EDITORIAL ASTREA

*Na borda: dados pessoais e não pessoais nos dois Regulamentos da União Europeia**

Por Manuel David Masseno

"Assistimos a uma nova revolução industrial induzida pelos dados digitais, a informática e a automatização. As atividades humanas, os processos industriais e a investigação conduzem, todos eles, à recolha e ao tratamento de dados numa escala sem precedentes, favorecendo o surgimento de novos produtos e serviços, assim como de novos processos empresariais e metodologias científicas [e] desde que as regras relativas à proteção dos dados pessoais, quando aplicáveis, sejam cumpridas, os dados, uma vez registados, podem ser reutilizados muitas vezes sem perda de fidelidade. Esta geração de valor agregado está no cerne do conceito de cadeia de valor dos dados [tendo sempre presente que]. O direito fundamental à proteção dos dados pessoais aplica-se aos grandes volumes de dados no caso de se tratar de dados pessoais: o seu tratamento tem de respeitar todas as regras aplicáveis em matéria de proteção de dados" (COM/2014/0442 final, de 2 de julho).

1. As referências

Antes de mais, é necessário ter presente que, uma vez operada a *constitucionalização* da Proteção de Dados operada em 2009 com a entrada em vigor do Tratado de Lisboa, com a inclusão da mesma no Tratado sobre o Funcionamento da União Europeia (art. 16) e com a receção da Carta dos Direitos Fundamentais (art. 8) no Direito Primário da União (Ex vi, art. 6 do Tratado da União Europeia), o respetivo microssistema ficou consolidado, ainda que não completo, com a adoção do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/C (Regulamento Geral sobre a Proteção de Dados) o RGPD[1].

Ao mesmo tempo e enquanto ainda decorria o processo legislativo correspondente ao RGPD, a Comissão –presidida por Jean-Claude– *Juncker* avançou com a "Estratégia para o Mercado Único Digital na Europa" (COM/2015/192 final, de 6 de maio), dando continuidade a orientações que vinham da *Comissão* –presidida por José Manuel Durão– Barrosoe constavamda Comunicação "Para uma economia dos dados próspera" (COM/2014/0442 final, de 2 de julho)[2].

---

* Bibliografía recomendada.

[1] Os estudo sobre o RGPD são hoje multidão. Mas, sempre podemos referir os estudos de Angelina Teixeira (2016), de Alfonso Ortega Jiménez e Juan José Gonzalo Domenech (2018) e ainda de Chris Hoofnagle, Bart van der Sloot e Frederik Zuiderveen Borgesius (2019).

[2] Aliás, na sua "Estratégia para o Mercado Único Digital na Europa" a Comissão acentua que "As empresas e os consumidores continuam a não se sentirem suficientemente confiantes para adotar serviços de computação em nuvem transfronteiras para fins de armazenamento ou processamento de dados, devido a preocupações relacionadas com a segurança, o respeito dos direitos fundamentais e a proteção de dados em termos mais gerais. A adoção do Pacote Reforma da Proteção de Dados assegurará que o tratamento de dados pessoais seja regido por regras atualizadas e uniformes em toda a União. No entanto, frequentemente os contratos excluem, ou limitam de forma significativa, a

O que foi explicitado através de uma sua nova Comunicação, "Construir uma Economia Europeia dos Dados" (COM/2017/9 final, de 10 de janeiro), agora centrada na necessidade de avançar com disciplinas para os "dados em bruto", com um especial ênfase na sua portabilidade em todo o Mercado Interno da União[3]. Daí que a Comissão tenha avançado com a *Proposta* (COM/2017/0495 final, de 13 de setembro) do que veio a ser o Regulamento (UE) 2018/1807 do Parlamento Europeu e do Conselho de 14 de novembro de 2018 relativo a um regime para o livre fluxo de dados não pessoais na União Europeia o Regulamento LFD[4].

No entanto e entre outras, voltou a ser colocada questão a necessitar de respostas jurídicas tão robustas quanto possível, a de existir uma borda, mutável de acordo com a evolução das tecnologias, entre os âmbitos de aplicação material de ambos os Regulamentos, isto é, entre os dados pessoais e os dados não pessoais. A determinação dessa borda, e um breve esboço do que fazer, constitui o objeto desta intervenção.

2. Até mesmo nos limites

Para começar, temos que o RGPD "aplica-se ao tratamento de dados pessoais" (art. 2, n° 1), não só a uma "pessoa singular [física] identificada", mas também a uma que venha a ser "identificável", em termos potenciais e através de meios técnicos, incluindo os indiretos[5].

---

responsabilidade contratual do prestador de serviços de computação em nuvem caso os dados deixem de estar disponíveis ou fiquem inutilizáveis, ou dificultam a rescisão do contrato. Isso significa que não existe, de facto, uma portabilidade dos dados. No domínio da proteção de dados, tanto o atual como o futuro quadro legislativo impede as restrições à livre circulação de dados pessoais na União. As restrições à livre circulação de dados por outros motivos não são abordadas. [Pelo que] A Comissão irá propor em 2016 a Iniciativa Europeia 'Livre Circulação de Dados' que aborda a questão das restrições à livre circulação de dados por motivos não relacionados com a proteção de dados pessoais na UE e das restrições injustificadas sobre a localização de dados para fins de armazenamento ou de tratamento. A iniciativa abordará as questões emergentes de propriedade, interoperabilidade, utilizabilidade e acesso aos dados nomeadamente em situações entre empresas, entre empresas e consumidores e dados gerados por máquinas e máquina-a-máquina. Incentivará o acesso aos dados públicos a fim de contribuir para dinamizar a inovação".

[3] Sobre estes documentos e em termos gerais sobre o Mercado Único Digital e por todo, é de atender à exposição de Fernanda Ferreira Dias (2016).

[4] Para uma perspetiva geral do Regulamento LFD, embora tratando essencialmente de outras questões, Pedro De Miguel Asensio (2019).

[5] Ou seja "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" (art. 4, 1). O que incluí os quase-identificadores e os metadados, ao ser certo que, "As pessoas singulares podem ser associadas a identificadores por via eletrónica …tais como endereços IP (protocolo internet) ou testemunhos de conexão (*cookie*) ou outros identificadores como as etiquetas de identificação por radiofrequência" (considerando 30). Diversamente, a propósito da reindentificação de dados pseudonimizados, o RGPD acrescenta que "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

Consequentemente, do RGPD resulta que: “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*).

Por sua vez, o Regulamento LFD veio esclarecer que o mesmo “aplica-se ao tratamento de dados eletrónicos que não sejam dados pessoais” (art. 2, n° 1), entendendo estes “na aceção do artigo 4°, ponto 1, do Regulamento (UE) 2016/679 [o RGPD]” (art. 3, n° 1)[6].

Assim, ao Regulamento Geral sobre Proteção de Dados é conferida uma *vis atractiva*, sempre que não seja possível identificar os dados em presença como, exclusivamente, não pessoais. Pelo que, “No caso de um conjunto de dados compostos por dados pessoais e não pessoais, o presente regulamento aplica-se aos dados não pessoais do conjunto de dados. Caso os dados pessoais e não pessoais de um conjunto de dados estejam indissociavelmente ligados, o presente regulamento não prejudica a aplicação do Regulamento (UE) 2016/679” (art. 2, n° 2 do Regulamento LFD).

3. Mas, afinal, nada é para sempre

No que concerne a distinção que nos ocupa, temos que a diretiva 95/46/CE, que precedeu o Regulamento sobre Proteção de Dados, assentara numa *fictio iuris*, ao abstrair-se da evolução da técnica, ainda que previsível. Daí, na mesma constar que “os princípios da proteção não se aplicam a dados tornados anónimos de modo tal que a pessoa já não possa ser identificável [os quais são, também] conservados sob uma forma que já não permita a identificação da pessoa em causa” (considerando 26).

O que já não ocorre com o RGPD, ao ser assumido que “As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos [e também que] Estes identificadores

---

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).

Neste particular, há ainda que atender ao conteúdo do Parecer 4/2007 sobre o conceito de dados pessoais, de 20 de junho de 2007, do Grupo de Trabalho do 29 [o qual antecedeu o CEPD - Comité Europeu para a Proteção de Dados], 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. Quanto a estas referências, são de atender os estudos, complementares entre si, de Rossana Ducato (2016), de Nadezhda Purtova (2018), de A. Barreto Menezes Cordeiro (2018) e ainda de Lorenzo dalla Corte (2019), inclusive quanto a referências bibliográficas adicionais.

[6] Isto, porque “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. Exemplos concretos de dados não pessoais incluem conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados, os dados relativos à agricultura de precisão que podem ajudar a controlar e a otimizar a utilização de pesticidas e de água ou ainda dados sobre as necessidades de manutenção de máquinas industriais” (considerando 9).

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" (considerando 30).

Por sua vez, o Regulamento LFD é transparente, ao explicitar 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" (considerando 9 *in fine*), o mesmo valendo para os dados originariamente anónimos, por identidade de razão.

Porém, é necessário ter presente que não estamos face a algo verdadeiramente novo. Aliás, as Instituições da União Europeia foram ficando cientes desta realidade, como mostram os Pareceres do Grupo de Trabalho do art. 29.

Assim e num primeiro momento, tal ocorreu a propósito dos riscos para a proteção dos dados dos administrados que poderiam advir da transposição da Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de Novembro de 2003, relativa à reutilização de informações do sector público, designadamente, o Parecer n° 7/2003 sobre a reutilização de informações do setor público e a proteção dos dados pessoais, de 12 de dezembro. A que se seguiu o Parecer n° 6/2013 sobre dados abertos e reutilização de informações do setor público (ISP), de 5 de junho, suscitado pela adoção da Diretiva 2013/37/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, que altera a Diretiva 2003/98/CE relativa à reutilização de informações do setor público[7].

Mas, uma análise detalhada destas questões, tanto desde o ponto de vista técnico quanto numa perspetiva jurídica, constituiu o objeto do Parecer n° 5/2014 sobre técnicas de anonimização, de 10 de abril[8].

Por isso mesmo, algumas autoridades nacionais avançaram com orientações destinadas a mostrar padrões aos respetivos responsáveis pelo tratamento de dados, como no Reino Unido coma ICO - *Information Commissioner's Office*, que aprovou o *Anonymisation: managing data protection risk code of practice*, em novembro de 2012, ou com a *Agencia* Española de Protección de Datos, com as suas *Orientaciones y garantias en los procedimientos de anonimización de datos personales*, de outubro de 2016.

Entretanto ea propósito da entrada em vigor do Regulamento LFD, a Comissão Europeia publicou as suas "Orientações sobre o regulamento relativo a um quadro para o livre fluxo de dados não pessoais na União Europeia" (COM/2019/250 final, de

[7] Sobre esta tensão entre as políticas de dados abertos e a proteção de dados, criticamente, temos também o artigo de Katleen Janssen e Sara Hugelier (2013).

[8] No qual é afirmado, precisamente, que "A anonimização de dados pessoais pode ser uma boa estratégia para manter os benefícios e atenuar os riscos. Quando um conjunto de dados se encontra verdadeiramente anonimizado e as pessoas deixam de ser identificáveis, a legislação europeia de proteção de dados deixa de ser aplicável.

No entanto, estudos de casos e publicações de investigação evidenciam que criar um conjunto de dados verdadeiramente anónimo a partir de um conjunto substancial de dados pessoais mantendo, simultaneamente, as informações subjacentes exigidas para a tarefa não é um desafio simples. Por exemplo, um conjunto de dados considerado anónimo pode ser combinado com outro conjunto de dados de modo a que uma ou mais pessoas sejam passíveis de ser identificadas".

29 de maio), com referências específicas e desenvolvidas quanto a esta questão[9], 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".

Acrescente-se que preocupações idênticas, em especial motivadas pela disponibilização de informações do Setor Público destinadas à sua reutilização por privados num contexto tecnológico de acesso generalizado às analíticas de *Big Data*, enformaram o Anexo II do Relatório de 24 de novembro de 2016 (A/HRC/31/64) do Relator Especial para a Privacidade do Conselho dos Direitos Humanos das Nações Unidas, Joseph A. Cannataci.

Adicionalmente e como resulta também dos documentos antes referidos, diversos estudos académicos foram mostrando as dificuldades de manter distinções claras, consistentes e, mais ainda, irreversíveis entre dados pessoais e dados não pessoais. O que se concretiza na explicitação dos limites das técnicas de anonimização disponíveis em cada momento, assim como nas possibilidades de personalização de dados anónimos ou anonimizados.

A título exemplificativo, logo em 2010 e desde uma perspetiva jurídica, Paul Ohm expôs as insuficiências das técnicas então disponíveis. Entretanto, em julho último, seguindo uma metodologia de natureza matemática, Luc Rocher, Julien M. Hendrickx e Yves-Alexandre de Montjoye demonstraram como a reidentificação de dados anónimos ou anonimizados pode ser alcançada, com níveis muito altos de eficácia e uma relativa facilidade técnica[10].

---

[9] "Todos os dados que não sejam 'dados pessoais', na aceção do Regulamento Geral sobre a Proteção de Dados, são dados não pessoais. Os dados não pessoais podem ser classificados segundo a origem:

· Desde o início - dados originalmente não relacionados com uma pessoa singular identificada ou identificável, tais como dados sobre as condições meteorológicas gerados por sensores instalados em turbinas eólicas ou dados sobre as necessidades de manutenção de máquinas industriais.

· Em segunda fase - dados inicialmente pessoais, mas posteriormente anonimizados. A 'anonimização' de dados pessoais é diferente da pseudonimização (ver supra), uma vez que os dados devidamente anonimizados não podem ser atribuídos a uma determinada pessoa, nem sequer pela utilização de dados adicionais, pelo que se tratam de dados não pessoais.

Aferir da correta anonimização dos dados depende de circunstâncias específicas e únicas de cada caso. Os vários exemplos detetados de reidentificação de conjuntos de dados supostamente anonimizados demonstraram que essa avaliação pode ser exigente. Para determinar se uma pessoa é identificável, é necessário ter em conta todos os meios suscetíveis de serem razoavelmente utilizados por um responsável pelo tratamento ou qualquer outra pessoa para identificar uma pessoa direta ou indiretamente.

No entanto, 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".

[10] Depois das conclusões de Paul Ohm, a questão continuou a sem debatida na doutrina de ambas margens do Atlântico, procurando uma compatibilização, porventura impossível, entre uma tecnologia crescentemente mais poderosa no sentido de viabilizar a repersonalização de dados

4. E “que fazer?”...antes do tratamento de dados, pessoais e não pessoais

Atendendo a este contexto técnico e regulatório, também resultante do Princípio da responsabilidade proativa (*Accountability*)[11] e por força da aplicação dos Princípios e regras constantes do RGPD, o Responsável pelo Tratamento deverá promover a realização de análises de risco, previamente à anonimização de dados pessoais ou aos tratamento de dados não pessoais[12]. O que o afastará de incorrer em qualquer uma das responsabilidades previstas nas tipologias constantes do RGPD em resultado da personalização de dados, mesmo se apenas potencial ou realizada por terceiros[13].

Aliás, embora se nos afigure evidente, deve ficar claro que a anonimização de dados pessoais pressupõe a presença dos inerentes requisitos no que respeita à “Licitude do tratamento” (arts. 6 a 11), assim como a observância dos “Princípios relativos ao tratamento de dados pessoais” (art. 5). O mesmo valendo para a personalização, ou a repersonalização, de dados anónimos ou anonimizados.

Especificamente, deverão ser seguidos os critérios indicados no RGPD a propósito tanto da “Proteção de dados desde a conceção e por defeito [omissão]” (art.

---

anonimizados e as regras pressupondo a correspondente irreversibilidade, sobretudo durante o processo legislativo que culminou na adoção do *Regulamento Geral sobre Proteção de Dados*, ou logo após, como ocorreu com Paul Schwartz e Daniel Solove (2011) e (2014), Samson Esayas (2015) ou ainda com Sophie Stalla-Bourdillon e Alison Knight (2017).

Quanto à utilização de analíticas de *Big Data* para a “definição de perfis” (isto é, uma “qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações”, art. 4, n° 4) do RGPD) e para a personalização, também a partir de dados anónimos ou anonimizados, são de referir os estudos de Benjamin Habegger *et al*. (2014), de Alessandro Mantelero (2016) e de Elena Gil (2016, *maxime* p. 86 a 110) ou, desde uma perspetiva técnica de, Nils Gruschka *et al*. (2018) e ainda o meu trabalho e de Cristiana Teixeira Santos (2019), tal como as reflexões críticas de Lorenzo Cotino Hueso (2017).

[11] Havendo sido objeto do Parecer 3/2010 sobre o princípio da responsabilidade, adotado em 13 de julho de 2010 pelo Grupo de Trabalho do art. 29, o mesmo ficou explicitado n° 2 do art. 5 do RGPD, em cujos termos, “O responsável pelo tratamento é responsável pelo cumprimento do disposto no n° 1 [isto é, pelo cumprimento dos “Princípios relativos ao tratamento de dados pessoais] e tem de poder comprová-lo”, sobre o mesmo, além das considerações de Teresa Vale Lopes (2018) e de Emanuele Lucchini Guastalla (2018), tem muito interesse o recente estudo de Lachlan Urquhart, Tom Lodge e Andy Crabtree (2019).

[12] Isto, porque “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 do RGPD). A propósito das análises de risco neste contexto, em termos gerais, são de referir os estudos de Niels van Dijk, Raphaël Gellert e Kjetil Rommetveit (2016), de Alessandro Mantelero (2017), assim como as considerações de Teresa Vale Lopes (2018).

[13] Como ocorre com o “direito de indemnização e responsabilidade”, objetiva e solidária (art. 82), com as “coimas” [sanções administrativas], que podem atingir montantes muito elevados (arts. 58, n° 1 *i* e 83), e, sendo o caso, com outras “sanções”, designadamente de ordem penal (art. 84). Para uma melhor compreensão destes preceito e por todos, atente-se no estudo Brendan Van Alsenoy, (2017) e na síntese de Pedro Miguel Freitas (2018).

25), em particular no que se refere à "Segurança do tratamento" (art. 32), ou seja, "Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas"[14].

E ainda, se isso resultar da análise de risco ou for necessário por a mesma ser obrigatória para tratamentos de dados pessoais análogos aos pretendidos (art. 35, n° 3)[15], deverá também ser efetuada uma "Avaliação de impacto sobre a proteção de dados", com especial ênfase no acompanhamento da evolução das técnicas de personalização ou de repersonalização de dados anónimos ou anonimizados, isto é, "Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (art. 35, n° 1)[16].

Por outras palavras, essas avaliações devem realizar-se periodicamente ou sempre que se verifique a emergência de novas técnicas neste domínio, não apenas para a anonimização mas também para a personalização[17].

Adicionalmente, o enquadramento de tais tratamentos de dados no âmbito de "um procedimento de certificação aprovado nos termos do artigo 42" (tal como referido no art. 25, n° 3 a propósito da "proteção de dados desde a conceção e por defeito" e no art. 32, n° 2 no que se refere à "segurança do tratamento") poderá assumir uma grande importância para evitar males maiores no que se refere às várias

[14] Quanto ao conteúdo e ao sentido destas previsões, são sobretudo os estudos encomendados pela ENISA - agora, Agência da União Europeia para a Cibersegurança, antes da adopção do *RGPD*, a George Danesis *et al.* (2014) e a Giuseppe D'Acquisto *et al*. (2015), e, depois, a Marit Hansen e Konstantinos Limniotis (2018), sendo ainda de considerar os contributos de Simone Calzolaio (2017), de Lee A. Bygrave (2017), de Irene Kamara (2017), este centrado na definição e aplicação de normas técnicas neste domínio, assim como de Teresa Vale Lopes (2018).

[15] Especificamente, "*a*) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; *b*) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9, n° 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10; ou *c*) Controlo sistemático de zonas acessíveis ao público em grande escala".

[16] A este propósito e em geral, são de assinalar as referências breves de Luís Pica (2018) e as considerações de Teresa Vale Lopes (2018), bem como e sobretudo os estudos de Niels van Dijk, Raphaël Gellert e Kjetil Rommetveit (2016) e de Bruno Pereira e João Orvalho (2019).

[17] Para tanto, cumprirá 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.

responsabilidades nas quais os responsáveis pelos tratamentos podem incorrer, embora não as afastem, pelo menos por inteiro[18].

Neste mesmo sentido, a aprovação de "critérios de certificação", contendo parâmetros objetivos e detalhados quanto às técnicas de anonimização mais robustas, pelo Comité Europeu para a Proteção de Dados, conduzindo a um "Selo Europeu de Proteção de Dados", reveste-seda maior relevância (arts. 42, n° 5, e 70, n° 1)[19].

Sempre a propósito da certificação das técnicas de anonimização e do tratamento de dados anónimos ou anonimizados, ferramentas complementares poderiam resultar donovel "sistema europeu de certificação da cibersegurança", tal como previsto no Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho de 17 abril de 2019 relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n° 526/2013 (Regulamento Cibersegurança)[20]. O que teria consequências, pelo menos no que se refere à segurança no tratamento dos dados, sobretudo perante uma "violação de dados pessoais"[21], com implicações quanto à presença e conteúdo do dever de notificação da mesma aos titulares dos dados (art. 34 do RGPD).

Em especial, estaria em causa uma certificação facultando um "nível de garantia" "substancial"[22] ou, até mesmo, um "alto"[23] (art. 52), relativamente a ameaças por

[18] No que se refere a este regime, atente-se nosestudos de Giovanni María Riccio e Federica Pezza (2018) ede Jorge A. Viguri Cordero (2018), assim como nos apontamentos de Luís Pica (2018) e de Teresa Vale Lopes (2018).

[19] Aliás, essa mesma preocupação já consta, ainda que como referências muitos sintéticas, das Orientações 1/2018 relativas à certificação e à definição de critérios de certificação de acordo com os artigos 42 e 43 do Regulamento (Versão 3.0, de 4 de junho de 2019), adotadas pelo CEPD.

[20] A propósito destas questões, em termos gerais, é de atender aos estudos de Helena Carrapiço e André Barrinha (2017), na expetativa de uma próxima publicação de trabalhos específicos, embora estas questões não sejam novas, como mostra o estudo de Roksana Moore (2013), por exemplo.

[21] Por "Violação de dados pessoais", entende-se "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (art. 4°, 12 do RGPD). No que se refere a esta matéria, é de atender ao conteúdo do muito recente artigo de Stephanie von Maltzan (2019).

[22] "6. Um certificado europeu de cibersegurança que ateste um nível de garantia 'substancial' dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos conhecidos para a cibersegurança e do risco de incidentes e ciberataques levados a cabo por autores com competências e recursos limitados. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público e a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC aplicam corretamente as funcionalidades de segurança necessárias".

[23] "7. Um certificado europeu de cibersegurança que ateste um nível de garantia 'elevado' dá garantia de que os produtos, serviços e processos de TIC objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos de ciberataques sofisticados levados a cabo por autores com competências e recursos significativos. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público, a realização de ensaios para demonstrar que os produtos, serviços ou

parte de terceiros, no sentido de afastar no tempo os riscos resultantes da evolução das tecnologias e da redução dos respetivos custos, pelo menos.

5. E para prevenir responsabilidades, pelo menos em parte

Como acabámos de ver, a minimização dos riscos de incumprimento do RGPD resultantes de personalizações futura de dados anónimos ou anonimizados, de forma a manter até aos limites do possível a liberdade de tratamento dos mesmo, incluindo a respetiva negociação, implica acompanhar de perto a evolução do estado da técnica, assim como da ações das autoridades, de proteção de dados ou de cibersegurança, no que se refere às certificações de ferramentas ou de procedimentos. Porém, os riscos de incumprimento estarão sempre presentes, apenas podendo ser contidos.

No entanto, o procedimento mais eficaz para afastar tais riscos, ainda que inviável em muitos casos, pela própria *natureza das coisas*, passaria pela aplicação da disciplina constante do RGPD a todos os tratamentos de dados, pessoais e não pessoais, pelo menos quando fossem empregues tecnologias como as inerentes à "internet das coisas, a inteligência artificial e a aprendizagem automática" (considerando 9 do Regulamento LFD)[24]. Designadamente e pelo menos, com a cifragem de tais massas de dados, de modo a prevenir as consequências e responsabilidades resultantes de eventuais "violações de dados"[25].

Bibliografia

Alsenoy, Brendan Van (2017), *Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation*, "JIPITEC Journal of Intellectual Property, Information Technology and E-Commerce Law", vol. 7.

Bygrave, Lee A. (2017), *Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements*, "Oslo Law Review", vol. 4, n° 2, p. 105 a 120.

processos de TIC aplicam corretamente as funcionalidades de segurança necessárias, ao nível tecnológico mais avançado, e uma avaliação da sua resistência a atacantes competentes através de ensaios de penetração".

[24] Em síntese, trata-se de observar os "Princípios relativos ao tratamento de dados pessoais" em especial no que se refere à "limitação das finalidades", à "minimização dos dados" e à sua "integridade e confidencialidade" (art. 5, n° 1 *b*, e *c*, e n° 2), de acatar os requisitos de licitude que couberem (arts. 6 a 11), de respeitar pelos "direitos dos titulares dos dados" (arts. 12 a 22), bem como cumprir as obrigações impostas aos responsáveis pelo tratamento (arts. 24 a 39), em especial formulando e seguindo políticas de privacidade (art. 24, n° 2), metodicamente. A este propósito, vejam-se as considerações breves de Lurdes Alves Dias (2018), os artigos de Dag Wiese Schartum (2017) e de Filippo A. Raso (2018), os estudos temáticos realizados por mim e por Cristiana Teixeira Santos (2018) e (2019), e ainda as reflexões críticas de Miguel Moreno Muñoz (2017).

[25] No que se refere à utilização desta técnica no âmbito do RGPD, é de referir o trabalho de Gerald Spindler e Philipp Schmechel (2016), sendo ainda de muito interesse as reflexões contextuais de Samson Esayas (2015).

Calzolaio, Simone (2017), *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, "Federalismi.it Rivista di Diritto Pubblico Italiano, Comparator e Europeo", n° 24, p. 2 a 21.

Carrapiço, Helena - Barrinha, André (2018), *European Union cyber security as an emerging research and policy field*, "European Politics and Society", vol. 19, n° 3, p. 299 a 303.

Corte, Lorenzo dalla (2019), *Scoping personal data: Towards a nuanced interpretation of the material scope of EU data protection law*, "European Journal of Law and Technology", vol. 10, n° 1.

Cotino Hueso, Lorenzo (2017), *Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales*, "Dilemata. Revista Internacional de Éticas Aplicadas", n° 24, p. 131 a 150.

Danesis, George *et al.* (2014), *Privacy and Data Protection by Design from policy to engineering*, ENISA Agência da União Europeia para a Cibersegurança.

D'Acquisto, Giuseppe *et al.* (2015), *Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*, ENISA Agência da União Europeia para a Cibersegurança.

De Miguel Asensio, Pedro A. (2019), *Servicios de almacenamiento y tratamiento de datos: el Reglamento (UE) 2018/1807 sobre libre circulación de datos no personales*, "La Ley. Unión Europea", n° 66, p. 1 a 6.

Dias, Lurdes Alves (2018), *RPGD: Principais Dificuldades e Dúvidas das Organizações e dos Titulares de Dados Pessoais na Adaptação ao Atual Regime*, "Cyberlawby CIJIC", n° 6.

Dias, Fernanda Ferreira (2016), *O Mercado Único Digital Europeu*, "Análise Europeia. Revista da Associação Portuguesa de Estudos Europeus", n° 2, p. 17 a 41.

Dijk, Niels van - Gellert, Raphaël - Rommetveit, Kjetil (2016), *A risk to a right? Beyond data protection risk assessments*, "Computer Law & Security Review", vol. 32, n° 2, p. 286 a 306.

Ducato, Rossana (2016), *La crisi della definizione di dato personale nell'era del web 3.0*, "Quaderni della Facoltà di Giusrisprudenza dell'Università di Trento", n° 26, p. 143 a 178.

Esayas, Samson Yoseph (2015), *The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the "all or nothing" approach*, "European Journal of Law and Technology", vol. 6, n° 2.

Freitas, Pedro Miguel (2018), *The General Data Protection Regulation: an overview of the penalties' provisions from a Portuguese standpoint*, "UNIO EU Law Review", vol. 4, n° 2.

Gil, Elena (2016), *Big data, privacidad y protección de datos*, Madrid, Agencia Española de Protección de Datos, Boletín Oficial del Estado.

Gruschka, Nils *et al.* (2018), *Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR*, Proceedings of the 2018 IEEE International Conference on Big Data, Seattle.

Habegger, Benjamin *et al.* (2014), *Personalization vs. Privacy in Big Data Analysis*, "International Journal of Big Data", n° 1, p. 25 a 35.

Hansen, Marit - Limniotis, Konstantinos (2018), *Recommendations on shaping technology according to GDPR provisions - Exploring the notion of data protection by default*, ENISA Agência da União Europeia para a Cibersegurança.

Hoofnagle, Chris J. - Sloot, Bart van der - Zuiderveen Borgesius, Frederik (2019), *The European Union general data protection regulation: what it is and what it means*, "Information & Communications Technology Law", vol. 28, n° 1, p. 65 a 98.

Janssen, Katleen - Hugelier, Sara (2013), *Open data as the standard for Europe? A critical analysis of the European Commission's proposal to amend the PSI Directive*, "European Journal of Law and Technology", vol. 4, n° 3.

Kamara, Irene (2017), *Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation "mandate"*, "European Journal of Law and Technology", vol. 8, n° 1.

Lopes, Teresa Vale (2018), *Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados*, "Anuário da Proteção de Dados", 2018, p. 45 a 69.

Lucchini Guastalla, Emanuele (2018), *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, "Contratto e Impresa", n° 1, p. 106 a 125.

Maltzan, Stephanie von (2019), *No Contradiction Between Cyber-Security and Data Protection? Designing a Data Protection Compliant Incident Response System*, "European Journal of Law and Technology", vol. 10, n° 1.

Mantelero, Alessandro (2016), *Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection*, "Computer Law & Security Review", vol. 22, n° 2, p. 238 a 255.

— (2017), *Responsabilità e rischio nel Reg. UE 2016/679*, "Le nuove leggi civili commentate", vol. XL, n° 1, p. 144 a 164.

Masseno, Manuel David - Santos, Cristiana Teixeira (2018), *Assuring Privacy and Data Protection within the Framework of Smart Tourism Destinations*, "Media Laws Rivista di diritto dei media", n° 2, p. 251 a 266.

— (2019), *Personalization and profiling of tourists in smart tourism destinations - a data protection perspective*, "International Journal of Information Systems and Tourism", vol. 4, n° 2, p. 7 a 23.

Menezes Cordeiro, A. Barreto (2018), *Dados pessoais: conceito, extensão e limites*, "Revista de Direito Civil", A. 3, n° 2, p. 297 a 321.

Moreno Muñoz, Miguel (2017), *Privacidad y procesado automático de datos personales mediante aplicaciones y bots*, "Dilemata. Revista Internacional de Éticas Aplicadas", n° 24, p. 1 a 23.

Moore, Roksana (2013), *The Case for Regulating Quality within Computer Security Applications*, "European Journal of Law and Technology", vol. 4, n° 3.

Ortega Jiménez, Alfonso - Gonzalo Domenech, Juan José (2018), *Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea*, "Revista de la Facultad de Derecho de la Universidad de la República", n° 44.

Pereira, Bruno - Orvalho, João (2019), *Avaliação de Impacto sobre a Protecção de Dados*, "Cyberlawby CIJIC", n° 7.

Pica, Luís (2018), *As Avaliações de Impacto, o Encarregado de Dados Pessoais e a Certificação no Novo Regulamento Europeu de Proteção de Dados Pessoais*, "Cyberlawby CIJIC", n° 5.

Purtova, Nadezhda (2018), *The law of everything. Broad concept of personal data and future of EU data protection law*, "Law, Innovation and Technology", vol. 10, n° 1, p. 40 a 81.

Raso, Filippo A. (2018), *Innovating in Uncertainty: Effective Compliance and the GDPR*, "Harvard Journal of Law & Technology Digest".

Riccio, Giovanni María - Pezza, Federica (2018), *Certification Mechanism as a Tool for the Unification of the Data Protection European Law*, "Media Laws. Rivista di diritto dei media", n° 1, p. 249 a 260.

Schartum, Dag Wiese (2017), *Intelligible Data Protection Legislation: A Procedural Approach*, "Oslo Law Review", vol. 4, n° 1, p. 48 a 59.

Schwartz, Paul - Solove, Daniel (2011), *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, "New York University Law Review", vol. 86, p. 1814 a 1894.

— (2014), *Reconciling Personal Information in the United States and European Union*, "California Law Review", vol. 102, p. 877 a 916.

Spindler, Gerald - Schmechel, Philipp (2016), *Personal Data and Encryption in the European General Data Protection Regulation*, "JIPITEC Journal of Intellectual Property, Information Technology and E-Commerce Law", vol. 7.

Stalla-Bourdillon, Sophie - Knight, Alison (2017), *Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, "Wisconsin International Law Journal", vol. 34, n° 2, p. 285 a 322.

Teixeira, Angelina (2016), *A Chave para a Regulamentação da Protecção de Dados (Das pessoas singulares)*, "Data Venia. Revista Jurídica Digital", n° 6, p. 6 a 32.

Urquhart, Lachlan - Lodge, Tom - Crabtree, Andy (2019), *Demonstrably doing accountability in the Internet of Things*, "International Journal of Law and Information Technology", vol. 27, n° 1, p. 1 a 27.

Viguri Cordero, Jorge A. (2018), *La certificación en el nuevo Reglamento Europeo de Protección de Datos y Anteproyecto de Ley Orgánica de Protección de Datos*, "El Tiempo de los Derechos", n° 11.