Tiago Branco da Costa (2019),além das referências de Marco Alexandre SAIAS (2017) e do comentário de Cristina Pimenta COELHO (2018 a).

[13] 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, temos as referências prospetivas de Catarina Sarmento e CASTRO (2016), assim como as iniciais de Marco Alexandre SAIAS (2017), além da análise de José Lobo MOUTINHO e David Silva RAMALHO (2017), depois retomada por José Lobo MOUTINHO (2018) e ainda as considerações de Pedro Miguel FREITAS (2018), sem esquecer o comentário breve de Cristina Pimenta COELHO (2018 b).

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. 6 VII).

Pelo que,

> “Os 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. 49).

e, por isso mesmo,

> “Os 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. 47)

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. 46, caput)

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. 6º X)

Embora a LGPD vá 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. 32).

De igual modo e além de nas regras e medidas de segurança, este princípio tem uma especial importância no concernente às matéria “Da Responsabilidade e do Ressarcimento de Danos” (Art.s 42 a 44) e das “Sanções Administrativas” (Art.s 52 a 54).

3. AS REGRAS DE SEGURANÇA

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 n.ºs 1 e 2 e 32 n.º 1)14, ou de avaliações de impacto (Art.º 35.º), se estiverem reunidos os correspondentes pressupostos15.

O que afasta esta disciplina da prevista pela Diretiva ePrivacy16, 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).

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

[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 (2019), e, desde uma perspetiva jurídica, as considerações de Teresa Vale LOPES (2018), Joana MOTA (2019) e, ainda, de estudo de A. Barreto MENEZES CORDEIRO (2018), cujas conclusões são retomadas em A. Barreto MENEZES CORDEIRO (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 (2018) e as considerações de Teresa Vale LOPES (2018) e Joana MOTA (2019), bem como e sobretudo o estudo de Bruno PEREIRA e João ORVALHO (2019).

[16] A antes mencionada Diretiva relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, em cujos termos "O prestador de um serviço de comunicações eletrónicas publicamente disponível adotará as medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços, se necessário conjuntamente com o fornecedor da rede pública de comunicações no que respeita à segurança da rede. Tendo em conta o estado da técnica e os custos da sua aplicação, essas medidas asseguram um nível de segurança adequado aos riscos existentes. [pelo que] As autoridades nacionais competentes devem ter competência para auditar as medidas tomadas por prestadores de serviços de comunicações eletrónicas acessíveis ao público e para emitir recomendações sobre melhores práticas relativas ao nível de segurança que estas medidas devem alcançar. [enquanto] a Comissão poderá, após consulta da Agência Europeia para a Segurança das Redes e da Informação (ENISA), do Grupo de Proteção das Pessoas no que respeita ao Tratamento de Dados Pessoais instituído nos termos do artigo 29.º da Diretiva 95/46/CE, e da Autoridade Europeia para a Proteção de Dados, aprovar medidas técnicas de execução respeitantes às circunstâncias, ao formato e aos procedimentos aplicáveis aos requisitos de informação e notificação a que se refere o presente artigo. Na aprovação dessas medidas, a Comissão deve envolver todos os interessados, de modo, designadamente, a ser informada sobre os melhores meios técnicos e económicos disponíveis para a aplicação do presente artigo." (Art.º 4.º, n.ºs 1 e 5). Nesta particular, têm interesse as reflexões de Carlos Pinto de ABREU (2018).

[17] Neste particular, temos 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 (2018) e de Teresa Vale LOPES (2018).

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).

Resultando que,

> "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, e devem ter em conta [designadamente, a sua] conformidade com as normas internacionais" (Art.º 16.º n.º 1 alínea e)

Ainda neste âmbito e como referência, temos 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 digitais19 na gestão dos riscos que se colocam à segurança das redes e dos sistemas de informação […]". Designadamente, quando esclarece que

> "As normas internacionais referidas no artigo 16.º, n.º 1, alínea e), da Diretiva (UE) 2016/1148 são normas aprovadas por um organismo internacional de normalização, como referido no artigo 2.º, n.º 1, alínea a), do Regulamento (UE) n.º 1025/2012, do Parlamento Europeu e do Conselho [de 25 de outubro de 2012, relativo à normalização europeia]." (Art.º 2.º n.º 5)

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 pessoais21.

---

[18] A propósito desta disciplina, são de indicar as referências de Alexandre L. Dias PEREIRA (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 Helena CARRAPIÇO e André BARRINHA (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*. (2018) e, ainda mais recentemente, por José C. Lourenço Martins (2019), este tendo já

Por sua vez, na LGPD a abordagem é simétrica, pois se

> "Os 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. 49).

Da mesma resulta que, proativamente,

> "A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput 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 do art. 6º desta Lei." (Art. 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. 55-J, XII).

De este 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. 50, caput).

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

4. OS DADOS PESSOAIS E A LIMITAÇÃO DO SEU TRATAMENTO

em atenção a respetiva articulação com a Norma ISO/IEC 27701:2019, cujo Anexo D estabelece os correspondentes critérios.

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)[22].

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. 5, 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. 5, II) e "Poderão 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. 12 § 2)

A delimitando, negativamente, pela de "dado anonimizado: [enquanto] dado relativo a titular que não possa ser identificado […]" (Art. 5, 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. 14 I).

[22] 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. 5, VIII)]. Até, porque "As 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 (2015), esta ainda durante as negociações do *Regulamento Geral*, e de Mafalda Miranda BARBOSA (2017), tal como o estudo de A. Barreto MENEZES CORDEIRO (2018), cujas conclusões são retomadas em A. Barreto MENEZES CORDEIRO (2020, pp. 107-131), ademais do comentário à definição por parte de Alexandre Sousa PINHEIRO (2018 b).

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"23-24

Assim, no RGPD é enunciado o princípio da «minimização dos dados», já que estes devem ser "Adequados, 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, o que o articula com o princípio da «limitação da conservação», sendo aqueles apenas "Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados […]" (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

[23] Como dá conta explicita o Parecer 3/2013 do GT 29, sobre a "limitação de finalidade", de 2 de abril de 2013, "O termo "Megadados refere-se ao aumento exponencial da disponibilidade e da utilização automatizada de informações: refere-se a conjuntos de dados digitais gigantescos detidos por empresas, governos e outras organizações de grandes dimensões, que são depois extensivamente analisados (daí o nome 'analítica') com recurso a algoritmos informáticos."

[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, temos as referências de Catarina Sarmento e CASTRO (2016), assim como o meu estudo de 2016, no âmbito do Direito Privado, e o de Maria Eduarda GONÇALVES (2016), no do Público, seguidos do de Ana Alves LEAL (2017), podendo ainda indicar a abordagem jurídica interdisciplinar que publiquei em 2019.

[25] Sobre o conteúdos deste(s) princípio(s) são de indicar as referências breves de Alexandre Sousa PINHEIRO (2018 b) e de A. Barreto MENEZES CORDEIRO (2020, pp. 158-131) e ainda as do meu estudo com Cristiana Teixeira SANTOS (2018).

> 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. 6.º, 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. 15, I).

5. 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 a referindo 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].

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 Data28.

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 respetivas 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 sugerida29, 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).

---

[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 (2016), sendo que, logo após a publicação do *RGPD*, esta questão foi identificada e analisada por Ana Alves LEAL (2017), a propósito das implicações da *Big Data*, entretanto, a questão foi enfrentada por A. Barreto MENEZES CORDEIRO (2018), a propósito dos limites da "identificabilidade", retomando-a A. Barreto MENEZES CORDEIRO (2020, pp. 126-131); porém, permito-me remeter para o meu estudo sobre os limites entre ambos os Regulamentos referidos, já publicado em 2020.

[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, "Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa,

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 conceção (Art.º 25.º n.º 1), 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 RGPD30.

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 e define-a como a

---

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".

[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 "Se 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.

> "utilização de meios 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. 5, XI).

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

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. 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. 18 IV), ficando ainda excluída a portabilidade dos dados anonimizados (Art. 18 § 7º).

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. 5, III), o mesmo valendo para a anonimização enquanto processo, como acabámos de ver.

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. 12).

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. 44, Parágrafo único)

a aplicação dos "meios técnicos razoáveis e disponíveis no momento do tratamento", afastará a correspondente ilicitude (Art. 43, III), não torna sequer irregular o tratamento de esses dados, o mesmo é dizer que

> "[…] 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. 44).

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. 52 § 1º, 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. 13 § 4º).

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. 13, caput). Embora podendo empregue em geral, ao ser 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. 6, 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. 46)

Porém, ao não existir uma previsão análoga à anonimização, no que se relativa à determinação de regras técnicas de segurança pela autoridade nacional (Art. 12 §3º), apenas releva o poder genérico de esta dispor "padrões técnicos mínimos", também a este propósito (§ 1º do Art. 46).

Consequentemente, fica mais difícil afastar a ilicitude em caso de incidente de segurança, no que se refere à responsabilidade civil e às sanções administrativas.

6. 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."

Embora, devamos 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 respetivas integridade e disponibilidade32. 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:33.

Já na LGPD a cifragem não é, sequer, mencionada, embora esteja implícita quando refere que

> "No 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. 48 § 3º).

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. 46)

[32] Daí, o caráter cumulativo das medidas de segurança (Art. 32 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).

[33] Como ocorreu, reiteradamente, com a Declaração Conjunta da Europol e da ENISA, de 20 de maio de 2016, sobre "uma investigação criminal lícita que respeite a proteção dos dados no século XXI", a Resolução sobre "a luta contra a cibercriminalidade", do Parlamento Europeu, de 3 de outubro de 2017 (2017/2068(INI) e, mais ainda, a "Declaração sobre a cifragem e o seu impacto na proteção das pessoas singulares [físicas] relativamente ao tratamento dos seus dados pessoais na EU", de 11 de abril de 2018, do GT 29.

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. 48 § 1º, VI, e § 2º, II), por sua natureza, a cifragem é a técnica mais pertinente para prevenir danos maiores, tal como se verifica no RGPD.

REFERÊNCIAS

[34]

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, 2018, pp. 49-78. <http://www.concorrencia.pt/vPT/Estudos_e_Publicacoes/Revista_CR/Documents/Revista_ReC_35.pdf>

ATAÍDE, Rui P. Coutinho de Mascarenhas. Direito ao esquecimento. Cyberlaw by CIJIC. Lisboa, n. 6, 2019. <https://www.cijic.org/wp-content/uploads/2019/05/Rui-Ata%C3%ADde_Direito-esquecimento.pdf>

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, 2017, pp. 75-131. <https://www.fd.uc.pt/cdc/pdfs/rev_12_completo.pdf>

BARBOSA, Mafalda Miranda. Data controllers e data processors: da responsabilidade pelo tratamento de dados à responsabilidade civil. Revista de Direito Comercial. Lisboa, n. 2, 2018, pp. 424-494. <https://www.revistadedireitocomercial.com/data-controllers-e-data-processors>

BOTELHO, Catarina Santos. Novo Ou Velho Direito? – o direito ao esquecimento e o princípio da proporcionalidade no constitucionalismo global. AB INSTANTIA. Coimbra, n. 7, 2017, pp. 49-71. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3130258>

CALDAS, Gabriela. O direito à explicação no Regulamento Geral sobre a Proteção de Dados. Anuário da Proteção de Dados. Lisboa, 2019, pp. 37-53. <http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf>

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

CALVÃO, Filipa Urbano. O modelo de supervisão de tratamento de dados pessoais na União Europeia: da atual diretiva ao futuro regulamento. Fórum de Proteção de Dados, Lisboa, n. 1, 2015, pp. 36-48. <https://www.cnpd.pt/bin/revistaforum/forum2015_1/index.html#36>

[34] Todas as hiperconexões foram verificadas no dia 3 de fevereiro de 2020.

CARRAPIÇO, Helena; BARRINHA, André. European Union cyber security as an emerging research and policy field. London, European Politics and Society, Vol. 19, n. 3, 2018, pp. 299-303. <https://www.tandfonline.com/doi/full/10.1080/23745118.2018.1430712>

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

CASTRO, Catarina Sarmento e. Direito da Informática, Privacidade e Dados Pessoais. Coimbra, Almedina, 2005.

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

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. Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos, Vol. I. Coimbra, Almedina, 2016, pp. 1047-1070.

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 (a), pp. 633-37.

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 (b), pp. 637-647.

COELHO, Cristina Pimenta. Artigo 84.º - Sanções. In PINHEIRO, Alexandre Sousa (Ed.). Comentário ao Regulamento Geral de Proteção de Dados. Coimbra, Almedina, 2018 (c), pp. 648-650.

CORDEIRO, A. Barreto Menezes. Dados pessoais: conceito, extensão e limites. Revista de Direito Civil. Coimbra, Vol. 3 n. 2, 2018 (a), pp. 297-321. <https://blook.pt/publications/publication/e38a9928dbce/>

CORDEIRO, A. Barreto Menezes. Da responsabilidade civil pelo tratamento de dados pessoais – Working paper. Lisboa, BLOOK, 2018 (b). <https://blook.pt/publications/publication/2ae6399f13bb/>

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. <http://repositorium.sdum.uminho.pt/bitstream/1822/61446/3/UNIO_EBOOK_INTEROP_2019.pdf>

FERREIRA, Afonso José. Profiling e algoritmos autónomos: um verdadeiro direito de não sujeição. Anuário da Proteção de Dados. Lisboa, 2018, pp. 35-43. <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>

FREITAS, Pedro Miguel. The General Data Protection Regulation: an overview of the penalties' provisions from a Portuguese standpoint. UNIO - EU Law Review. Braga, Vol. 4 n. 2, 2018, pp. 99-104.
<http://www.unio.cedu.direito.uminho.pt/Uploads/UNIO%204%20.%20Vol%201/Unio%204%20n.%202%20PT/Unio%204%20n.%202%20EN/Pedro%20Miguel%20Freitas%20(1).pdf>

GALANTE, Maria de Fátima. A Internet e o Direito ao Esquecimento: Análise jurisprudencial. Data Venia - Revista Jurídica Digital. S.l, n. 9, 2018, pp. 223-250. <http://datavenia.pt/ficheiros/edicao09/datavenia09_p223_250.pdf>

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.

GONÇALVES, Maria Eduarda. Direito da Informação: novos direitos e formas de regulação na sociedade da informação. Coimbra, Almedina, 2 Ed., 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, 2016, pp. 46-63. <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>

JESUS, Inês O. Andrade de. O direito à proteção de dados pessoais e o regime jurídico das transferências internacionais de dados: a proteção viaja com as informações que nos dizem respeito? Lisboa, Anuário da Proteção de Dados - 2018, pp. 71-90. <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>

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.

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

MARQUES, João. Direito ao Esquecimento – A Aplicação do Acórdão Google pela CNPD. Fórum de proteção de dados. Lisboa, n. 3, 2016, pp. 44-55. <https://www.cnpd.pt/bin/revistaforum/forum2016_3/files/assets/basic-html/page-48.html>

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. <https://www.academia.edu/40439061/M%C3%A9todo_de_Design_Implementa%C3%A7%C3%A3o_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_>

MARTINS, José C. Lourenço [et al.]. Modelo Integrado de Atividades para a Gestão da Segurança da Informação, Cibersegurança e Proteção de Dados Pessoais. Lisboa, Cyberlaw by CIJIC, n. 5, 2018. <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>

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, 2016, pp. 2-13. <http://www.comparazionedirittocivile.it/download/volumi/201604.pdf>

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, Vol. 14, n. 3. <https://periodicos.ufsm.br/revistadireito/article/view/41708/pdf>

MASSENO, Manuel David. Na borda: dados pessoais e não pessoais nos dois Regulamentos da União Europeia. In MARTINO, Antonio (Ed.). Actas del IV Congreso Interactivo Virtual / Humanos – Máquinas - Derechos (20 y 21 de noviembre / 2019). Buenos Aires, Astrea, 2020. <https://www.astrea.com.ar/resources/doctrina/doctrina0511.pdf>

MASSENO, Manuel David; SANTOS, Cristiana Teixeira. Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations. MediaLaws – Rivista di diritto dei media. Milano, n. 2, 2018, pp. 251-266. <http://www.medialaws.eu/rivista/assuring-privacy-and-data-protection-within-the-framework-of-smart-tourism-destinations/>

MASSENO, Manuel David; SANTOS, Cristiana Teixeira Santos. Personalization and Profiling of Tourists in Smart Tourism Destinations – a Data Protection perspective. Revista Argumentum. Marília, Vol. 20 n. 3, 2019, pp. 1215-1240. <http://ojs.unimar.br/index.php/revistaargumentum/article/view/1243/752>

MENDES, Jorge Barros. O Novo Regulamento de Proteção de Dados: as principais alterações. Revista Luso-Brasileira de Direito do Consumo. Curitiba, pp. 27, 2017, pp. 13-37. <https://issuu.com/editorabonijuris9/docs/revista_luso-brasileira_de_direito__d0959fdb6ee330>

MOREIRA, Sónia. A proteção das pessoas singulares no novo Regulamento Geral de Protecção de Dados Pessoais. In CALHEIROS, Clara [et al.] (Eds.). Direito na Lusofonia: Direito e Novas

Tecnologias / Atas do 5º Congresso Internacional de Direito na Lusofonia. Braga, Escola de Direito Universidade do Minho / Centro de Investigação em Justiça e Governação, 2018, pp. 485-492. <http://repositorium.sdum.uminho.pt/bitstream/1822/59737/1/29-Lusofonia%20V%20RGPD%202018.pdf>

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, 2017, pp. 40-57. <https://www.cnpd.pt/bin/revistaforum/forum2017_1/files/assets/basic-html/page-40.html>

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, 2015, pp. 18-33. <https://www.cnpd.pt/bin/revistaforum/forum2015_1/files/assets/basic-html/page-20.html>

OLIVEIRA, Madalena Perestrelo de. Definição de perfis e decisões individuais automatizadas no Regulamento Geral sobre a Proteção de Dados. In CORDEIRO, António Menezes; OLIVEIRA, Ana Perestrelo de; DUARTE, Diogo Pereira (Eds.). FinTech II - Novos Estudos sobre Tecnologia Financeira. Coimbra, Almedina, 2019, pp. 61-88.

OLIVEIRA, Ricardo Rodrigues de. What´s in a Name? Uma Breve Análise do Nível de Protecção Adequado no Âmbito das Transferências de Dados Pessoais dos Cidadãos da União Europeia para Países Terceiros. Lisboa, Anuário da Proteção de Dados - 2018, pp. 119-145. <http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf>

PEREIRA, Alexandre L. Dias. 2018. A Proteção de Dados Pessoais e o Direito à Segurança Informática no Comércio Eletrónico. Banca, Bolsa e Seguros. Coimbra, n.º 3, 2013, pp. 303-329. <https://www.fd.uc.pt/bbs/wp-content/uploads/2019/01/bbs3_final_2p.pdf >

PEREIRA, Bruno; ORVALHO, João. Avaliação de Impacto sobre a Protecção de Dados. Cyberlaw by CIJIC. Lisboa, n. 7, 2919. <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>

PICA, Luís. As Avaliações de Impacto, o Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais. Lisboa, Cyberlaw by CIJIC, n. 5, 2018. <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>

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). Lisboa, Revista do Centro de Estudos Judiciários, n. 1 (2018 a). pp. 303-327.

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

PINHEIRO, Alexandre Sousa. "Artigo 51.º - Autoridade de controlo". In PINHEIRO, Alexandre Sousa (Ed.). Comentário ao Regulamento Geral de Proteção de Dados. Coimbra, Almedina, 2018 (c), pp. 533-535.

PINHEIRO, Alexandre Sousa. "Artigo 52.º - Independência". In PINHEIRO, Alexandre Sousa (Ed.). Comentário ao Regulamento Geral de Proteção de Dados. Coimbra, Almedina, 2018 (d), pp. 535-539.

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 (a), 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 (b), pp. 504-512.

PINTO, João Ferreira. Autoridades de Controlo Independentes no (Novo) Regulamento Geral (UE) sobre a Proteção de Dados (RGPD): "The Never Never Land"? Lisboa, Cyberlaw by CIJIC, n. 5, 2018 https://www.cijic.org/wp-content/uploads/2018/03/Opiniao_AUTORIDADES-DE-CONTROLO-<INDEPENDENTES-NO-NOVO-REGULAMENTO-GERAL-UE-SOBRE-A-PROTE%C3%87%C3%83O-DE-DADOS.pdf>

SAIAS, Marco Alexandre. Reforço da responsabilização dos responsáveis pelo tratamento de dados. Revista Luso-Brasileira de Direito do Consumo. Curitiba, n.. 27, 2017, pp. 72-90. <https://issuu.com/editorabonijuris9/docs/revista_luso-brasileira_de_direito__d0959fdb6ee330>

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, Vol. 61, n. 3, 2016, pp. 91-118. <https://revistas.ufpr.br/direito/article/view/48085/29828>

SANTOS, Luísa A. Inácio Varandas dos; MARQUES, Mário R. Monteiro. Gestão de Risco Aplicada à Segurança da Informação. Cyberlaw by CIJIC. Lisboa, n. 5, 2019. <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>

SANTOS, Lourenço Noronha dos. Inteligência Artificial e Privacidade. In ROCHA, Manuel Lopes; PEREIRA, Rui Soares. Inteligência Artificial & Direito. Coimbra, Almedina, 2020, pp. 147-159.

TEIXEIRA, Angelina. A Chave para a Regulamentação da Protecção de Dados (Das pessoas singulares). Data Venia - Revista Jurídica Digital. S.l., n. 1, 2016, pp. 6-32. <http://www.datavenia.pt/ficheiros/edicao06/datavenia06_p005-032.pdf>