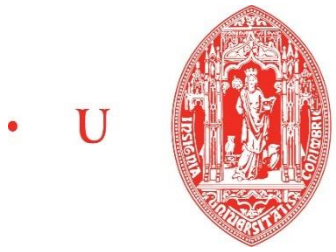
Ana Rita Vaz

O Regulamento Geral de Proteção de Dados: Desafios e Impactos

Dissertação em Ciências Jurídico-Forenses

2018

· U C ·



FDUC FACULDADE DE DIREITO
UNIVERSIDADE DE COIMBRA

O Regulamento Geral de Proteção de Dados: Desafios e Impactos

The General Data Protection Regulation:
Challenges and Impacts

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2.º Ciclo de Estudos em Direito (conducente ao grau de Mestre), na Área de Ciências Jurídico-Forenses

Orientador: Alexandre Dias Pereira

Autora: Ana Rita Francisco Vaz

Coimbra, 2018

Resumo

Encontrando-nos na iminência da aplicação do RGPD, vem-se gerando alguma dúvida e inquietação acerca das suas disposições. A introdução de novos direitos para os titulares, acarreta necessariamente novos deveres para os responsáveis pelo tratamento de dados e subcontratantes. Deste modo, as organizações deverão reconsiderar as suas práticas no âmbito do tratamento de dados pessoais, de modo a garantir a conformidade com este regulamento, por forma a evitar sanções em caso de infração.

Esta dissertação visa analisar o RGPD, confrontando-o com a anterior legislação nacional e europeia, de modo a depreender o impacto positivo e negativo que este terá no quadro jurídico da proteção de dados pessoais. Para isso, são apresentados os conceitos base relativos à proteção de dados, bem como as inovações introduzidas pelo RGPD e as eventuais repercussões que terão.

Palavras-chave: RGPD - dados pessoais - proteção de dados – tratamento de dados – princípios do tratamento – responsável pelo tratamento – titular de dados

Abstract

Along with the impending application of the GDPR, a sense of doubt and concern about its regulations has been growing.

The introduction of new rights for data subjects necessarily brings new obligations for controllers and processors of personal data. Therefore, organizations should reconsider their personal data processing practices in order to ensure compliance with the GDPR, thus avoiding sanctions in case of infringement.

This dissertation aims at analyzing the GDPR by confronting it with the previous national and European legislation with the purpose of perceiving the positive and negative impact that it will have on the personal data protection legal framework. Thus, here are presented the basic data protection concepts as well as the innovations introduced by the GDPR and their presumable repercussions.

Keywords: GDPR - personal data - data protection – data processing – data processing principles – controller – data subject

Siglas e Abreviaturas

CC – Código Civil

CE – Conselho Europeu

CNPD – Comissão Nacional de Proteção de Dados

CRP - Constituição da República Portuguesa

DPIA – Data Privacy Impact Assessment

DPO – Data Protection Officer

EUA – Estados Unidos da América

RGPD – Regulamento Geral de Proteção de Dados

TFUE – Tratado sobre o Funcionamento da União Europeia

TJUE - Tribunal de Justiça da União Europeia

UE – União Europeia

Índice

I. Introdução

Vivendo, hoje, na sociedade da informação, caracterizada pela sua fácil disponibilização e constante partilha, assistimos ao surgimento de novos desafios e ameaças à proteção dos dados pessoais dos cidadãos. Tratando-se, a proteção de dados, de um direito fundamental, é essencial que a legislação que a tutela seja regularmente atualizada e aperfeiçoada.

Esta temática tem vindo a assumir crescente relevância e a despertar a atenção dos cidadãos para a necessidade de salvaguardar a sua privacidade e os seus dados pessoais, na medida em que uma violação destes direitos, nos termos do considerando n.º 85, "pode causar danos físicos, materiais ou imateriais às pessoas singulares como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos", entre outras duras consequências. Ainda assim, há ainda um longo caminho a percorrer no que concerne à formação e consciencialização dos cidadãos para esta problemática.

"O direito à "privacy" foi autonomizado pela primeira vez em 1890, quando Samuel Warren e Louis Brandeis publicaram, na Harvard Law Review, um artigo sob o título "The Right to Privacy"." (CASTRO, 2005, p. 17). Hoje, é tomado pelo nosso ordenamento jurídico como um verdadeiro direito fundamental, positivado nos artigos n.º 26º da CRP e 80º do CC. Por outro lado, nos EUA, ainda se compreende a privacidade segundo a definição de Warren e Brandeis, isto é, como "*the right to be let alone*". Igualmente, o artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia e o artigo 16.º, n.º 1 do TFUE preveem o direito dos cidadãos à proteção dos seus dados pessoais.

O mais recente passo na eterna maratona da proteção de dados é o Regulamento Geral de Proteção de Dados. O RGPD passará a ser aplicado diretamente a partir de 25 de maio de 2018, e substituirá a atual lei de proteção de dados pessoais, a Lei n.º 67/98 de 26 de outubro, bem como a diretiva que esta transpõe, a Diretiva n.º 95/46/CE. Este, no seu capítulo III, atribui aos titulares de dados, um amplo número de direitos, relativos à proteção dos seus dados.

O RGPD assume como fim basilar a supressão das falhas e da insegurança jurídica causadas pela Diretiva 95/46/CE e pela sua heterogénea aplicação nos vários Estados-Membros. Esta ideia de uniformização do regime jurídico da proteção de dados na União, terá fundamentado a opção de elaboração de regulamento, ao invés de diretiva, e, portanto, de aplicação direta nos Estados-Membros, evitando assim as diferenças causadas pelas diversas transposições efetuadas. Ambicionamos, então, que venha a existir uma cooperação eficaz entre as autoridades de controlo dos diversos Estados-Membros.

Este regulamento implementa uma disciplina jurídica mais rígida ao alargar diversos conceitos jurídicos e ao introduzir novos. De entre as novidades apresentadas, destacam-se a figura do DPO e os direitos à portabilidade e ao esquecimento.

A tutela destes direitos gera, naturalmente, obrigações para as entidades que procedem ao tratamento de dados. Em razão disso, algumas destas introduções têm sido objeto de controvérsia, tanto devido ao aumento significativo do nível de tutela da proteção de dados que será exigido às organizações, como devido às múltiplas incongruências e ambiguidades presentes no RGPD.

Este trabalho debruçar-se-á justamente sobre as mais relevantes inovações apresentadas pelo RGPD e visará problematizar o impacto - positivo e negativo - dessas mesmas alterações e suas respetivas imprecisões e ambiguidades, nas práticas das diversas partes afetadas. Com vista a alcançar o fim visado, irei proceder à análise dos principais pontos inovativos do RGPD à luz da atual lei portuguesa da proteção de dados pessoais, clarificando simultaneamente os conceitos relevantes. A conclusão que me proponho a obter será a de compreender se os desígnios ambicionados pelo RGPD poderão ser alcançados através do regime jurídico que implementará ou se o legislador deveria ter optado por caminhos diversos. Para tal, será levada a cabo, uma ampla investigação, recorrendo maioritariamente à pesquisa bibliográfica, mas também à análise documental e da legislação aplicável e participação em conferências.

II. Considerações Introdutórias

1. Cibersegurança na Atual Conjuntura Internacional

Na atual conjuntura, a segurança dos dados pessoais encontra-se sob constante ameaça. Os desafios à cibersegurança são incessantes, estão em permanente atualização e assumem as mais diversas formas, entre elas ataques informáticos diretos, malware e phishing. Estas violações de segurança tanto são dirigidas diretamente aos titulares de dados, como a organizações que a eles têm acesso e resultam na divulgação de dados pessoais que podem ser usados para fins perniciosos e provocar danos gravosos aos titulares[1].

O peso desta ameaça à cibersegurança torna-se ainda mais tenebroso ao observar a omnipresença da internet na vida quotidiana dos cidadãos. Num estudo de 30 de junho de 2017[2], o site Internet Live Stats, reflete que 51.7% da população mundial é utilizadora da internet. "À medida que mais e mais dados são transferidos em formato eletrónico e enviados para os serviços de Internet ou de nuvem, a segurança torna-se mais num problema." (MAMEDE, 2015, p. 93)

Um estudo da Gemalto[3] relativo à primeira metade de 2017, revela números assustadores relativos a incidentes de violação de dados pessoais. É, aí, revelado que uma média de 10,507,550 de registos de dados foram perdidos ou roubados diariamente[4]. Isto significa um aumento significativo de 164% em dados roubados, perdidos ou

[1] No contexto nacional, em 2014, foi criado o Centro Nacional de Cibersegurança (CNCS) que funciona dentro do Gabinete Nacional de Segurança (GNS) e, tal como descrito seu site, "se trata de uma autoridade nacional especialista em matéria de cibersegurança junto das entidades do Estado, operadores de serviços essenciais e prestadores de serviços digitais, garantindo que o ciberespaço é utilizado como espaço de liberdade, segurança e justiça". https://www.cncs.gov.pt/sobre-nos
No Despacho n.º 1348/2017, foi instituída a notificação obrigatória de incidentes de cibersegurança do Serviço Nacional de Saúde (SNS) e do Ministério da Saúde, ao CNCS.

[2] Estudo disponível em: http://www.internetworldstats.com/stats.htm

[3] Estudo disponível em: http://storage.pardot.com/51442/176077/breach_level_index_infographic_h1_2017_gemalto_inforgraphic.jpg

[4] Note-se que a indústria com maior número de incidentes registados foi o setor da saúde com uma percentagem de 25%

comprometidos, relativamente à segunda metade de 2016. Sublinha-se também o facto de menos de 5% destas violações terem sido "*safe breaches*" que consistem naquelas em que a encriptação torna inúteis os dados roubados.

No que à proteção de dados concerne, em países como Inglaterra, França ou Alemanha, a tutela dos dados pessoais já era uma efetiva preocupação tomada em conta pela gestão das empresas. A nível nacional, a realidade parece não ser tão favorável. Um estudo da KPMG de março de 2017[5] concluiu que 85% das organizações inquiridas ainda não começou a implementar medidas efetivas para garantir a conformidade com o RGPD. Apenas que 43% nomearam um DPO que auxilie a aumentar o nível de conformidade com as obrigações legais de proteção de dados pessoais.

Também outro inquérito de maio de 2017[6], elaborado pelo Instituto de Apoio às Pequenas e Médias Empresas e ao Investimento (IAPMEI) e pelas associações para a Promoção e desenvolvimento da Sociedade de Informação (APDSI) e Portuguesa de Gestão das Pessoas (APG), apresenta conclusões algo desagradáveis. Das empresas inquiridas a cerca de um ano da aplicação do RGPD, apenas 3% têm "um plano a decorrer para garantir conformidade com o RGPD", sendo que 44% admitem "não ter qualquer plano" e apenas 22% das respostas acreditam estar "totalmente preparadas" para este regulamento, em maio de 2018. As respostas evidenciam ainda um generalizado desconhecimento do RGPD, com apenas 4,8% dos inquiridos a assumir "conhecer detalhadamente o RGPD e as suas principais obrigações".

Ora, a principal ilação que daqui pode ser retirada será a de que a generalidade das empresas portuguesas ainda não tomou as medidas necessárias e adequadas a garantir a *compliance* com o RGPD, embora se denote que há perceção da dimensão e importância da temática da proteção de dados pessoais.

Com a nova legislação, passamos de um regime de heterorregulação para um de autorregulação. Ou seja, a CNPD vai deixar de fazer controlo prévio e cada responsável

[5] Estudo disponível em: https://assets.kpmg.com/content/dam/kpmg/pt/pdf/pt-2017-rgpd.pdf
[6] Estudo disponível em: https://www.dn.pt/lusa/interior/empresas-portuguesas-pouco-preparadas-para-novas-regras-na-protecao-de-dados---estudo-8505622.html

é que vai ter de controlar se está a cumprir a lei, ao invés de aguardar pela autorização da autoridade. Posto isto, uma vez que o ónus passa para a própria organização, é aconselhável que as empresas iniciem a preparação para a implementação do RGPD considerando que todas estas inovações e exigências terão custos de implementação substanciais.

A realidade prova, assim, que há necessidade de criar e aprimorar a cultura para a cibersegurança[7], por forma a evitar que erros (muitas vezes, triviais) tenham repercussões gravosas.

[7] Um exemplo positivo deste tipo de cultura para a cibersegurança, é a campanha lançada pelo Serviços Partilhados do Ministério da Saúde (SPMS), "Dez mandamentos da Cibersegurança". Disponível em: https://www.tsf.pt/sociedade/saude/interior/ministerio-da-saude-vai-distribuir-dez-mandamentos-da-ciberseguranca-8914995.html

.

2. Evolução do Enquadramento Jurídico

O primeiro instrumento jurídico no qual seria consagrado o direito à privacidade[8] foi a Declaração Universal dos Direitos do Homem de 1948, no seu artigo 12º. Isto embora, o primeiro instrumento jurídico vinculativo a prever este direito tenha sido a Convenção Europeia dos Direitos do Homem de 1950 no seu artigo 8º[9].

No contexto português, "em 1976, o direito à protecção dos dados pessoais foi consagrado na Constituição da República Portuguesa, a qual foi a primeira Constituição do mundo a proteger expressamente os dados pessoais." (JESUS, 2012, p. 1). No art. 35º da CRP está consagrado o direito à autodeterminação informacional, "dando a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em «simples objeto de informações»." (CANOTILHO & MOREIRA, 2014, p. 551). Segundo os mesmos autores, a proteção deste art. 35º reflete-se em três direitos: o direito de acesso e retificação dos registos informáticos; o direito ao sigilo em relação aos responsáveis de ficheiros automatizados e a terceiros e direito à sua não interconexão; e o direito ao não tratamento de certos tipos de dados pessoais.

Em 1991 surge a Lei nº 10/91 - Lei da Proteção de Dados Pessoais face à Informática – que no seu 1º artigo estabelece que "o uso da informática deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada e familiar e pelos direitos, liberdades e garantias fundamentais do cidadão."

[8] Artigo 12.º - "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei."
9 Artigo 8.º, nº 1 – "Qualquer pessoa tem direito ao respeito da sua vida privada e da sua correspondência só podendo haver interferência se estiver em causa a segurança nacional."

Em 1998, é aprovada a Lei n.º 67/98[10], Lei da Proteção de Dados Pessoais, atualmente em vigor, que transpõe a Diretiva n.º 95/46/CE[11] para o ordenamento jurídico português[12].

"Na evolução da proteção jurídica dos dados pessoais o Tribunal de Justiça da União Europeia tem desempenhado um papel hermenêutico muito importante, em diversos acórdãos (e.g. *Lindqvist*, *Google Spain*) fixando jurisprudência de interpretação dos conceitos normativos da Dir. 95/46." (PEREIRA, 2018)

Decorrido o período de transição de 2 anos até à implementação total, o RGPD terá aplicação a partir de 25 de maio de 2018.

[10] "A Lei 67/98 complementada por legislação especial, em especial a lei de informação pessoal e genética (Lei 12/2005) e a lei de acesso aos documentos da administração e à sua reutilização (Lei 26/2016)." (PEREIRA, 2018)

11 Além disto, no que toca à proteção de dados no setor das telecomunicações, surgiu ainda em 1998 a Lei n.º 69/98 que transpôs a Diretiva 97/66/CE e, atualmente, a Lei nº Lei 41/2004, transpondo a Diretiva 2002/58/CE.

12 Com o objetivo de regular o tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e a livre circulação desses dados, surgiu em 2000 o Regulamento 45/2001/EC do Parlamento Europeu e do Conselho

3. Âmbito de Aplicação do RGPD

O RGPD revoga a Diretiva 95/46/CE[13] e é de direta aplicação em todos os Estados-Membros[14], a partir de 25 de maio de 2018, o que significa para as organizações que tratem dados, um período de dois anos de organização e preparação para garantir a conformidade[15]. Este regulamento é aplicável a todas as entidades que efetuem o tratamento de dados pessoais, isto é, que realizem operações que envolvam dados pessoais, incluindo não apenas os responsáveis pelo tratamento[16], como também as que efetuam essas operações em regime de subcontratação, os designados "subcontratantes[17]".

No considerando nº 14, afirma-se que o RGPD tutela "pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais." Não abrange, portanto, o tratamento de dados pessoais relativos a pessoas coletivas. Esta proteção não se aplica, porém, ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas[18], isto é, que não possuam ligação com uma atividade profissional ou comercial. Todavia, é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas, como esclarecido pelo considerando nº18.

Estas disposições são também aplicáveis às atividades dos tribunais e outras autoridades judiciais, como resulta do considerando nº 20. Todavia, não estará sob a

[13] Segundo o considerando nº 171, "as decisões da Comissão que tenham sido adotadas e as autorizações que tenham emitidas pelas autoridades de controlo com base na Diretiva 95/46/CE, permanecem em vigor até ao momento em que sejam alteradas, substituídas ou revogadas."
[14] O caso do *Brexit* levanta a questão da aplicabilidade do RGPD ao Reino Unido. Estima-se que, devido às negociações, o Reino Unido não deverá sair da União até março de 2019. Entretanto, o governo do Reino Unido publicou um *Statement of Intent* comprometendo-se a reforçar e atualizar a legislação de proteção de dados através da elaboração de uma lei de proteção de dados que seja consentânea com o RGPD.
[15] O considerando nº 171 esclarece que "os tratamentos de dados que se encontrem já em curso à data de aplicação do presente regulamento deverão passar a cumprir as suas disposições no prazo de dois anos após a data de entrada em vigor."
[16] *"Controllers",* na versão original em inglês.
[17] "*Processors*", na versão original em inglês.
[18] O considerando nº 18 clarifica: "as atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades."

competência das autoridades de controlo, o tratamento levado a cabo pelos tribunais no exercício da sua função jurisdicional.

A tutela estabelecida por este regulamento é aplicável não somente ao tratamento de dados por meios automatizados, mas também ao tratamento manual, "se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros", nos termos do considerando n.º 15.

Em oposição, os considerandos n.º 16 a 19 estabelecem algumas matérias cujo tratamento de dados não está sujeito ao RGPD, designadamente, questões que se prendem com a política externa e segurança comum da União, atividades pessoais ou domésticas e tratamento para fins de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais[19].

No que respeita à aplicação territorial, o art. 3º clarifica que se aplica ao tratamento de dados levado a cabo no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante, situado no território da União, quer o tratamento ocorra dentro ou fora da União. O RGPD é igualmente aplicável a responsáveis pelo tratamento ou subcontratantes não estabelecidos na União, quando seja realizado o tratamento de dados de titulares residentes na União, em duas situações: quando houver oferta de bens e serviços aos titulares; ou quando haja controlo do seu comportamento, que tenha lugar na União.

Importa denotar neste domínio, que a versão portuguesa do RGPD, no art. 3º, n.º 2, refere que é aplicável ao tratamento de dados pessoais de titulares residentes no território da União. Diferentemente, no inglês original, não se faz referência a "residentes", mencionando apenas a aplicabilidade a "*subjects who are in the Union*", ou seja, nesta versão original, o RGPD abrange qualquer cidadão que se encontre na União Europeia. Aguardamos que a legislação nacional a ser elaborada apresente solução para esta questão, de forma a evitar ambiguidade e disparidades na interpretação.

O considerando n.º 19 ressalva que "os Estados-Membros deverão poder manter ou aprovar disposições mais específicas para adaptar a aplicação das regras previstas no

[19] Estes casos deverão ser regulados pela Diretiva (UE) 2016/680.

presente regulamento. Tais disposições podem estabelecer requisitos mais específicos e precisos a respeitar pelas referidas autoridades competentes no tratamento dos dados pessoais para esses outros efeitos."

Visto que ainda se aguarda legislação nacional complementar ao regulamento, não se encontra fixada a entidade que assumirá o papel de autoridade de controlo, todavia parece sensato presumir que esse estatuto caberá à Comissão Nacional de Proteção de Dados.

A nível europeu, a entidade independente que supervisiona o cumprimento das regras da proteção de dados ao nível dos órgãos e instituições comunitárias, estabelecidas no Regulamento (CE) n.º 45/2001, é a Autoridade Europeia para a Proteção de Dados. Outro dos órgãos importantes para a privacidade e proteção de dados, é o Grupo de Trabalho do Artigo 29º que se trata de um órgão independente de carácter consultivo, criado pelo artigo 29.º da Diretiva 95/46/CE. Este grupo de trabalho, de acordo com o considerando n.º 139, será substituído pelo Comité Europeu para a Proteção de Dados e "deverá contribuir para a aplicação coerente do presente regulamento em toda a União".[20]

[20] Também de acordo com o considerando n.º 139º, "a fim de promover a aplicação coerente do presente regulamento, o Comité deverá ser um órgão independente da União" e dotado de personalidade jurídica.

III. Dados Pessoais e seu Tratamento

1. Dados Pessoais

A Lei n.º 67/98, de 26 de outubro dá-nos, na alínea a) do art. 3.º, uma noção de dados pessoais, considerando como tal "qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável".

No RGPD, no art. 4, n.º 1, há um alargamento do conceito de dados pessoais, abarcando toda a informação relativa a uma pessoa singular identificada ou identificável[21] - o titular dos dados. "A definição dos dados pessoais (…) tem de cobrir todos os dados relativos a qualquer pessoa que esteja identificada, isolada, ou puder ser identificada ou isolada — seja pelo responsável pelo tratamento dos dados ou por qualquer outra parte." (BUTTARELLI, 2015). Também no considerando nº 26 é referido que "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." O mesmo considerando exclui deste conceito os dados anónimos, isto é, "as 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."

Deste modo, torna-se um conceito muito lato, passando nomeadamente a incluir dados de localização e identificadores por via eletrónica (IP) mas também metadados[22] e *big data*[23]. Embora houvesse pressão por parte das grandes empresas que procedem ao tratamento de dados em grande escala, para que o *profilling* não fosse incluído no conceito

[21] Segundo o art. 4º, n.º1, será identificável a pessoa que "possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".
[22] Metadados podem ser definidos como "uma descrição estruturada das informações de um recurso". (SMIRAGLIA, 2012, p. 2)
[23] *Big data* "consiste na vasta quantidade de informação susceptível de recolha, armazenamento e análise em grande escala." (ALLEN, 2016). Na sua versão original, "Big Data is the vast quantities of information amenable to large-scale collection, storage, and analysis."

de dados pessoais, por serem criados pelas empresas e não concedidos pelo cidadão, o legislador optou pelo conceito amplíssimo, abarcando também a definição de perfis.

Também o conceito de dados sensíveis foi alargado, passando a abranger designadamente os dados biométricos. Assim, o art. 9º afirma como categorias especiais de dados pessoais, os que "revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa." Na generalidade, será proibido o tratamento de dados sensíveis, sendo que o mesmo artigo lista algumas situações de exceção, nomeadamente quando haja consentimento explícito do titular ou o tratamento seja necessário por motivos de interesse público. O considerando n.º 51 fundamenta a proteção específica dos dados sensíveis com o facto de o tratamento desses dados poder "implicar riscos significativos para os direitos e liberdades fundamentais."

Os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.

2. Tratamento

A Lei n.º 67/98 define, no seu art. 3º, alínea a), tratamento de dados como "qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados", nomeadamente a recolha, a organização e a conservação dos mesmos.[24]

"A criação e a manutenção de um conjunto estruturado de dados pessoais, pelos perigos que pode constituir para os titulares dos dados, é uma tarefa de responsabilidade." (CASTRO, 2005, p. 65). Daí que, antes da vigência do novo regulamento, o tratamento de dados pessoais, na maioria das vezes, estivesse dependente de uma notificação[25] prévia à Comissão Nacional de Proteção de Dados e respetiva autorização ou registo do tratamento.

No art. 6º do RGPD são apresentadas as condições de licitude do tratamento. Aqui estão previstas as situações em que se afasta a ilicitude do tratamento, sendo elas exemplificativamente: a existência de consentimento do titular; a necessidade do tratamento para o cumprimento de uma obrigação jurídica ou execução de um contrato; ou até a existência de interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros. No caso dos menores de 16 anos, para que o tratamento seja lícito é necessário haver o consentimento ou autorização dos titulares das responsabilidades parentais da criança. É, no entanto, dado aos Estados-Membros o poder de diminuir esta idade, até ao limite de 13 anos.

Estando cumpridas estas as condições gerais de legitimidade, terá de ser verificado igualmente o cumprimento dos princípios gerais relativos ao tratamento de dados.

---

[24] Para a definição do conceito de tratamento de dados, importa também o acórdão do caso *Google Spain*, em que o TJUE declarou que "a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência deve ser qualificada de «tratamento de dados pessoais», na aceção do artigo 2.°, alínea b), quando essas informações contenham dados pessoais, e de que, por outro, o operador desse motor de busca deve ser considerado «responsável» pelo dito tratamento, na aceção do referido artigo 2.°, alínea d)."
Acórdão disponível em: http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046

[25] Esta obrigação de notificação foi imposta pelo art. 27.º, n.º 1 da Lei n.º 67/98, de 26 de outubro.

IV. Princípios

No seu artigo 5º, o RGPD elenca os princípios pelos quais o tratamento de dados se deve pautar.

1. Alínea a) - Princípios da Licitude, Lealdade e Transparência

"A licitude do tratamento é aferida pela verificação do cumprimento das regras nacionais, comunitárias, europeias e internacionais a que este está sujeito." (CASTRO, 2005, p. 235)

No que concerne ao princípio da lealdade, este norteia a relação entre o responsável pelo tratamento dos dados e o titular dos mesmos e implica que o primeiro dê a conhecer ao titular as operações de tratamento a que os seus dados serão sujeitos, mas também que o informe e esclareça cabalmente acerca das circunstâncias da recolha dos dados, no momento em que esta for levada a cabo. "O princípio da lealdade concentra o espírito de todos os outros princípios que fundamentam e legitimam o tratamento dos dados, contribuindo para a transparência e segurança jurídica." (RIBEIRO, 2017, p. 88)

A lealdade relaciona-se com a transparência, pelo que o titular tem direito a que lhe sejam prestadas informações, nomeadamente relativamente à finalidade do tratamento e à identidade do responsável. Este princípio "efetiva-se, designadamente, através dos direitos à informação e acesso garantidos ao titular dos dados pessoais." (CASTRO, 2005, p. 229). Encontra-se positivado também no artigo 35º da CRP e estabelece o direito das pessoas singulares a saber quais os seus dados pessoais sujeitos a tratamento, a entidade encarregue desse tratamento e qual a finalidade da operação, sendo que o RGPD explica em que termos estas informações devem ser dadas. O considerando n.º 39 do RGPD exige que "as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples.

Para que haja transparência, o considerando nº 39 menciona, ainda, que "as pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento." A comunicação das finalidades específicas do tratamento dos dados pessoais deverá, ainda, ser feita aquando da recolha dos dados pessoais. Em especial, no que toca a tratamentos de dados *big data* feito por máquinas, deve ser esclarecido quais os critérios usados para a criação dos perfis[26]. Este tipo de regulamentação da recolha, armazenamento e uso dos dados permite que haja uma maior antecipação e avaliação dos riscos para a privacidade das pessoas singulares.

2. Alínea b) - Princípio da Limitação das Finalidades

É imperioso que haja finalidades determinadas para o tratamento de dados e este será realizado para a prossecução dessas finalidades e não de forma incompatível com estas. As finalidades do tratamento de dados deverão ser explícitas e legítimas, e ser determinadas aquando da recolha dos dados pessoais, tal como expresso no considerando n.º 39. Retira-se, portanto, a ideia de que a finalidade do tratamento deve ser conhecida pelo titular antes do início desse tratamento.

O considerando n.º 61 complementa este princípio, esclarecendo que quando o responsável pelo tratamento planear "tratar os dados pessoais para outro fim que não aquele para o qual tenham sido recolhidos, antes desse tratamento o responsável pelo tratamento deverá fornecer ao titular dos dados informações sobre esse fim e outras informações necessárias." Acresce que, caso pretenda realizar o tratamento de dados para finalidades diferentes daquelas para os quais os dados pessoais foram recolhidos e não haja consentimento para tal, o n.º 4 do art. 6º requer que o responsável averigue se "o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos." Para isso, deverá ter em conta designadamente a eventual ligação entre a finalidade que fundou a recolha dos dados e a finalidade do tratamento subsequente, o contexto da recolha e a natureza dos dados.

[26] A este propósito, ver o considerando n.º 60 do RGPD.

3. Alínea c) - Princípio da Minimização dos Dados

De acordo com este conceito de minimização dos dados, os dados pessoais deverão ser "adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados", nos termos desta alínea c), do artigo 5º. A mesma ideia está presente no considerando n.º 39, pelo que, deverá ser recolhido o mínimo possível de dados para a realização do propósito e evitar a recolha de dados excessivos e desnecessários. Acresce que, os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios.

Deste princípio decorre também que, em vez de trabalhar com dados pessoais, se deverá proceder à anonimização desses dados, de forma a tratar os dados pessoais de modo a que não seja possível identificar o seu titular. "A criptografia e a anonimização asseguram um dos princípios da proteção de dados que consiste nas proteções de privacidade seguirem os dados, independentemente de onde estes residam e através de todo o seu ciclo-de-vida. " (MAMEDE, 2015, p. 96)

O RGPD introduz o conceito de "pseudonimização" que consiste na codificação da informação, todavia, de modo a que, através de cruzamento de dados, seja possível a identificação do titular. "Portanto, os dados anonimizados devem ser mantidos separadamente de qualquer informação adicional de modo a garantir a não-atribuição a um indivíduo identificado ou identificável." (MAMEDE, 2015, p. 96)

Conquanto esta ideia de pseudonimização introduzida pelo RGPD seja uma mais valia nos instrumentos para a proteção de dados, não será uma solução perfeita. Isto porque, no caso da *big data*, considerando que o tratamento de dados é levado a cabo por máquinas e inteligência artificial, é realizado um vasto e rápido cruzamento de dados através destes mecanismos, acabando por se obter a identificação do titular mesmo quando se tenha procedido à pseudonimização dos dados.

4. Alínea d) - Princípio da Exatidão

O princípio da exatidão está consagrado também no art 35º n.º1[27] da CRP. A conformidade com este princípio, implica que os dados recolhidos sejam corretos e atualizados sempre que seja necessário. Como o previsto no considerando n.º 39, "deverão ser adotadas todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados", pelo que o responsável pelo tratamento fica adstrito ao dever de retificação ou apagamento dos dados.

"A exatidão e actualização deve ser aferida em função da finalidade do tratamento" (CASTRO, 2005, p. 237). Assim, o responsável pelo tratamento dos dados dever assegurar, tal como estabelecido no art. 6º, n.º 1 da Diretiva 95/46/CE, que os dados recolhidos são adequados, pertinentes, proporcionais e exatos, relativamente à finalidade do tratamento. A retificação deve ser feita quando os dados sejam incorretos e a atualização, caso os dados tenham sofrido alteração e estas devem ser feitas com a devida celeridade.

5. Alínea e) -Princípio da Limitação da Conservação

Da limitação da conservação resulta que os dados devem conservados de uma forma que permita a identificação dos seus titulares, apenas durante o período necessário para as finalidades para as quais são tratados[28], nos termos deste artigo.

"As normas sobre a limitação da conservação dos dados, no RGPD, devem ser conjugadas com o direito a ser esquecido, previsto no art.º 17º, ou seja, o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora

[27] Art. 35º, n.º1 da CRP: "Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei."

[28] Abre-se a exceção de poderem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos e sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados.

injustificada, e nalguns casos antes do termo do período máximo de retenção." (RIBEIRO, 2017, p. 99)

O próprio RGPD, no considerando n.º 39, refere que "a fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica."

6. Alínea f) – Princípio da Integridade e Confidencialidade

A confidencialidade do tratamento de dados implica que este seja feito sendo garantida a segurança desses dados, "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", nos termos deste artigo. "A [norma] ISO 27001 ajuda a garantir o princípio consagrado no regulamento que devem ser tomadas medidas técnicas e organizativas adequadas contra o tratamento não autorizado ou ilegal de dados pessoais e contra a perda ou destruição acidental, ou dano de dados pessoais." (MAMEDE, 2015, p. 96)

O considerando n.º 83 refere que, por forma a garantir a segurança do tratamento de dados e dar cumprimento a este princípio, o responsável pelo tratamento deverá aplicar medidas técnicas e organizativas que possam atenuar os riscos para os dados pessoais, nomeadamente a cifragem. Este considerando esclarece que no cumprimento desta exigência de segurança, serão tidos em consideração "as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger."

Daí que seja importante a realização, pelo responsável pelo tratamento, das avaliações de impacto sobre a proteção de dados pessoais e que o RGPD tenha consagrado a obrigação de notificação de violação de dados pessoais.

7. Art. 5º, n.º 2 - Princípio da Responsabilidade

Deste princípio resulta a ideia de que a responsabilidade pelo cumprimento dos princípios do tratamento de dados enunciados, é do responsável pelo tratamento, sendo que este terá de estar apto a comprovar essa conformidade com o RGPD, nos termos do art. 24º, n.º 1.

Daqui decorre a nova obrigação de registo de atividades de tratamento[29], bem como a obrigação ou possibilidade de designação de encarregado de proteção de dados. As organizações deverão proceder à revisão das suas políticas de privacidade, políticas internas e restantes práticas, atualizando-as, para poder comprovar a conformidade com o RGPD.

[29] Ver ponto 3 do capítulo V.

V. Principais Reformas e Inovações

1. Sanções

Uma das mais controversas novidades do RGPD, é a implementação de coimas por incumprimento substancialmente superiores às anteriormente estabelecidas[30] . Em casos mais graves, podem ascender a 20 milhões ou a 4% da faturação anual da empresa em causa. "Os dados pessoais, que são na sua génese um "direito do homem", passam a ser também um "Corporate Risk"." (FAZENDEIRO, 2017, p. 9)

No art. 83º, o Regulamento distingue dois níveis de aplicação destas coimas. Num nível menos grave, serão aplicadas coimas até 10 milhões de euros ou 2% do volume de negócios[31] da empresa[32] em causa, consoante o montante que for mais elevado, caso sejam violadas: obrigações do responsável pelo tratamento e do subcontratante (nos termos dos artigos 8º, 11º, 25º, 39º, 42º e 43º); obrigações do organismo de certificação (nos termos dos artigos 42º e 43º); ou obrigações do organismo de supervisão (nos termos do artigo 41º, n.º 4).

A casos de maior gravidade, poderão ser aplicadas coimas até 20 milhões de euros ou até 4 % do volume de negócios da empresa em causa, consoante o montante que for mais elevado, casos sejam violados, entre outros: os princípios básicos do tratamento; os direitos dos titulares dos dados; ou ordens emitidas pela autoridade de controlo.

Na aplicação destas coimas, devem ser tidos em consideração os fatores previstos no art. 83º, n.º 2, nomeadamente, as categorias de dados afetados e a gravidade e duração da infração.

O RGPD trouxe também para os subcontratantes novas obrigações, passando inclusivamente a ter responsabilidade em caso de incumprimento, nos termos do art. 82º, e sendo até possível que fiquem sujeitos ao pagamento das coimas estabelecidas no art. 83º. Também a obrigação de registo de atividades de tratamento e a nomeação de DPO

[30] Ver arts. 37º e 38º da Lei n. º 67/98.
[31] Valor do volume de negócios anual, a nível mundial, correspondente ao exercício financeiro anterior.
[32] Consultar arts. 1º e 2º do anexo da Recomendação 2003/361/CE da Comissão.

constituem novas obrigações que recaem não só sobre os responsáveis pelo tratamento, como sobre os próprios subcontratantes.

É inclusivamente solicitado ao responsável para o tratamento, no considerando n.º 81, que recorra a "subcontratantes que ofereçam garantias suficientes, especialmente em termos de conhecimentos especializados, fiabilidade e recursos".

As novas sanções implementadas pelo RGPD, foram inseridas com o fim de serem "efetivas, proporcionadas e dissuasivas", como caracteriza o próprio. Numa tentativa de salvaguardar a proporcionalidade das sanções, o considerando n.º 148, admite que "pode ser feita uma repreensão, em vez de ser aplicada uma coima." Também no considerando n.º 150 podemos ver este esforço, na medida em que, quando as coimas forem impostas a pessoas singulares, se deverá ter em conta "o nível geral de rendimentos no Estado-Membro, bem como a situação económica da pessoa em questão" aquando do estabelecimento do montante.[33]

A estipulação de sanções tão onerosas acarretará para as organizações, não apenas uma obrigação de envidar esforços no sentido de uma efetiva proteção dos dados que são alvo do seu tratamento, mas também criará um permanente sentimento de apreensão e forçá-las-á a vastos encargos destinados a minimizar a possibilidade de lhes ser aplicada tal punição. É previsível que este regime sancionatório incentive o fenómeno de *forum shopping* por parte dos responsáveis pelo tratamento, a fim de procurar as autoridades de controlo mais flexíveis e benevolentes. Outra das questões do RGPD que, na minha perspetiva, poderão gerar dificuldades, é o facto de não haver uma tipificação das infrações que podem gerar a aplicação das coimas previstas, na medida em que criará alguma insegurança jurídica e abrirá espaço a novas divergências na aplicação da legislação.

[33] Importa, ainda, salientar que, ao contrário do anterior regime jurídico estabelecido pela Lei n.º 67/98, o RGPD não prevê a criminalização de comportamentos infratores, pelo que teremos de aguardar a opção tomada pelo legislador nacional.

2. Encarregado de Proteção de Dados

A figura do encarregado da proteção de dados ou *data protection officer* (DPO) é uma das inovações trazidas pelo RGPD que mais questões tem levantado. Estes encarregados assumirão ampla importância na viabilização do cumprimento das normas do RGPD, perante as organizações, mas também na posição de intermediários entre os diversos intervenientes na proteção de dados pessoais.

2.1. Designação

Como estabelece o art. 37º, a designação de um DPO é obrigatória se o tratamento for efetuado por autoridade ou organismo público[34] ou se as atividades principais[35] do responsável pelo tratamento ou do subcontratante consistirem em operações de tratamento em grande escala[36] de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações ou operações de tratamento que exijam controlo regular e sistemático[37] dos titulares dos dados em grande escala[38].

É ainda admitida a possibilidade de os Estados-Membros legislarem a obrigatoriedade de designação de DPO em outras situações. Mesmo quando esta designação não for obrigatória, as organizações poderão designar um DPO

[34] A definição de "autoridade" ou "organismo público", não consta do RGPD. O GT 29 considera que este conceito deve ser definido ao abrigo da legislação nacional.
[35] O GT 29 esclarece que "as «atividades principais» podem entender-se como as operações essenciais necessárias para alcançar os objetivos do responsável pelo tratamento ou do subcontratante." Neste conceito, o GT 29 inclui as atividades em que o tratamento de dados constitui parte indissociável das atividades do responsável pelo tratamento ou do subcontratante e exclui as funções acessórias necessárias para a atividade principal da organização. Em *Guidelines on Data Protection Officers* (WP 243) pág. 8
[36] Considerando que o RGPD não define o que constitui um tratamento de grande escala, o GT 29 elenca alguns fatores a ser tomados em conta para caracterização de um tratamento como sendo em grande escala. Assim, deve-se atender ao número de titulares de dados afetados, ao volume de dados e à duração e âmbito geográfico da atividade de tratamento de dados.
[37] Embora o RGPD não apresente uma noção de controlo regular e sistemático dos titulares dos dados, o GT 29 esclarece que inclui "todas as formas de seguimento e de definição de perfis na internet, designadamente para fins de publicidade comportamental." Na interpretação do GT 29, o controlo será regular se for: contínuo ou que ocorre a intervalos específicos num determinado período; recorrente ou repetido em horários estipulados; ou constante ou periódico. Ademais, o controlo será sistemático se for: predefinido, organizado ou metódico; realizado no âmbito de um plano geral de recolha de dados; ou efetuado no âmbito de uma estratégia. Em *Guidelines on Data Protection Officers* (WP 243) pág.10
[38] A proposta inicial da Comissão apontava para a nomeação obrigatória de DPO apenas nas empresas que contassem com mais de 250 trabalhadores.

voluntariamente, se o considerarem conveniente, sendo o Grupo de Trabalho do Artigo 29º para a Proteção de Dados, favorável a estas iniciativas voluntárias. Quando uma organização designa um DPO a título voluntário, são aplicáveis à sua nomeação, posição e atribuições os mesmos requisitos aplicáveis à designação obrigatória.

O RGPD admite que um grupo empresarial possa designar um único DPO, desde que consiga garantir a sua acessibilidade em todos os estabelecimentos, isto devido ao facto de o DPO ser o ponto de contacto entre titulares dos dados, autoridade de controlo e a própria organização. Desta necessidade de acessibilidade, decorre também a recomendação do Grupo de Trabalho do Artigo 29º de que o DPO esteja localizado na União, independentemente de o responsável pelo tratamento ou o subcontratante estar ou não estabelecido na União. Nos termos do art. 37º, n.º 7, o responsável pelo tratamento ou o subcontratante deve dar publicidade aos contactos do DPO, bem como comunicá-los à autoridade de controlo competente.

O DPO pode ser interno, ou seja, pertencer ao quadro de pessoal do responsável pelo tratamento ou do subcontratante ou ser externo e exercer as suas funções com base num contrato de prestação de serviços.

2.2 Responsabilidade

O DPO deve exercer as suas funções com autonomia, como tal, o art. 38, n.º 3 estabelece que o responsável pelo tratamento e o subcontratante devem assegurar que o DPO não recebe instruções relativamente ao exercício das suas funções. Embora o considerando n.º 97 refira que "sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência", caso o DPO seja interno, haverá um risco aumentado de deturpação desta autonomia, por força da relação laboral pré-existente.

O n.º 3 do art. 38º veda ainda a hipótese de o DPO ser destituído ou penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções, concedendo assim, ao encarregado alguma proteção da sua autonomia.

A responsabilidade pelo cumprimento das disposições de proteção de dados, como resulta do art. 5º, n.º 2, é do responsável pelo tratamento ou do subcontratante. O art. 38º, n.º 3 estabelece que o DPO comunica diretamente com "a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante." De acordo com o Grupo de Trabalho do Artigo 29º, "esta comunicação direta assegura que os quadros de gestão superiores têm conhecimento do parecer e das recomendações do DPO, no âmbito da missão do DPO de informar e aconselhar o responsável pelo tratamento ou o subcontratante."[39]

.

2.3 Qualidades Profissionais e Competências

O RGPD não determina de forma suficientemente rigorosa o nível de competências que o DPO deve reunir, delimitando, todavia, que se deve coadunar com "a sensibilidade, a complexidade e a quantidade de dados tratados por uma organização." O Grupo de Trabalho do Artigo 29º entende que a designação do DPO deverá ser feita com base nas suas qualidades profissionais e nos seus conhecimentos especializados no domínio das normas e práticas de proteção de dados.

2.4 Funções

O artigo 39º, n.º 1, alínea b), aponta como função basilar do DPO a de controlar a conformidade com o RGPD. Todavia, o art. 24.º, n.º 1 refere que é ao responsável pelo tratamento que incumbe aplicar as medidas técnicas e organizativas adequadas para assegurar esta conformidade, e não ao DPO. O controlo da conformidade não significa que seja imputada responsabilidade ao DPO, em caso de incumprimento.

Da mesma forma, nos termos do artigo 35.º, n.º 1, é ao responsável pelo tratamento que cabe proceder a uma avaliação de impacto sobre a proteção de dados, e não ao DPO. Ainda assim, o DPO deve assistir o responsável nesta avaliação, como resulta do art. 39.º, n.º 1, alínea c).

[39] *Guidelines on Data Protection Officers* (WP 243), pág. 18.

A obrigação consagrada no art. 30º, n.ºs 1 e 2, de conservação de registo de atividades é do responsável pelo tratamento dos dados ou o subcontratante, e não do DPO. Ainda assim, o responsável pode atribuir esta função ao DPO, nos termos do art. 39º, n.º 1

Outra das importantes funções do DPO é a de cooperação e comunicação com a autoridade de controlo. Este contacto que o DPO deve manter com a autoridade de controlo não viola o dever de sigilo a que está obrigado nos termos do art. 38º, n.º 5.

O artigo 38º, n.º 6, admite que os DPO possam "exercer outras funções e atribuições", desde que estas outras funções não deem origem a conflitos de interesses. O Grupo de Trabalho do Artigo 29º defende que haverá potencialmente conflito de interesses dentro de uma organização se o DPO assumir cargos de gestão superiores ou outros cargos que impliquem a determinação das finalidades e dos meios de tratamento[40].

O responsável pelo tratamento e o subcontratante devem conceder ao DPO os recursos necessários ao desempenho das suas funções, tomando em conta a natureza das operações de tratamento e dimensão da organização. Entre estes recursos, podem ser incluídos: apoio às suas funções pelos quadros de gestão superiores, apoio a nível financeiro e de infraestruturas e também formação contínua.

Em suma, é possível constatar que a obrigatoriedade (ou mesmo a mera conveniência) da designação de um DPO, se trata de uma novidade para a generalidade dos países e constituirá um encargo oneroso para uma grande parte das empresas. Todavia, acredito que a questão mais problemática será a possibilidade de designação de um DPO interno. Esta opinião assenta na ideia de que ao cumular funções dentro da mesma organização, o DPO potencialmente verá diminuída a independência necessária ao desempenho eficaz desta função, nomeadamente por receber instruções que, mesmo indiretamente, o poderão condicionar. Posto isto, considero que o DPO deverá ser tomado como uma figura paralela à organização e não, interna, na medida em que deverá cooperar estreitamente com esta, sem perder a sua autonomia.

[40] *Guidelines on Data Protection Officers* (WP 243), pág. 19.

3. Registo de Atividades de Tratamento

A nova exigência de registo de atividades de tratamento, é manifestação do princípio da responsabilidade presente no art. 5º n.º 2. A constituição e atualização de um registo das operações de tratamento de dados efetuadas, possibilita a comprovação do cumprimento da lei, por parte dos responsáveis pelo tratamento, nos termos do art. 5º, n.º 2.

O registo de atividades de tratamento deverá ser disponibilizado, a pedido, à autoridade de controlo[41] e deverá incluir as informações elencadas no n.º 1 do artigo 30º do RGPD, entre elas: a identificação do responsável pelo tratamento, as finalidades do tratamento, as transferências de dados pessoais para países terceiros ou organizações internacionais e os prazos previstos para o apagamento dos dados. Também os subcontratantes devem manter um registo das operações de tratamento realizadas em nome de um responsável pelo tratamento.

Este registo deve ser efetuado por escrito e será obrigatório para empresas com mais de 250 trabalhadores, excetuando alguns casos[42].

[41] Como estabelece o considerando n.º 82.

[42] A obrigação de registo de atividades de tratamento não é aplicável nos casos determinados pelo n.º 5 do art. 30º, isto é, "empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9º, n.º 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10º."

4. Avaliação de Impacto Sobre a Proteção de Dados

A avaliação de impacto sobre a proteção de dados ou *Data Privacy Impact Assessment* (DPIA) trata-se de uma das inovações trazidas pelo RGPD e consiste numa avaliação que deverá ser realizada pelo responsável pelo tratamento de dados com o objetivo de detetar eventuais ameaças à proteção de dados e, minorar o seu impacto. "Estas avaliações devem ser levadas a cabo antes de serem iniciadas as operações de tratamento de dados que utilizem novas tecnologias e que possam implicar elevado risco para os direitos e liberdades dos titulares dos dados." (FAZENDEIRO, 2017, p. 24)

Como decorre do art. 35º do RGPD, há situações em que avaliações desta índole são obrigatórias. Assim, nos termos do art. 35º, n.º 3, a DPIA será obrigatória quando ocorram: avaliações sistemáticas e completas dos aspetos pessoais, baseada no tratamento automatizado, incluindo a definição de perfis; operações de tratamento em grande escala de categorias especiais de dados; ou controlos sistemáticos de zonas acessíveis ao público em grande escala. O n.º 4 do mesmo artigo afirma, ainda, que a autoridade de controlo será incumbida da tarefa de elaborar uma lista dos tipos de operações de tratamento sujeitas à avaliação de impacto sobre a proteção de dados, pelo que haverá que aguardar a legislação nacional a ser criada.

Esta avaliação a ser efetuada antes de iniciar o tratamento, deve conter uma descrição sistemática das operações de tratamento previstas e quais as finalidades e fundamentos dos tratamentos, bem como, a avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos, dos riscos para os titulares dos dados e das medidas previstas para fazer face a esses mesmos riscos.

De acordo como art. 35º, n.º 7 a avaliação deve, pelo menos, incluir: a descrição das operações de tratamento e sua finalidade, a avaliação da proporcionalidade das operações e dos riscos que podem trazer para os direitos e liberdades dos titulares de dados, mas também eventuais medidas[43] a adotar para fazer face a esses mesmos riscos e garantir a proteção dos dados pessoais.

[43] No mesmo sentido aponta o considerando n.º 90.

Do artigo 35º, n.º1, em conjunto com o considerando n.º 84, resulta a imposição da consulta prévia[44] da autoridade de controlo, nos casos em que da DPIA resultar que existe um elevado risco para a privacidade dos titulares dos dados, que o responsável pelo tratamento não conseguirá atenuar através da adoção de medidas adequadas, atendendo à tecnologia disponível e aos custos da sua aplicação.

Nos casos em que tenha sido designado DPO, o responsável deve solicitar parecer ao mesmo. O Grupo de Trabalho do Artigo 29º recomenda que o responsável pelo tratamento solicite o parecer do DPO sobre se de se deve, ou não, efetuar uma DPIA ou qual a metodologia a seguir na realização de uma destas avaliações, entre outras questões pertinentes que devem passar pelo crivo do DPO. Caso o responsável pelo tratamento discorde do parecer dado pelo DPO, o Grupo de Trabalho do Artigo 29º recomenda, como boa prática, que na DPIA se explicitem os fundamentos que o levaram a não seguir tal parecer.

[44] Esta consulta prévia também deverá ter lugar durante os trabalhos de elaboração de uma medida legislativa ou regulamentar que preveja o tratamento de dados pessoais, de acordo com o considerando n.º 96.

5. Notificação de Violação de Dados Pessoais

O RGPD fixa a obrigação, para o responsável pelo o tratamento, de notificação de uma violação de dados pessoais (*data breach*) tanto à autoridade de controlo (art. 33º), como ao próprio titular dos dados (art. 34º).

Do art. 33º, n.º 1 decorre que em caso de violação de dados[45], o responsável pelo tratamento deve notificar a autoridade de controlo desse facto, sem demora injustificada. Se for possível, deve fazê-lo até 72 horas após ter tido conhecimento dessa violação, a menos que daí não resulte risco para os direitos e liberdades dos titulares, como é o caso das *safe breaches*[46]. "O uso de criptografia evita a necessidade de notificação da violação, desde que tenha sido completamente implementada, uma vez que o recurso a este mecanismo torna os dados indecifráveis a qualquer pessoa sem autorização para aceder aos mesmos." (MAMEDE, 2015, p. 94). A norma acrescenta que caso a notificação seja feita após o limite das 72 horas, deve ser acompanhada da justificação do atraso. Também o subcontratante deve notificar o responsável pelo tratamento, sem demora injustificada, após ter conhecimento de uma violação de dados pessoais, de acordo com o art. 33º, n.º 2. Um incidente de violação de dados pessoais, além dos evidentes riscos para a segurança e privacidade dos titulares dos dados, pode culminar numa sanção bastante gravosa.

Os elementos que devem integrar a notificação encontram-se no n.º 3 do mesmo artigo. Daí resulta, nomeadamente que, na notificação, deve ser feita a descrição da natureza da violação dos dados pessoais, da estimativa de titulares de dados afetados e das consequências prováveis da violação de dados. Para além disto, a notificação deve também conter as medidas propostas para atenuar os seus eventuais efeitos negativos da violação, bem como o contacto do encarregado de proteção de dados.

[45] O RGPD apresenta no art. 4º, n.º 12, como conceito de violação de dados pessoais "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".

[46] S*afe breaches* tratam-se de incidentes de violação que dados em que a encriptação torna inúteis os dados roubados.

No que respeita à comunicação da violação de dados ao próprio titular[47], o art. 34º, n.º 1, refere que deverá ser feita quando esta seja "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" e sem demora injustificada[48]. Todavia, o n.º 3 aponta algumas condições sob as quais esta comunicação não será exigida, entre elas, quando o responsável pelo tratamento tenha aplicado medidas de proteção adequadas aos dados afetados ou medidas subsequentes que eliminem o risco para os direitos e liberdades dos titulares dos dados. Esta comunicação ao titular permitir-lhe-á tomar as precauções necessárias e deverá incluir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos da violação, como resulta do considerando n.º 86. Estes incidentes de violação de dados pessoais, devem ficar obrigatoriamente registados pelo responsável pelo tratamento dos dados.

Caberá ao Comité Europeu para a Proteção de Dados a ser criado, nos termos do art. 70º, n.º 1, alíneas g) e h), a determinação de conceitos como "violação de dados pessoais" e "demora injustificada" e também, das circunstâncias concretas em que a notificação de violação de dados pessoais será obrigatória.

47 A comunicação ao titular dos dados será realizada em linguagem clara e simples, de acordo com o n.º 2 do art. 34º.

48 Para aferição do envio sem demora injustificada "importa ter em consideração, em especial, a natureza e a gravidade da violação dos dados pessoais e as respetivas consequências e efeitos adversos para o titular dos dados", nos termos do considerando n.º 87.

6. Consentimento

Com o RGPD, o consentimento terá de obedecer a regras mais rigorosas. Para que o tratamento de dados seja lícito, o artigo 6º, n.º 1, do RGPD exige que se verifique, no mínimo, uma das seguintes condições: que haja consentimento do titular; que o tratamento seja necessário para execução contratual ou para o cumprimento de obrigação jurídica do responsável; ou que o tratamento seja fundamental ao exercício de funções de interesse público do responsável ou para a defesa de interesses vitais de uma pessoa singular. O tratamento será também lícito se for essencial aos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. O RGPD deixa alguma liberdade ao legislador nacional para adotar requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude do tratamento.

No que concerne ao consentimento em si, o art. 7º estabelece as condições de validade a que está sujeito. Assim, é exigido que pedido de consentimento seja escrito em linguagem clara e simples, sendo que o considerando n.º 42 estabelece que o consentimento só poderá ser considerado consentimento informado se, no mínimo, o titular dos dados conhecer a identidade do responsável pelo tratamento dos dados e os fins do tratamento. Será, da mesma forma, necessário que o responsável pelo tratamento possa demonstrar que lhe foi concedido esse consentimento para o tratamento de dados por parte do titular.

A anterior Diretiva 95/46/CE "deixava em aberto a possibilidade de o consentimento ser prestado através de opt-out, isto é, o consentimento podia resultar quer de uma ação quer de uma não ação." (FAZENDEIRO, 2017, p. 35) Diversamente, o regulamento retira esta possibilidade, afirmando no considerando n.º 32 que "o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados." Ficam, assim, excluídas do conceito

de consentimento lícito, o silêncio, a omissão ou as opções pré-validadas[49], ou seja, consentimento tácito será inválido.

O consentimento concedido engloba a totalidade das atividades de tratamento que sejam realizadas com o mesmo fim, sendo que, se o tratamento for realizado com diversas finalidades, deverá haver consentimento para todas elas. Na hipótese de o responsável ter recolhido dados pessoais, com consentimento do titular, para certos fins e pretender tratar esses dados para diferentes finalidades, o RGPD, mediante determinadas reservas, permite que o responsável possa verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos. Para isso, como decorre do n.º4 do art. 6º, deverá ter em conta, entre outros fatores: a ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior; a natureza dos dados pessoais; as eventuais consequências do tratamento posterior pretendido para os titulares dos dados; e a existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

Como resulta do n.º 3 do art. 7º, o consentimento pode ser retirado pelo titular de dados a qualquer momento, sendo que a retirada do mesmo não compromete a licitude do tratamento efetuado. Este artigo afirma até que "o consentimento deve ser tão fácil de retirar quanto de dar."

O regime aplicável ao consentimento apresenta condições especiais quando for relativo a crianças, no que respeita à oferta de serviços da sociedade da informação[50], como resulta do art. 8º do RGPD. Nesta esfera, o consentimento será lícito se a criança for maior de 16 anos, caso contrário, só será legítimo se for dado ou autorizado pelos titulares das responsabilidades parentais da criança[51]. Porém, é dada liberdade aos Estados-Membros para estipular, neste contexto, uma idade inferior, até ao limite mínimo de 13 anos[52].

---

[49] O art 4º, n.º 11 refere que o consentimento seja dado "mediante declaração ou ato positivo inequívoco."
[50] O considerando n.º 38 refere que "essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças."
[51] O art. 7º, n.º 1 ressalva que "não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança."
[52] No Projeto de Lei Orgânica de Proteção de Dados Pessoais (*Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal)*, publicado a 24 de novembro de 2017, podemos verificar que, no seu art. 7º, é estipulado o limite mínimo de 13 anos de idade para a validade do consentimento.

No que concerne ao tratamento de categorias especiais de dados, na ainda atual Diretiva 95/46/CE, para se tratar de dados sensíveis tem de haver consentimento expresso. No seu art. 9º, n.º1, o RGPD elenca como dados sensíveis aqueles que "revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, dados genéticos e dados biométricos que identifiquem inequivocamente uma pessoa, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa"[53]. O tratamento destes é proibido neste artigo, abrindo-se exceção para determinadas circunstâncias, nomeadamente o caso de o titular dos dados dar consentimento expresso[54].

Assim, confrontando o RGPD com a atual Lei da Proteção de Dados, conclui-se que nesta lei, para haver tratamento lícito de dados sensíveis tem de haver consentimento expresso. Por outro lado, com o RGPD, o tratamento de qualquer tipo de dados requer este consentimento expresso e não poderá haver presunção ou consentimento tácito, terá de existir uma ação positiva. No que respeita às operações tratamento para as quais o consentimento foi dado nos termos da Diretiva 95/46/CE, o considerando n.º 171 clarifica que "não será necessário obter uma vez mais o consentimento do titular dos dados, se a forma pela qual o consentimento foi dado cumprir as condições previstas no presente regulamento".

[53] Mais profundamente explicitado no considerando n.º 51.
[54] "exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados", nos termos do art. 9º, n.º 2, alínea a).

7. Direito ao Esquecimento

"O direito ao esquecimento (*the right to be forgotten* ou *droit à l'oubli)* obriga a que os dados apenas possam ser conservados de forma a permitir a identificação dos seus titulares durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior art. 5º, n.º 1, alínea e), da Lei n.º 67/98)." (CASTRO, 2005, p. 239)

Embora constitua uma inovação do RGPD, o direito ao esquecimento já apresentava ecos em diversos ordenamentos jurídicos. Este direito surge como decorrência dos já estabelecidos direitos de cancelamento e de oposição[55] no âmbito dos motores de busca na internet. "De facto, num mundo digital onde a memória não é enfraquecida naturalmente com o passar do tempo, surge a necessidade de adotar medidas com vista a provocar o esquecimento forçado." (FÉLIX, 2015, p. 16)

Crucial para a consagração deste direito no RGPD foi o acórdão de 13 de maio de 2014[56] do processo C-131/12, referente ao caso *Google Spain* SL, *Google Inc*. v AEPD[57], Mario Costeja González que contribuiu substancialmente para a "discussão acerca do reconhecimento do direito ao esquecimento na Europa e para além dela, intensificando o interesse doutrinário, legislativo e jurisprudencial em discutir essa problemática." (TRIGUEIRO, 2016, p. 8). Neste acórdão foi reconhecida a responsabilidade de um operador de motor de busca pelo tratamento que realiza de dados pessoais que surjam em sites de terceiros. Assim, como previsto neste acórdão, "quando, na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, a lista de resultados exibe uma ligação para uma página web que contém informações sobre a pessoa em questão, esta pode dirigir-se diretamente ao operador ou, quando este não dê seguimento ao seu pedido, às autoridades competentes para obter, em certas condições, a supressão dessa ligação da lista de resultados." Desta forma, em determinadas circunstâncias, dá-se ao titular de dados a possibilidade de solicitar aos motores de busca, o apagamento de links que surjam como resultados de pesquisa realizada através do seu nome.

[55] O direito de oposição já se encontrava presente no art. 12º da Lei n.º 67/98.
[56] Acórdão do processo C-131/12, disponível em: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=PT
[57] *Agencia Española de Protección de Datos.*

O direito ao esquecimento tem, assim, o intuito de "impedir a difusão de informação pessoal através da internet quando a sua publicação não cumpre com os requisitos de adequação e pertinência previstos na normativa, limitando a difusão universal e indiscriminada de dados pessoais nos motores de busca gerais quando a informação é obsoleta ou já não tem relevância nem interesse público." (YÁÑEZ, 2016). Permite-se, então, ao titular de dados "determinar o desenvolvimento da sua vida de forma autónoma, sem que seja perpetuamente ou periodicamente estigmatizado como consequência de uma ação específica levada a cabo no passado."[58] (MANTELERO, 2013) Todavia, não deve ser tomado com uma oportunidade dada aos cidadãos para manipular a informação disponibilizada, de forma a criar um passado "à medida".

O direito a ser esquecido encontra-se positivado no art. 17º que elenca as circunstâncias que poderão conceder ao titular, o direito a que os seus dados sejam apagados sem demora injustificada. Entre elas, incluem-se situações em que haja oposição do titular ao tratamento ou o consentimento para o tratamento seja retirado[59], sendo que no n.º 3 estão consagradas algumas exceções.

O n.º 3 do art. 17º em conjunto com o considerando n.º 66, exigem ainda que, havendo a publicação de dados e pedido da sua remoção, sejam informados terceiros "que estejam a tratar esses dados pessoais de que os titulares dos dados solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos."

Como estabelecido no considerando nº 59, de forma a agilizar este processo, o direito de apagamento deve ser exercido sem custos para o titular e o responsável pelo tratamento "deverá fornecer os meios necessários para que os pedidos possam ser apresentados por via eletrónica". A resposta a este pedido deve ser dada "sem demora injustificada" e no prazo máximo de um mês, sendo que terá de ser justificada uma eventual recusa do pedido.

[58] Tradução livre da autora. Versão original: "determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past."
[59] No mesmo sentido, o considerando n.º 65.

Neste domínio, a problemática que surge é sobretudo a relativa à colisão entre o direito ao esquecimento e os direitos à liberdade de expressão e à informação[60]. Na perspetiva de alguns autores, tal como Jeffrey Rosen[61], a consagração deste direito representa a maior ameaça para a liberdade de expressão na internet, da próxima década[62]. Importa, aqui, salientar que em países como os EUA, a tutela da privacidade não tem tanto peso como na Europa, dando prevalência a valores como a liberdade de expressão.

Posto isto, será vital que esta colisão de direitos não seja desconsiderada e que se proceda à constante procura de um ponto de equilíbrio que permita a tutela da privacidade, salvaguardando o mais possível, outros direitos fundamentais.

Por outro lado, ao ter em conta as exigências feitas no considerando n.º 59, nomeadamente de que este direito de apagamento seja exercido sem custos para o titular e que o responsável pelo tratamento forneça os meios para que os pedidos possam ser apresentados por via eletrónica, "entende-se que a decisão pode colocar as pequenas e médias empresas em maiores dificuldades na concorrência em virtude dos investimentos que serão necessários em pessoal qualificado." (PEREIRA, 2018)

[60] Acerca desta temática, consultar: LEE, Edward. *The Right to Be Forgotten v. Free Speech*. I/S: A Journal of Law and Policy for the Information Society, vol. 12:1

[61] ROSEN, J. *The Right to Be Forgotten*. The Stanford Law Review, vol. 64

62 Tradução livre da autora "it represents the biggest threat to free speech on the Internet in the coming decade."

8. Direito à Portabilidade

O direito à portabilidade "confere aos titulares o direito a solicitarem ao responsável pelo tratamento dos dados, os seus dados pessoais num formato de uso comum e mesmo a sua transferência para outro responsável pelo tratamento." (FAZENDEIRO, 2017, p. 42). O art. 20º, consagrando este direito, estabelece como condições de aplicação que o titular de dados tenha dado seu consentimento e que o tratamento se realize por meios automatizados. Quando se revele tecnicamente exequível, o titular tem inclusivamente o direito a que os dados sejam transmitidos diretamente entre os responsáveis pelo tratamento. Assim e segundo o Grupo de Trabalho do Artigo 29º[63], o responsável pelo tratamento deve permitir ao titular descarregar diretamente os seus dados, mas também possibilitar que os transmita diretamente a outro responsável pelo tratamento[64].

O direito de acesso no RGPD concede ao titular de dados a possibilidade de solicitar ao responsável pelo tratamento, uma cópia dos dados que estão a ser tratados, em formato eletrónico de uso comum. Por outro lado, este direito à portabilidade vai mais além, na medida em que exige, não somente que a informação seja fornecida "num formato estruturado, de uso corrente, de leitura automática e interoperável"[65] mas também que esses dados sejam transmitidos diretamente a outro responsável pelo tratamento, sempre que se revele tecnicamente possível. Para este efeito, o considerando n.º 68, incita os responsáveis pelo tratamento de dados, a desenvolver formatos interoperáveis que viabilizem a portabilidade.

No art. 12º, n.º 5 é explicitado que este fornecimento de dados deve ser feito a título gratuito. Todavia, é aberta a possibilidade de o responsável pelo tratamento de exigir o pagamento de uma taxa para esta operação caso o responsável pelo tratamento possa demonstrar que os pedidos são manifestamente infundados ou excessivos ou "devido ao seu caráter repetitivo".

[63] *Guidelines on the right to data portability (WP 242).*
[64] O GT 29 elucida no WP 242 que com vista a dar cumprimento a estes requisitos, pode, por exemplo, ser disponibilizada uma interface de programação de aplicações.
[65] Considerando n.º 68

A portabilidade não será aplicável se o tratamento for baseado em fundamento jurídico que não seja um contrato ou o consentimento do titular nem ao "tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento", nos termos do art. 20º, n.º 3.

Com este novo direito advêm alguns pontos problemáticos, especialmente ao nível da interoperabilidade dos sistemas. Considerando que nem ao nível da Administração Pública foi alcançada a total interoperabilidade, entre empresas e organizações essa realidade é ainda mais notória. Não obstante o considerando n.º 68 referir que este direito "não deverá implicar para os responsáveis pelo tratamento a obrigação de adotar ou manter sistemas de tratamento que sejam tecnicamente compatíveis", a portabilidade criará encargos adicionais substanciais para os responsáveis para o tratamento, pela necessidade de adotar soluções técnicas adequadas às expetativas dos titulares de dados. Assim, a legislação nacional de proteção de dados que está atualmente a ser desenvolvida para possibilitar a aplicação do RGPD, deverá ter em conta particularmente as pequenas e médias empresas, por forma a evitar um ónus gravoso para estas entidades.

9. Profiling

O *profiling*[66] ou definição de perfis, permite aos responsáveis pelo tratamento de dados, traçar perfis comportamentais e de consumo dos titulares desses mesmos dados. Nos termos do art. 4º, n.º4, para que haja *profiling*, o tratamento dos dados deve ser automatizado e estes devem ser utilizados para avaliar aspetos pessoais relativos a uma pessoa singular, tal como as suas preferências pessoais, a sua situação económica e até o seu comportamento e localização.

Também o considerando n.º 24 assume relevância na conceptualização do *profiling*, distinguindo-o do mero *tracking*. Para haver *profiling* têm, então, de ser definidos os perfis de determinada pessoa singular, "especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes." O mesmo considerando esclarece ainda que quando o tratamento de dados, relativo a *profiling*, for levado a cabo por um responsável ou subcontratante fora da União, deverá também ser abrangido pelo regulamento, na medida em que o comportamento dos titulares dos dados tenha lugar dentro da União.

Para que seja garantido um tratamento equitativo e transparente na definição de perfis, o considerando n.º 71 refere que o responsável pelo tratamento deverá implementar medidas técnicas e organizativas que permitam minorar o risco de erros e os potenciais riscos para os direitos do titular. Ademais, menciona que este tipo de tratamento "deverá ser acompanhado das garantias adequadas[67], que deverão incluir a informação específica[68] ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão."

---

[66] O método de *profiling* mais vastamente utilizado, são as chamadas *cookies*. Este instrumento "trata-se de um pequeno ficheiro enviado pelo gestor do site para o disco rígido do utilizador, que permite identificar o utilizador aquando da sua conexão e proceder à respetiva memorização" (MARQUES, 2006, p. 440)

[67] O art. 21º do RGPD concede ao titular o direito de oposição: "o titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais (…) incluindo a definição de perfis."

[68] Segundo o art. 13º, n.º 2, alínea f), devem ser fornecidas ao titular, informações relativas ao *profiling*, "bem como a importância e as consequências previstas de tal tratamento para o titular dos dados."

Com um crescente número de empresas a lucrar com a criação e posterior venda de perfis detalhados dos seus clientes, estas terão de envidar esforços adicionais para garantir a conformidade com o RGPD. O consentimento parece ser a forma ideal para garantir esta conformidade, porém, no âmbito da definição de perfis de trabalhadores dessas organizações, na medida em que há uma relação de subordinação entre responsável pelo tratamento e o titular de dados, pode haver alguma incerteza na efetiva validade do consentimento.

No art. 22º, relativo a decisões individuais automatizadas, incluindo a definição de perfis, é referido que, em princípio, o titular tem o direito a não ficar sujeito a decisões baseadas em tratamentos automatizados de dados "que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar"[69]. Todavia, no n.º 2 exclui a aplicação, se a decisão: for necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; se for autorizada pela lei de um Estado membro; ou se tiver havido consentimento explícito do titular.

Esta alínea c) do n.º 2, do art. 22º tem originado algumas dúvidas de interpretação, levando por vezes a pensar que esta referência ao consentimento significa uma obrigatoriedade de consentimento para que possa haver *profiling*. Importa aqui notar que "um responsável pelo tratamento poderá utilizar o perfil de um indivíduo para uma tomada de decisão automatizada, porém o profiling não é, em si, uma decisão automatizada[70]." (LEE, 2017). Deste modo, caso não haja tomada de decisão automatizada, o mesmo autor defende que os responsáveis pelo tratamento poderão, em princípio, justificar o *profiling* com base em fundamentos que não o consentimento, como os interesses legítimos referidos no art. 6º, n.º 1, alínea f).

[69] No mesmo sentido, o considerando n.º 71.
[70] Tradução livre da autora. Versão original:"A controller might use an individual's profile in order to make an automated decision, but profiling is not in and of itself an automated decision."

10. Privacy By Design e By Default

Estes conceitos de proteção de dados desde a conceção (*privacy by design*) e por defeito (*privacy by default*), são introduzidos pelo art. 25º e estabelecem que "as organizações devem implementar medidas técnicas e organizativas de forma a demonstrarem que consideraram e integraram medidas de conformidade com as regras de proteção de dados nos tratamentos de dados que levam a cabo, que apenas devem incidir sobre os dados que sejam realmente necessários para a prossecução das finalidades específicas do tratamento." (FAZENDEIRO, 2017, p. 67). Deve, por conseguinte, haver nas organizações, essa preocupação com a privacidade e proteção de dados, aquando da criação das plataformas destinadas a operações de tratamento de dados.

De acordo com o n.º 1 deste art. 25º, para a aplicação de medidas técnicas que cumpram esta exigência de *privacy by design* e *by default*, o responsável pelo tratamento deve ter em conta, as técnicas mais avançadas, os custos da sua aplicação, as finalidades do tratamento e os riscos decorrentes do tratamento para os direitos e liberdades dos titulares.[71] "Entre as medidas a serem tomadas estão a minimização da quantidade de dados coletados, as restrições à partilha de dados e a implementação e a adesão a políticas de retenção." (MAMEDE, 2015)

Uma destas técnicas potenciadoras da proteção dos titulares de dados é introduzida pelo RGPD e trata-se da pseudonimização. "Pseudonimização representa o ato de anonimizar o processamento de dados de tal forma que não pode ser atribuído a um indivíduo específico, sem a utilização de informação adicional." (MAMEDE, 2015, p. 96).

[71] "Através da inclusão da proteção de dados no desenho dos seus sistemas e processos, e ao ajustar a proteção de dados para permitir um controlo do utilizador e uma transparência mais genuínos, os responsáveis pelo tratamento dos dados responsabilizáveis também poderão beneficiar das vantagens dos grandes volumes de dados e simultaneamente assegurar que a dignidade e liberdades das pessoas são respeitadas." (BUTTARELLI, 2015)

Para isso, e como decorre do art. 4º, n.º 5, as informações suplementares devem ser conservadas separadamente dos dados anonimizados, por forma a que não se possam atribuir a uma pessoa identificada ou identificável. Como anteriormente referido, a propósito do princípio da minimização dos dados, nas organizações que procedem ao tratamento de dados em grande escala, a utilização de inteligência artificial para estas operações põe em risco a eficácia da pseudonimização, pela velocidade e quantidade de cruzamentos de dados que conseguem executar., acabando, desta forma, por identificar o titular dos dados.

11. Autoridade de Controlo

1. One Stop Shop

O conceito de *one stop shop* ou princípio do balcão único, apresentado pelo art. 56º, diz respeito à competência da autoridade de controlo principal. Segundo esta ideia, a autoridade de controlo competente será a do estabelecimento principal ou único do responsável pelo tratamento ou do subcontratante.

Como determinado pelo considerando n.º 36, o estabelecimento principal de um responsável pelo tratamento na União será o local em que se encontra estabelecida a sua administração central na União, a menos que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutro estabelecimento do responsável pelo tratamento na União. A determinação do estabelecimento principal de um responsável pelo tratamento na União deverá ser feita através de critérios objetivos. Esse critério não deverá consistir no facto de esse ser o local onde o tratamento é executado, mas "deverá pressupor o exercício efetivo e real de atividades de gestão que determinem as decisões principais quanto às finalidades e aos meios de tratamento mediante instalações estáveis."

No que respeita ao subcontratante, como decorre deste considerando, o seu estabelecimento principal será aquele em que se situe a sua administração central na União. Caso não possua administração central na União, o estabelecimento principal será o local onde são realizadas as principais atividades de tratamento de dados na União. Nos contextos que envolvam o responsável pelo tratamento e o subcontratante, a autoridade de controlo competente, será a do Estado-Membro onde o responsável pelo tratamento tem o estabelecimento principal[72]. "No caso de reclamações ou de violações do

[72] Todavia, nestas circunstâncias, como resulta do considerando n.º 36, "a autoridade de controlo do subcontratante deverá ser considerada uma autoridade de controlo interessada e deverá participar no processo de cooperação previsto pelo presente regulamento." Segundo o GT29, "o conceito de autoridade de controlo interessada destina-se a garantir que o modelo da «autoridade principal» não impede que outras autoridades de controlo tenham uma palavra a dizer quanto à forma de tratar uma questão".

O n.º 22 do art. 4º prevê as situações em que uma autoridade de controlo, possa ser considerada autoridade de controlo interessada e assim, poder tratar um processo mesmo não sendo a autoridade de controlo principal. Assim, será considerada autoridade de controlo interessada nomeadamente, se o responsável pelo tratamento ou o subcontratante estiver estabelecido no território do seu Estado-Membro

Regulamento, estas são da competência da autoridade de proteção de dados do Estado-Membro em que ocorram" (FAZENDEIRO, 2017, p. 65)

O Grupo de Trabalho do Artigo 29º esclarece que o mecanismo do balcão único se aplica unicamente aos responsáveis pelo tratamento com estabelecimento na União, pelo que "os responsáveis pelo tratamento sem qualquer estabelecimento na UE têm de responder perante as autoridades de controlo locais em cada Estado-Membro onde exerçam atividades, por intermédio do seu representante local."[73]

O RGPD não regula especificamente como deverá ser determinada a autoridade de controlo principal de uma organização cuja administração central se encontra fora da União. Consequentemente, o Grupo de Trabalho do Artigo 29º veio esclarecer[74] que, no caso de uma entidade não ter a sua administração central na União, deverá ser a própria a determinar o estabelecimento localizado na União que funcionará como estabelecimento principal. Neste sentido, o Grupo indica exemplificativamente alguns fatores a ter em conta nesta designação, tais como, onde são tomadas as decisões sobre as finalidades do tratamento ou as decisões sobre as operações de tratamento de dados. Contudo, esta identificação poderá ser ulteriormente contestada pela correspondente autoridade de controlo interessada.

Alguns autores entendem este princípio do balcão único como vantajoso, na medida em que um "benefício para as organizações com operações transfronteiriças será não necessitarem de lidar com a agência de proteção de dados em cada Estado-Membro separadamente." (MAMEDE, 2015, p. 94). Porém, com este novo regime, os cidadãos da União, deixam de poder recorrer a apenas uma autoridade de proteção de dados fixa, tendo de se sujeitar à autoridade determinada pelo responsável pelo tratamento. Poderá, assim, prever-se algumas dificuldades especialmente de comunicação, devido às línguas estrangeiras.

---

ou se os titulares de dados residentes no Estado-Membro dessa autoridade de controlo forem ou sejam suscetíveis de ser substancialmente afetados pelo tratamento dos dados.

O RGPD, como se pode observar nomeadamente no art. 60ºss, impõe que haja uma eficaz cooperação entre as autoridades de controlo principais e as interessadas, inclusivamente prestando assistência mútua.

[73] *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority* (WP 244), pág. 11

[74] *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority* (WP 244), pág. 7

2. Tratamento Transfronteiriço de Dados Pessoais

A questão da identificação da autoridade de controlo principal releva quando há tratamento transfronteiriço de dados pessoais por parte do responsável pelo tratamento ou subcontratante. Tal como afirma o Grupo de Trabalho do Artigo 29º, "a autoridade de controlo principal tem como responsabilidade fundamental gerir a atividade de tratamento transfronteiriço de dados"[75].

"Este Regulamento dá especial ênfase à livre circulação dos dados permitindo um aumento significativo dos fluxos transfronteiriços de dados pessoais causado pela integração económica e social resultante do funcionamento do mercado interno." (COUTO, 2016, p. 6)

No n.º 23 do art. 4º, o RGPD apresenta duas hipóteses para a definição de tratamento transfronteiriço. Será considerado tratamento transfronteiriço, aquele que é executado em mais do que um Estado-Membro, caso o responsável pelo tratamento ou subcontratante tenha estabelecimento em mais do que um Estado-Membro da União. Mas também será considerado tratamento transfronteiriço aquele que ocorre num único estabelecimento de responsável pelo tratamento ou de um subcontratante, mas que "que afeta substancialmente[76], ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estado-Membro", nos termos do artigo.

No que respeita ao tratamento transfronteiriço de dados, o RGPD, no seu art. 44º, impõe como princípio geral das transferências que, para que possa haver transferência de dados pessoais para um país terceiro ou uma organização internacional, seja cumprido o RGPD e garantido o nível de proteção dos titulares que o regulamento assegura[77].

Como previsto no art. 45º, n.º 1, só se pode realizar uma transferência de dados para país terceiro, se a Comissão "tiver decidido que o país terceiro (…) assegura um

[75] *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority* (WP 244), pág. 4
[76] Este conceito de afetar substancialmente não se encontra definido pelo RGPD. Porém, o GT 29, no WP 244 (pág. 3 e 4), esclarece que "o intuito da redação é assegurar que nem todas as atividades de tratamento, com qualquer efeito e que ocorram no contexto de um único estabelecimento, sejam abrangidas pela definição de «tratamento transfronteiriço»." Acrescenta, ainda, que "As autoridades de controlo interpretarão caso a caso o conceito de «afeta substancialmente»".
[77] No mesmo sentido, o art. 45º, n.º 1, refere que este tipo de transferência transfronteiriça só será possível se a Comissão entender que não trará perda de segurança face à proteção dos dados transmitidos.

nível de proteção adequado". No sentido de avaliar a adequação desse nível de proteção, devem ser considerados os elementos referidos no n.º 2 do art. 45º. Tal como no art. 45º, n.º 3, ao avaliar a adequação do nível de proteção de determinado país ou organização internacional, a Comissão decide se garante um nível de proteção adequado. Estas decisões de adequação devem ser periodicamente revistas pela Comissão.[78] Caso não haja este tipo de decisão, o art. 46º, n.º 1 estabelece que só poderá haver transferência de dados para países terceiros "se tiverem apresentado garantias adequadas[79], e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes."

Relativamente a este tipo de decisões de adequação da Comissão, importa abordar a Decisão *Safe Harbor*, por ter constituído uma das mais importantes na matéria. Esta decisão *Safe Harbor* ou Porto Seguro, foi criada em 2000 pelo Departamento de Comércio dos EUA, conjuntamente com a Comissão Europeia, como forma de permitir o processo de transferência de dados pessoais da UE para os EUA, garantindo a privacidade e proteção de dados. Tratava-se de um processo de autocertificação, pelo que eram as próprias empresas norte-americanas que declaravam subscrever os princípios do Porto Seguro e cumprir as normas europeias relativas à proteção dos dados pessoais.

Todavia, o TJUE, no acórdão de 6 de outubro de 2015, relativo ao caso Schrems[80], veio declarar a invalidade do *Safe Harbor*[81].

[78] Este ato estará sujeito a "avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional", nos termos do art. 45º, n.º 3.

[79] "Mesmo que se conclua que um Estado terceiro não assegura um nível de proteção adequado a CNPD pode autorizar a transferência se for (a) inequivocamente consentida pelo titular dos dados ou necessária para certos fins (responsabilidade contratual, interesse público, exercício de direitos, proteção de interesses vitais do titular) ou (b) realizada a partir de um registo público aberto à consulta do público ou de qualquer pessoa que possa provar um interesse legítimo (artigo 20/1; ver também o 27/4), ou (c) se o responsável pelo tratamento assegurar, mediante cláusulas contratuais adequadas – em especial cláusulas tipo aprovadas pela Comissão Europeia -, mecanismos suficientes de garantia de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, bem como do seu exercício." (PEREIRA, 2018)
O art. 46º lista diversas destas garantias, incluindo os códigos de conduta e mecanismos de certificação. O catálogo de garantias de adequação aumentou substancialmente face à Diretiva 95/46/CE.

[80] Sobre este caso, consultar SILVA, H. S. (2017). *A Protecção de Dados Pessoais na Era Global: o Caso Schrems.* Pág. 41 a 55.

[81] Os pontos mais relevantes apresentados contra o *Safe Harbor* foram o acesso excessivo aos dados europeus, permitido aos EUA, bem como a falta de procedimentos eficazes para que os cidadãos europeus pudessem comunicar as suas queixas.

Fruto de nova negociação entre os EUA e a Comissão, foi aprovado em 2006, o *EU-U.S Privacy Shield* ou Escudo de Proteção da Privacidade UE-EUA que veio permitir a transferência dos dados pessoais da União para empresas[82] nos EUA, desde que estas tratem os dados em conformidade com as normas de proteção de dados pessoais estabelecidas. Deste modo, a União visa garantir um elevado nível de proteção para os dados transferidos, sejam de cidadão da União ou não.

Para poderem ser certificadas, as empresas devem ter uma política de proteção da privacidade conforme com os princípios de proteção da privacidade. Entre estes princípios a ser cumpridos pelas empresas, encontramos o direito a ser informado, a minimização dos dados e também, o direito de apresentar uma queixa e de obter reparação.

[82] Para consulta da lista de empresas pertencentes ao *Privacy Shield*, aceder a: https://www.privacyshield.gov/welcome

VI. Conclusão

Volvidos, dentro de poucos meses, os dois anos de período transitório concedido pelo RGPD, as organizações que procedem ao tratamento de dados e os próprios titulares, ver-se-ão confrontadas com as novas exigências e transformações trazidas por esta legislação. Assim, o maior desafio neste âmbito da proteção de dados será a implementação prática do RGPD, na medida em que vai obrigar as organizações a repensar e melhorar as suas práticas, de forma a poder assegurar um nível de privacidade equivalente ao imposto por este regulamento. "O que se pode esperar é a necessidade de as organizações terem de fazer investimentos em tecnologia para reduzir o impacto da nova regulamentação de proteção de dados, em geral, com foco na criptografia e em capacidade analítica e de produção de relatórios na área da segurança." (MAMEDE, 2015, p. 97). Esta ideia de necessidade de investimento é agravada pelo facto de, ao contrário de países como Alemanha ou Inglaterra, em Portugal a preocupação com a temática da proteção de dados não estar, até agora, particularmente enraizada na maioria das empresas.

Entre todas as preocupações e imprecisões que têm vindo a ser apontadas ao RGPD, não podemos deixar de reconhecer os méritos deste regulamento. Perante um substancialmente fragmentado e díspar quadro jurídico europeu de proteção de dados, o RGPD trará certamente uma maior uniformização legal. Acrescem ainda, como principal impacto positivo, os novos direitos concedidos ao titular, nomeadamente o direito ao esquecimento e à portabilidade. Estes direitos, apesar das inconveniências que representarão para as entidades processadoras de dados, representam um importante passo na aproximação e conformação do Direito à realidade prática.

Por outro lado, o ponto que vem trazendo maior preocupação às empresas é o facto de a falta de conformidade com o RGPD poder resultar em coimas de gravidade acrescida, expondo as entidades à possibilidade de lhes serem aplicadas coimas que podem atingir valores substanciais como vinte milhões de euros, no caso de infração.

Ora, será aconselhável que as entidades responsáveis pelo tratamento de dados envidem esforços no sentido de garantir a conformidade com o RGPD até ao dia 25 de

maio de 2018. Importará, aqui, notar que estas medidas técnicas e organizativas a ser adotadas, não devem ter em vista apenas esta data, na medida em que deverão representar um plano de longa duração. No entanto, após análise das exigências feitas pelo RGPD, podemos perceber que garantir a conformidade com este regulamento requer um considerável investimento. Prevêem-se dificuldades particularmente para as pequenas e médias empresas e esperamos que o legislador nacional consiga assegurar a proporcionalidade das obrigações.

No que concerne ao controlo e fiscalização, "para assegurar que efetivamente se fará respeitar as regras, as autoridades de proteção de dados independentes têm de estar equipadas não só com poderes legais e instrumentos fortes, mas também com os recursos necessários para igualar a sua capacidade com o crescimento dos negócios baseados em dados." (BUTTARELLI, 2015). Todavia, num artigo do *Diário de Notícias* de 12 de janeiro de 2018[83], a CNPD alerta que, com a entrada em vigor do RGPD, esta não estará apta a levar a cabo as suas novas competências. Isto porque, pelo facto de se passar de um regime de heterorregulação, feita pela CNPD, para um regime de autorregulação, haverá um necessário aumento das ações de fiscalização que requerem um aumento do quadro de pessoal. Além disso, a fim de evitar novas disparidades de interpretação da legislação, a União deverá garantir uma efetiva comunicação e colaboração com as autoridades de controlo nacionais, concertando um nível uniforme de privacidade e proteção de dados.

Para que possamos testemunhar o êxito do RGPD, terá ainda necessariamente de haver um empenho e investimento na formação particularmente das empresas e seus trabalhadores acerca da relevância e aspetos cruciais da matéria de privacidade e proteção de dados. Da mesma forma, será essencial cultivar a cultura da cibersegurança, para evitar a completa frustração dos objetivos deste regulamento.

O caminho para a total *compliance* com o RGPD será complexo e incessante. Impõe-se atualmente a questão de saber se será sequer possível para as organizações, atuar de modo perfeitamente conforme a este regulamento. Resta, ainda, aguardar pela legislação nacional que se encontra em elaboração e complementará o RGPD, para perceber se as dificuldades apontadas foram mitigadas e se será esbatido e sentimento de

[83] Disponível em: https://www.dn.pt/lusa/interior/protecao-de-dados-sem-meios-para-cumprir-regulamento-europeu-a-partir-de-maio-9043624.html

incerteza que tem pairado sobre as organizações. Em todo o caso, aguarda-se uma ampla modificação do paradigma da proteção de dados a nível europeu e uma maior consciencialização para esta temática. “De resto, a Internet é, por natureza, uma rede global não devendo a proteção de dados servir apenas de pretexto para a construção de uma Grande Muralha técnico-digital da Europa.” (PEREIRA, 2018)

Bibliografia

ALLEN, A. L. (Disponível em: https://harvardlawreview.org/2016/12/protecting-ones-own-privacy-in-a-big-data-economy/ de 2016). Protecting One's Own Privacy in a Big Data Economy. *Law, Privacy & Technology Commentary Series*.

BUTTARELLI, G. (2015). *Parecer da Autoridade Europeia para a Proteção de Dados sobre «Corresponder aos desafios dos Grandes Volumes de Dados: Um apelo à transparência, controlo do utilizador, proteção de dados desde a conceção e responsabilidade»*.

CANOTILHO, J. G., & MOREIRA, V. (2014). *Constituição da República Portuguesa Anotada, vol. I.* Coimbra Editora.

CASTRO, C. S. (2005). *Direito da Informática, Privacidade e Dados Pessoais.* Almedina.

COUTO, M. L. (2016). *O E-Commerce à luz do direito – Análise do Regulamento Geral da Proteção de Dados – A Uniformização na União Europeia.* Dissertação de Mestrado apresentada à Faculdade de Direito do Porto - UCP.

FAZENDEIRO, A. (2017). *Regulamento Geral Sobre a Proteção de Dados.* Almedina.

FÉLIX, F. A. (2015). *Direito a Ser Esquecido na Internet: Uma Nova Realidade?* Dissertação de Mestrado: Universidade Nova de Lisboa.

JESUS, I. O. (2012). *O Novo Regime Jurídico de Protecção de Dados Pessoais na Europa.* Obtido em 16 de Outubro de 2017, de Faculdade de Direito - Universidade Nova de Lisboa: http://www.fd.unl.pt/Anexos/7039.pdf.

LEE, P. (2017). Obtido de Privacy, Security and Information Law: http://privacylawblog.fieldfisher.com/2017/let-s-sort-out-this-profiling-and-consent-debate-once-and-for-all/

MAMEDE, H. S. (2015). Revista de Ciências da Computação, nº10. *Notas leitura / Recensão crítica [de] Protection of Personal Data*, p. 91 a 98.

MANTELERO, A. (2013). "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'". *Computer Law & Security Review, vol 29 iss 3*, pp. 229–235.

MARQUES, G. (2006). *Direito da Informática.* Almedina.

PEREIRA, A. L. (2018). *Big Data, E-Health e «Autodeterminação Informativa»: A Lei 67/98, A Jurisprudência e o Regulamento 2016/679 (GDPR).* (Artigo gentilmente cedido pelo autor).

RIBEIRO, F. d. (2017). *O Tratamento de Dados Pessoais de Clientes para Marketing.* Dissertação de Mestrado em Direito: Universidade Autónoma de Lisboa.

SILVA, H. S. (2017). *A Protecção de Dados Pessoais na Era Global: O Caso Schrems.* Dissertação de Mestrado, apresentada à Faculdade de Direito da Universidade Nova de Lisboa.

SMIRAGLIA, R. P. (2012). *Metadata: A Cataloger's Primer.* Routledge.

TRIGUEIRO, F. (2016). *Direito ao Esquecimento na Sociedade da Informação.* Dissertação de Mestrado: Universidade de Coimbra.

YÁÑEZ, S. (23 de Dezembro de 2016). Reclamar o «Direito ao esquecimento». *JusJornal, N.º 2509,* p. Wolters Kluwer.