Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados

Teresa Vale Lopes*

Resumo: O novo Regulamento Geral sobre a Proteção de Dados apresenta como uma das suas caraterísticas essenciais a consagração dos princípios da responsabilidade e de *data protection by design* e *by default*, bem como o estabelecimento de novas medidas organizativas e técnicas que recaem sobre os responsáveis pelo tratamento e subcontratantes. Por outro lado, é prevista a aplicação, por parte das autoridades de controlo, de sanções mais exigentes em caso de incumprimento. O presente texto pretende analisar as principais obrigações e responsabilidades que este Regulamento vem estabelecer para as empresas e o respetivo impacto a nível organizacional.

Palavras-chave: *Regulamento; Proteção de Dados; Responsabilidade; Obrigações.*

Abstract: The new General Data Protection Regulation presents as one of its essential features the acknowledgement of the principles of responsibility and data protection by design e by default, as well as the establishment of organizational and technical measures required to controllers and processors. Additionally, the enforcement of more stringent penalties by supervisory authorities is foreseen in case of non-compliance. This paper intends to analyze the main obligations and responsibilities that this Regulation sets for the companies and the corresponding impact at organizational level.

Keywords: *Regulation; Data Protection; Accountability; Obligations.*

---

* Licenciada em Direito pela Universidade de Coimbra e *LL.M. International Business Law* pela Faculdade de Direito da Universidade Católica Portuguesa. Integra a equipa *Health Care Compliance Iberia* na Johnson & Johnson Medical, com responsabilidade pelo sector em Portugal, e coordena a área de *Data Privacy*, *cross sector*, no Grupo Johnson & Johnson Portugal.

Introdução

Em 27 de abril de 2016, foi adotado pela União Europeia (UE) o RGPD[1], mais de quatro anos após ter sido apresentada pela Comissão Europeia[2] a proposta para a sua implementação. Este regulamento entrou em vigor em maio de 2016 e será diretamente aplicável a todos os Estados-Membros a partir de 25 de maio de 2018 (art. 99.º do RGPD).

O RGPD, que substituirá a atual Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, visa modernizar e harmonizar as regras de proteção de dados entre os Estados-Membros, representando assim um marco fundamental na reforma europeia do regime jurídico de proteção de dados.

Esta reforma constitui um elemento essencial da "Estratégia para o Mercado Único Digital na Europa", lançada em 2015 pela União Europeia, que visa o estabelecimento de um mercado que assegure a livre circulação de pessoas, serviços e capitais e em "que os cidadãos e as empresas podem beneficiar livremente de atividades "on-line" e desenvolver essas atividades em condições de concorrência leal e com um elevado nível de proteção dos consumidores e dos seus dados pessoais, independentemente da nacionalidade ou local de residência", assim como manter a posição da Europa como líder mundial na economia digital[3].

Entre as várias novidades, este novo Regulamento carateriza-se pelo especial enfoque no respetivo cumprimento (*compliance*), sendo consagradas medidas mais rigorosas a nível de governação, responsabilidade e documentação para os responsáveis pelo tratamento ou subcontratantes.

---

[1] Aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (RGPD).

[2] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD), de 25 de janeiro de 2012. Disponível em: <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pt.pdf> (acedido a 10/12/2017).

[3] Neste sentido, v. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Estratégia para o Mercado Único Digital na Europa*, Bruxelas, 6.5.2015, COM (2015) 192 final, p. 3.

Com efeito, enquanto alguns requisitos de natureza burocrática previstos na Diretiva 95/46/CE são suprimidos, tais como a obrigação de notificação prévia às autoridades de controlo das operações de tratamento de dados pessoais[4], são também introduzidas novas "regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades[5]".

Em apreço encontram-se medidas relativas à realização de uma avaliação de impacto sobre a proteção de dados e subsequente consulta prévia às autoridades de controlo, ao registo das atividades de tratamento, à notificação de violação de dados pessoais, bem como a obrigação de nomear um encarregado da proteção de dados, responsável por zelar, de forma independente, pela observância das obrigações legais por parte de cada organização e por ser o ponto de contacto com as autoridades de controlo em matéria de proteção de dados pessoais.

O RGPD incentiva ainda a criação de códigos de conduta pelas associações ou outras entidades representativas de categorias de responsáveis pelo tratamento ou de subcontratantes, de forma a tornar mais efetivo o cumprimento das disposições por parte dos diferentes setores, tendo em consideração as suas especificidades, bem como a certificação na área da proteção de dados e de selos e marcas de proteção.

Por outro lado, é prevista a aplicação pelas autoridades de controlo de sanções administrativas, em caso de incumprimento, que poderão atingir 20.000.000 EUR ou, tratando-se de uma empresa, até 4% do respetivo volume de negócios anual a nível mundial (art. 83.º do RGPD).

---

[4] A este propósito, veja-se a posição da Comissão Europeia, que considera que "outro elemento concreto para a redução da sobrecarga administrativa e dos custos dos responsáveis pelo tratamento seria *a revisão e simplificação do sistema de notificação actual*. É consensual entre os responsáveis pelo tratamento que a actual obrigação geral de notificar todas as operações de tratamento de dados às autoridades de protecção de dados é uma obrigação bastante pesada que não traz, por si só, qualquer valor acrescentado à protecção dos dados pessoais". v. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia*, 4.11.2010, COM (2010) 609 final, p. 11.

[5] Neste sentido, v. o considerando 89 do RGPD.

Com o presente texto, pretende-se analisar algumas das principais obrigações e responsabilidades que o novo Regulamento vem estabelecer para as empresas e o respetivo impacto a nível organizacional.

1. Principais elementos impulsionadores da reforma

A rápida evolução tecnológica, a globalização e o fenómeno do *big data* vieram estabelecer novos desafios em matéria de proteção de dados, levando assim à necessidade de rever o quadro normativo vigente.

Com efeito, em 4 de novembro de 2010, a Comissão Europeia concluiu que, apesar dos princípios nucleares da atual Diretiva 95/46/CE se manterem válidos, este diploma já não respondia aos desafios das novas tecnologias, sendo exigível a reforma e modernização do regime jurídico de proteção de dados, de molde a "desenvolver uma abordagem global e coerente que garanta que o direito fundamental das pessoas singulares à proteção dos dados é plenamente respeitado na UE e fora dela[6]".

As mudanças decorrentes do Tratado de Lisboa, que entrou em vigor em 1 de dezembro de 2009, vieram também impulsionar a necessidade de um envolvimento mais ativo da UE, como entidade supranacional, na regulação destas matérias[7]. Em especial, destaca-se a consagração, no art. 16.º do TFUE, de que "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito", cabendo ao Parlamento Europeu e ao Conselho estabelecer as normas relativas ao tratamento de dados pessoais e à livre circulação desses dados[8]. Este artigo vem introduzir uma "base jurídica abrangente para a proteção de dados pessoais nas

---

[6] V. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia*, p. 4. Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_pt.pdf> (acedido a 10/12/2017).

[7] Neste sentido, v. também Burri, Mira e Schär, Rahel. "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", *Journal of Information Policy*, vol. 6, 2016, p. 481.

[8] Saliente-se que a política externa e de segurança comum não é abrangida pelo art. 16.º do TFUE, visto que, de acordo com o art. 39.º do Tratado da União Europeia, as normas específicas nesta área que regulam o tratamento de dados pelos Estados-Membros devem ser estabelecidas por uma decisão do Conselho.

políticas da União", eliminando a anterior "estrutura em pilares" da UE[9] e permitindo assim que a mesma proteção legal seja aplicada a todo o tipo de tratamento de dados. Adicionalmente, o art. 6.º do TUE veio estabelecer que a Carta dos Direitos Fundamentais da União Europeia – cujo art. 8.º reconhece um direito autónomo à proteção de dados[10] – tem o mesmo valor jurídico que os Tratados (art. 6.º do TUE).

Por outro lado, algumas decisões do TJ vieram estabelecer importantes alterações na prática jurídica existente, bem como no entendimento geral sobre os direitos dos indivíduos à proteção de dados na era digital.

Em apreço destaca-se o acórdão "Google Spain[11]", que introduziu na linguagem jurídica europeia o conceito de "direito a ser esquecido", representando agora um novo direito do titular dos dados, previsto no RGPD.

Outro acórdão merecedor de referência é o *Digital Rights Ireland*[12], que veio declarar inválida a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Tal Diretiva pretendera harmonizar a legislação dos Estados-Membros no sentido de assegurar a conservação de categorias de dados de comunicações telefónicas através de redes fixas, móveis ou de internet, bem como comunicações por e-mail, "por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação" (arts. 5.º e 6.º da Diretiva 2006/24/CE), e foi considerada inválida pelo referido acórdão por implicar restrições aos princípios fundamentais de "respeito pela vida privada" (art. 7.º da CDFUE) e da "proteção de dados pessoais" (art. 8.º CDFUE).

---

[9] Neste sentido, v. Comissão Europeia, *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Uma abordagem global da protecção de dados pessoais na União Europeia*, cit., p. 14.

[10] O direito à proteção dos dados constitui um direito fundamental previsto no art. 8.º da Carta de Direitos Fundamentais da União Europeia, autónomo em relação ao direito ao "respeito pela vida privada e familiar" previsto no art. 7.º.

[11] Acórdão do TJ, C-131/12, ECLI:EU:C:2014:317, *Google Spain*, de 13 de maio de 2014.

[12] Acórdão do TJ, C-293/12 e C-594/12, ECLI:EU:C:2014:238, *Digital Rights*, de 8 de abril de 2014.

Por outro lado, o acórdão *Schrems*[13] concluiu pela invalidade do mecanismo de *Safe Harbor*. Este mecanismo consistiu num acordo entre o Departamento de Comércio dos EUA e a Comissão Europeia que permitia às empresas sediadas nos EUA certificarem-se relativamente ao cumprimento de princípios sobre proteção de dados constantes da atual Diretiva 95/46/CE e, por conseguinte, proceder ao tratamento de dados pessoais provenientes de empresas europeias. Atendendo a que o *Safe Harbor* não vinculava as autoridades norte-americanas, prevalecendo sempre o direito interno dos EUA em caso de conflito com os princípios previstos na referida Diretiva, o TJ veio concluir que este mecanismo não conferia um nível de proteção adequado à luz daquela Diretiva.

Por conseguinte, estas decisões não apenas expuseram as deficiências do atual regime jurídico europeu de proteção de dados, como são também o reflexo dos desafios a enfrentar na área de proteção de dados na era digital e das grandes dificuldades em conciliar uma eficaz e efetiva proteção de dados com outros interesses essenciais, tais como a livre circulação da informação, enquanto base da nova economia digital e condição essencial para a liberdade de expressão na internet[14].

2. A "abordagem baseada no risco"

No que respeita às obrigações que recaem sobre o responsável pelo tratamento e subcontratante, é importante desde já salientar que o RGPD adotou a chamada "abordagem baseada no risco[15-16]". Este entendimento vai para além de uma estrita "abordagem centrada nos danos", tendo em consideração todo o potencial ou real efeito adverso avaliado numa escala

---

[13] Acórdão do TJ, C-362/14, ECLI:EU:C:2015:650, *Schrems*, de 6 de outubro de 2015.

[14] Neste sentido, v. Burri, Mira e Schär, Rahel. "The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy", cit., p. 488.

[15] Sobre esta abordagem, v. G29, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN WP 218, de 30 de maio de 2014.

[16] A chamada abordagem baseada no risco não é um conceito novo, tendo já sido adotada em algumas disposições da atual Diretiva: art. 8.º, relativo ao "tratamento de certas categorias específicas de dados", cujo tratamento é considerado de maior risco para os titulares dos dados, art. 17.º, relativo à "segurança do tratamento" e art. 20.º, relativo ao "controlo prévio".

abrangente, desde o impacto no titular dos dados em causa ao impacto geral na sociedade (por exemplo, a perda de confiança social).

Neste sentido, poderão existir diferentes níveis de obrigações e responsabilidades dos responsáveis pelo tratamento e subcontratantes, dependendo do grau de risco colocado pelo tratamento em questão para os titulares dos dados e para a sociedade.

Assim, a necessidade de implementação pelos responsáveis pelo tratamento de medidas técnicas e organizativas que assegurem o cumprimento das regras de proteção de dados (por exemplo, a avaliação de impacto sobre a proteção de dados e consulta prévia, o registo das atividades de tratamento, a implementação de medidas de segurança, a notificação de violação dos dados pessoais, ou a designação do encarregado da proteção de dados) poderá variar consoante o tipo de tratamento de dados e os respetivos riscos para os titulares dos dados. Isto significa que um responsável pelo tratamento que realiza um tratamento de dados com um nível de risco relativamente baixo pode não estar vinculado às mesmas obrigações legais que são aplicáveis a um responsável cujo tratamento representa um elevado risco.

Apesar do exposto, os princípios fundamentais aplicáveis aos responsáveis pelo tratamento (*i.e.* licitude, responsabilidade, minimização dos dados, limitação da finalidade, transparência, integridade, exatidão) deverão ser sempre assegurados, independentemente da natureza, âmbito, contexto, finalidades do tratamento e riscos para os titulares dos dados. Ainda assim, uma vez que a natureza e o âmbito do tratamento são sempre parte integrante da aplicação desses princípios, estes são inerentemente escaláveis, consoante os riscos em presença.

Por outro lado, é importante notar que, mesmo com a adoção de uma abordagem baseada no risco, os direitos dos titulares dos dados não deverão sofrer qualquer tipo de enfraquecimento [*i.e.* direitos de acesso, retificação, apagamento, limitação do tratamento, portabilidade, oposição (arts. 13.º a 22.º do RGPD)], devendo por isso manter a mesma robustez, ainda que o tratamento em causa envolva riscos reduzidos para os titulares dos dados.

3. O princípio da responsabilidade

O RGPD apresenta como uma das suas principais características a consagração do princípio da responsabilidade, estabelecendo expressamente

que, "tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis", cabe ao responsável pelo tratamento aplicar "as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o Regulamento" (art. 24.º do RGPD).

Este princípio foi pela primeira vez introduzido no contexto da proteção de dados, a nível internacional, nas *Guidelines* da OCDE, adotadas em 23 de setembro de 1980[17]. A partir dessa data, a sua importância tem vindo a ser discutida em inúmeros fóruns internacionais dedicados à matéria de proteção de dados[18]. Em especial, destaca-se a *Opinion 3/2010 on the principle of accountability*[19], emitida pelo "Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais" contemplado no artigo 29.º da Diretiva 95/46/CE (G29)[20], na qual foi defendida a introdução deste

---

[17] V. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Disponível em: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#top> (acedido a 10/12/2017). Estas *guidelines*, entretanto atualizadas em 2013, foram aprovadas com o objetivo de consolidar os princípios básicos de proteção de dados entre os Estados-Membros da OCDE e, complementarmente, promover a transferência de dados entre países, procurando resolver os potenciais obstáculos ao desenvolvimento económico provocados por divergências entre as diferentes legislações nacionais.

[18] Tais como, *Canadian Personal Information Protection and Electronic Documents Act* (PIPEDA) (*S.C.* 2000, c. 5*), Schedule 1,* Cláusula 4.1. Disponível em: <http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html> (acedido a 10/12/2017); *"APEC Privacy Framework", 2005* , para. 26 (disponível em: https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework); *Accountability Projects*, lançados a partir de 2009 pelo Center for Information Policy Leadership (CIPL) e várias autoridades de proteção de dados; European Data Protection Supervisory, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union*, janeiro 2011. Disponível em: <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/edps_en.pdf> (acedido a 10/12/2017).

[19] V. G29, *Opinion 3/2010 on the principle of accountability*, 00062/10/EN WP 173. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf> (acedido a 10/12/2017).

[20] O Grupo de Trabalho foi instituído pelo art. 29.º da Diretiva 95/46/CE e consiste num órgão consultivo europeu independente em matéria de proteção de dados e privacidade, cujas atribuições se encontram previstas no art. 30.º da Diretiva 95/46/CE e no art. 15.º da Diretiva 2002/58/CE.

princípio na revisão do regime geral de proteção de dados, com o objetivo de reafirmar e reforçar a responsabilidade do responsável pelo tratamento[21].

Parte do racional desta Opinião é fundado na premissa de que os princípios de proteção de dados e obrigações do responsável pelo tratamento são, no regime de proteção de dados atualmente aplicável, insuficientemente refletidos em medidas e práticas concretas. Desta forma, o princípio da responsabilidade apresenta-se como um mecanismo suscetível de promover a adoção, pelos responsáveis pelo tratamento, de medidas práticas internas que assegurem a eficácia da proteção de dados e, por outro lado, assistam as autoridades de controlo nas tarefas de supervisão e execução.

De acordo com o G29, a maioria dos requisitos inerentes a este princípio não são, em si, uma novidade, uma vez que já decorrem (embora de forma menos explícita) das leis atualmente aplicáveis. Na verdade, na atual Diretiva 95/46/CE, os responsáveis pelo tratamento são já obrigados ao cumprimento dos princípios e obrigações em matéria de proteção de dados pessoais, sendo para tal intrinsecamente necessário estabelecer e aplicar procedimentos para a proteção de dados. Por conseguinte, à luz desta perspetiva, a introdução de um princípio da responsabilidade não visa vincular os responsáveis pelo tratamento de dados a um novo princípio, mas sim promover a adoção de medidas práticas e concretas que assegurem o efetivo cumprimento dos princípios já existentes[22].

Conforme anteriormente referido, a abordagem baseada no risco constitui um dos elementos essenciais do princípio da responsabilidade. Com efeito, de acordo com este princípio, as medidas técnicas e organizativas a adotar pelos responsáveis pelo tratamento deverão ser determinadas em função dos factos e circunstâncias de cada caso em particular, incluindo o tipo de operações de tratamento de dados e os riscos para os direitos e liberdades das pessoas singulares. Mais concretamente, deverão ser tidos em conta aspetos como a dimensão da operação de tratamento de

---

[21] A sugestão de redação do artigo por parte do G29 era a seguinte:

"*Article X – Implementation of data protection principles.*

1. The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.

2. The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request".

[22] Neste sentido, v. para. 36 da *Opinion 3/2010*.

dados, a sua finalidade, a necessidade de transferência de dados, o tipo de dados que vão ser tratados, incluindo o tratamento de dados pessoais sensíveis[23].

Adicionalmente, o RGPD vem incentivar a adoção, por parte do responsável pelo tratamento, de políticas internas adequadas em matéria de proteção de dados, assim como o cumprimento de códigos de conduta e procedimentos de certificação, que poderão ser utilizados "como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento" (art. 24.º, n.º 2 e 3 do RGPD).

Em complemento ao princípio da responsabilidade, o RGPD estabeleceu um conjunto, não exaustivo, de medidas técnicas e organizativas destinadas a assegurar e demonstrar, por parte do responsável pelo tratamento, o cumprimento das regras de proteção de dados. Algumas destas medidas consistem na avaliação de impacto sobre a proteção de dados e consulta prévia, registo das atividades de tratamento, notificação de violação de dados pessoais, nomeação de um encarregado da proteção de dados, cuja implementação poderá variar, tal como anteriormente referido, consoante o tipo de tratamento de dados e os respetivos riscos para os titulares dos dados. O não cumprimento de qualquer uma destas obrigações, poderá implicar, para cada um dos atos, a aplicação de uma coima até 10.000.000 EUR ou, no caso de uma empresa, até 2% do seu volume de negócios anual (art. 83.º, n.º 4 do RGPD).

Nesta sede, cumpre salientar que a obrigação de demonstrar o cumprimento das regras de proteção de dados é suscetível de influenciar um comportamento mais pró-ativo por parte dos responsáveis pelo tratamento, não só no que respeita à implementação de medidas eficazes de proteção de dados nos seus processos de negócio, como também no que concerne à adotação de mecanismos que permitem a avaliação das referidas medidas antes da necessidade de ocorrência de incidentes[24].

De tal forma, enquanto demonstração pró-ativa da capacidade de uma organização em cumprir, a responsabilidade assume-se como um mecanismo

---

[23] A este propósito, v. também para. 45 e 46 da *Opinion 3/2010*.

[24] V. European Data Protection Supervisory, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – "A comprehensive approach on personal data protection in the European Union"*, paras. 99 e 100.

que poderá conferir maior confiança aos titulares dos dados pessoais e reguladores de que as garantias adequadas à proteção dos dados são implementadas.

Por outro lado, uma vez que as empresas, ao abrigo do princípio da responsabilidade, se encontram obrigadas a demonstrar o cumprimento das regras de proteção de dados, fomentando, por isso, uma maior transparência sobre as suas boas práticas corporativas e programas de *compliance*, os reguladores poderão focar a sua atenção nos atores que não demonstrem capacidade para o cumprimento das obrigações em apreço.

Este princípio assume, portanto, um papel fundamental como instrumento de compliance, ao promover a implementação, por parte do responsável pelo tratamento, das garantias necessárias ao cumprimento das regras de proteção de dados e respetiva demonstração, tanto a nível interno como externo[25-26].

4. Os princípios *data protection by design* e *by default*

Associados ao princípio da responsabilidade resultam também do RGPD outros dois novos princípios fundamentais que devem nortear os processos de tratamento de dados pessoais: a proteção de dados desde a conceção (*data protection by design*) e a proteção de dados por defeito (*data protection by default*) (art. 25.º do RGPD).

Estes princípios visam promover o cumprimento por parte do responsável pelo tratamento das regras de proteção de dados durante todo o ciclo de vida dos projetos que envolvem o tratamento de dados pessoais, *i.e.* desde a fase da sua conceptualização, até ao momento do próprio tratamento dos dados.

---

[25] Neste sentido, v. Alhadeff, Joseph, Alsenoy, Brendan Van, e Dumortier, J. "The accountability principle in data protection regulation: origin, development and future directions", *in*: Guagnin, D; Hempel, L. e Ilten, C. *et al.* (eds.). *Managing Privacy through Accountability*. Palgrave Macmillan, 2012, pp. 49-82.

[26] V. ainda European Data Protection Supervisory, *Opinion 7/2015 – Meeting the challenges of big data: A call for transparency, user control, data protection by design and accountability*, de 19 de novembro de 2015, pp. 15 e 16. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf> (acedido a 10/12/2017).

Com efeito, ao abrigo do princípio *data protection by design*, o responsável pelo tratamento deverá implementar, tanto no momento da determinação dos meios de tratamento, como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, destinadas a aplicar com eficácia os princípios da proteção de dados (tal como o da minimização) e a incluir as garantias necessárias no tratamento, de forma a cumprir com o RGPD e proteger os direitos dos titulares dos dados.

Tais medidas poderão incluir, entre outras, a minimização do tratamento de dados pessoais, a total ou parcial anonimização dos dados pessoais ou a sua pseudonimização o mais cedo possível, a separação funcional[27], a transparência no que respeita às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento, assim como a criação de medidas de segurança por parte do responsável pelo tratamento[28]. Este princípio assume, igualmente, particular importância no âmbito dos processos de avaliação de impacto sobre a proteção de dados, na medida em os resultados desta avaliação deverão ser tidos em conta na determinação das referidas medidas.

Por outro lado, à semelhança do princípio da responsabilidade, o RGPD adota uma abordagem flexível e baseada no risco relativa ao princípio de *data protection by design*[29], prevendo expressamente que para a sua aplicação o responsável pelo tratamento deverá ter em conta as técnicas mais avançadas e custos da sua aplicação, a natureza, âmbito, contexto e finalidades do tratamento dos dados, assim como os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento em causa.

Adicionalmente, de acordo com o princípio *data protection by default*, o responsável pelo tratamento deverá assegurar que, por defeito, só sejam tratados os dados pessoais que forem estritamente necessários para cada finalidade específica de tratamento (minimização do tratamento de dados pessoais). Esta obrigação aplica-se à quantidade de dados pessoais recolhidos,

---

[27] Sobre o conceito de separação funcional, v. G29, *Opinion 3/2013 on purpose limitation*, 00569/13/EN WP 203. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> (acedido a 10/12/2017).

[28] Neste sentido, v. o considerando 78 do RGPD.

[29] V., a este título, entendimento da *TaylorWessing – Global Data Hub*. Disponível em: <https://www.taylorwessing.com/globaldatahub/article-privacy-by-design-and-default.html> (acedido a 10/12/2017).

à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em particular, o responsável pelo tratamento deverá aplicar medidas técnicas e organizativas que garantam que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares (art. 25.º, n.º 2 do RGPD).

Assim sendo, ao optar por incluir os conceitos de *data protection by design* e *by default* como princípios-chave do RGPD, o legislador europeu visou assegurar que a proteção de dados representa uma componente fundamental na conceção e manutenção dos sistemas de informação e no *modus operandi* de cada organização. Tal pode levar a que potenciais questões de privacidade sejam identificadas numa fase inicial e menos dispendiosa dos projetos e a uma crescente conscientização de temas de privacidade e proteção de dados nas próprias organizações[30].

A violação deste princípio é suscetível de levar à aplicação de coimas até 10.000.000 EUR ou, no caso de uma empresa, até 2% do seu volume de negócios anual a nível mundial (art. 83.º, n.º 4, alínea a) do RGPD).

5. Novas obrigações para os responsáveis pelo tratamento de dados e subcontratantes

Antes de nos debruçarmos sobre as principais obrigações previstas no RGPD, importa desde logo salientar que, embora os princípios da responsabilidade e *data protection by design* e *by default* acima mencionados sejam diretamente aplicáveis aos responsáveis pelo tratamento, o RGPD vem também introduzir alterações ao âmbito de responsabilidade dos subcontratantes.

De acordo com a Diretiva 95/46/CE, o responsável pelo tratamento é identificado como a pessoa ou entidade que "determina as finalidades e os meios de tratamento dos dados pessoais" (art. 2.º, alínea d) da Diretiva 95/46/CE), enquanto o subcontratante é definido como a pessoa ou entidade que "trata os dados pessoais por conta do responsável pelo tratamento" (art. 2.º, alínea e) da Diretiva 95/46/CE).

---

[30] V., também a este propósito, *TaylorWessing – Global Data Hub*, cit.

Esta distinção é essencial, na medida em que, no âmbito da referida Diretiva, é ao responsável pelo tratamento que incumbe assegurar a observância das obrigações legais em matéria de proteção de dados[31], assim como a responsabilidade em caso de incumprimento, nomeadamente perante os titulares dos dados (art. 23.º da Diretiva 95/46/CE).

Por outro lado, a relação entre o responsável pelo tratamento e o subcontratante deverá ser regida por um contrato escrito que estipule que o subcontratante apenas atua mediante instruções do responsável pelo tratamento e fixe as obrigações a que o subcontratante se encontra vinculado, designadamente no que respeita a medidas de segurança de tratamento (art. 17.º da Diretiva 95/46/CE). A relação entre o responsável pelo tratamento e o subcontratante tem assim, no âmbito da Diretiva 95/46/CE, apenas efeito entre as partes, não concedendo por esta via direito aos titulares dos dados para agirem contra o subcontratante.

A divisão entre responsável pelo tratamento e subcontratante, no âmbito da Diretiva 95/46/CE, tem vindo a ser criticada, especialmente devido à crescente complexidade das operações de tratamento de dados, tais como os dados tratados em *cloud*, redes sociais, motores de busca, em que nem sempre é claro para o titular dos dados quem determina se e como os dados são tratados[32] e, portanto, a quem deve ser alocada a responsabilidade. Tal incerteza é suscetível de provocar efeitos negativos no cumprimento das regras de proteção de dados e na eficácia da legislação de proteção de dados como um todo[33].

---

[31] Em especial, obrigação de observância dos princípios relativos à qualidade dos dados (arts. 6.º, n.º 2), obrigações perante os titulares dos dados (arts. 10.º a 12.º e art. 14.º), obrigação de segurança dos dados (art. 17.º), obrigação de notificação à autoridade de controlo (art. 18.º e ss.).

[32] Alguma doutrina argumenta que a Diretiva possibilita, efetivamente, a um conjunto de atores na área de proteção de dados evitar a responsabilidade pelas suas ações. Neste sentido, v. Cuijpers, Colette; Purtova, Nadezhda e Kosta, Eleni. "Data Protection Reform and the Internet: The Draft Data Protection Regulation". *Tilburg Law School Research Paper No. 03/2014*, p. 6. Disponível em: <https://ssrn.com/abstract=2373683> (acedido a 10/12/2017).

[33] A este título, v. G29, *Opinion 1/2010 on the concepts of "controller" and "processor"*, p. 2. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> (acedido a 10/12/2017). Ainda de acordo com esta Opinião, se não estiver suficientemente claro o que deve ser exigido de cada ator, existe um risco claro que pouco, ou nada, aconteça em caso de incumprimento e que as disposições legais permaneçam inefetivas.

Por sua vez, o G29, reconhecendo as dificuldades em aplicar na prática as definições da Diretiva 95/46/CE, veio clarificar, na *Opinion 1/2010 on the concepts of "controller" and "processor"*, os conceitos de responsável pelo tratamento e de subcontratante, nomeadamente conferindo orientações para aplicar a sua distinção pragmaticamente e para avaliar, na determinação da origem do controlo efetivo sobre a decisão de tratar os dados, não só as cláusulas legais e contratuais aplicáveis, como também, as circunstâncias de facto[34]. O G29 articulou igualmente a possibilidade de múltiplos corresponsáveis pelo tratamento, com iguais ou diferentes graus de controlo e de responsabilidade.

O RGPD mantém a distinção da Diretiva 95/46/CE entre responsável pelo tratamento e subcontratante, sendo tais conceitos definidos no mesmo sentido. Contudo, vem introduzir novas obrigações e responsabilidades na esfera do subcontratante.

Com efeito, as obrigações do subcontratante que devem constar do contrato escrito a celebrar com o responsável pelo tratamento são especificadas de uma forma muito mais detalhada em relação àquelas que estão previstas na Diretiva 95/46/CE (art. 28.º, n.º 3 do RGPD).

Adicionalmente, o RGPD estabelece obrigações e responsabilidades que são aplicáveis, tanto ao responsável pelo tratamento como ao subcontratante, tais como a obrigação de manter registos das atividades de tratamento (art. 30.º, n.º 2 do RGPD), a obrigação de cooperar com as autoridades de controlo (art. 31.º do RGPD), a obrigação de implementar as medidas de segurança apropriadas, tais como, pseudonimização, cifragem, teste (art. 32.º do RGPD), a obrigação de, em certos casos, designar um encarregado da proteção de dados (art. 37.º do RGPD), o direito dos titulares dos dados proporem uma ação judicial contra o responsável pelo tratamento ou o subcontratante em caso de violação dos seus direitos nos termos do RGPD (art. 79.º, n.º 2 do RGPD) e receberem uma indemnização dos mesmos (art. 82.º, n.º 1 do RGPD).

Por outro lado, no RGPD a distinção entre o responsável pelo tratamento e subcontratante é aplicada pragmaticamente e é expressamente reconhecida a possibilidade de responsáveis múltiplos ou conjuntos. Neste sentido, o diploma em apreço estabelece que o subcontratante que, em violação do

---

[34] V. G29, *Opinion 1/2010 on the concepts of "controller" and "processor"*, cit., pp. 8-12.

RGPD, determinar as finalidades e os meios de tratamento, nomeadamente por exceder as instruções conferidas pelo responsável pelo tratamento, "é considerado responsável pelo tratamento no que respeita ao tratamento em questão" (art. 28.º, n.º 10 do RGPD). Mais acresce que o RGPD vem regular especificamente a relação entre responsáveis conjuntos pelo tratamento, prevendo de forma expressa que tais corresponsáveis devem adotar um acordo que defina as funções e responsabilidades de cada um (art. 26.º, n.º 1 e 2 do RGPD) e que, independentemente deste acordo, o titular dos dados pode exercer os seus direitos contra cada um dos responsáveis pelo tratamento (art. 26.º, n.º 3 do RGPD).

A extensão das obrigações e responsabilidades do subcontratante, em conjunto com as pesadas sanções no âmbito do RGPD, são assim suscetíveis de gerar alterações na dinâmica de negociação dos contratos a celebrar entre os responsáveis pelo tratamento e subcontratantes, designadamente no que respeita à transferência de risco e ações de direito de regresso no caso do subcontratante ser sancionado devido a qualquer incumprimento por parte do responsável pelo tratamento[35].

6. A avaliação de impacto sobre a proteção de dados

Às características anteriormente identificadas como relevantes novidades do RGPD deve ainda enfatizar-se, em matéria de responsabilidade e governação, a obrigação da avaliação de impacto sobre a proteção de dados e a consulta prévia.

Deste modo, quando o tratamento de dados pessoais, em particular com recurso a novas tecnologias, é suscetível de implicar um elevado risco para os direitos e liberdades de pessoas singulares, o responsável pelo tratamento encontra-se obrigado, nos termos do RGPD, a conduzir, antes de iniciar o tratamento, uma avaliação de impacto das operações de tratamento sobre a proteção de dados (art. 35.º, n.º 1 do RGPD). Através desta medida, os responsáveis pelo tratamento devem descrever as operações de tratamento

---

[35] A este título, v. Linklaters, *The General Data Protection Regulation – A survival guide*, outubro de 2016, p. 42. Disponível em: <http://www.linklaters.com/pdfs/mkt/london/TMT_DATA_Protection_Survival_Guide_Singles.pdf> (acedido a 10/12/2017).

e sua finalidade, assim como ponderar a respetiva necessidade e proporcionalidade, avaliar os riscos para os direitos e liberdades dos titulares dos dados decorrentes desse tratamento e determinar as medidas essenciais para a sua mitigação (art. 35.º, n.º 7 do RGPD). Esta obrigação constitui uma importante ferramenta complementar aos princípios da responsabilidade e *data protection by design* e *by default*. Isto porque, devendo a avaliação ter lugar num momento prévio ao tratamento, visa assegurar que a proteção de dados e privacidade sejam consideradas desde a conceção do processo de tratamento, promovendo, assim, a criação de soluções que assegurem o cumprimento das regras de proteção de dados e constituindo um elemento essencial para demonstrar tal cumprimento[36].

Em consonância com a abordagem baseada no risco adotada no RGPD, a condução de uma avaliação de impacto não é obrigatória para todo o tipo de tratamento de dados pessoais, sendo apenas exigível quando o tratamento "for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" (art. 35.º, n.º 1 do RGPD).

Desta forma, cumpre desde já salientar que, conforme clarificado pelo G29, a referência aos "direitos e liberdades dos indivíduos" diz respeito, *prima facie*, ao direito à privacidade, mas também envolve outros direitos fundamentais, tais como a liberdade de expressão, liberdade de circulação, proibição de discriminação, direito à liberdade de pensamento e religião[37].

É igualmente importante considerar que os riscos podem resultar não só da ineficiência das medidas de segurança adotadas, mas também de aspetos inerentes à própria natureza do tratamento de dados em questão. Por exemplo, a privacidade é comprometida se informação sobre a vida privada é recolhida e a proibição de discriminação é suscetível de ser afetada quando

---

[36] Neste sentido, v. G29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 17/EN-WP 248, de 4 de abril de 2017, pp. 4 e 13. Disponível em: <https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/guidelines_on_data_protection_impact_assessment_dpia.pdf> (acedido a 10/12/2017).

[37] Ver, a este título, G29, *Statement on the role of a risk-based approach in data protection legal frameworks*, 14/EN-WP 218, de 30 de maio de 2014, para. 8. Disponível em: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> (acedido a 10/12/2017).

os dados recolhidos são referentes à origem racial ou étnica. Deste modo, a avaliação de impacto sobre a proteção de dados não deve por isso cingir-se à avaliação da forma como os dados são recolhidos e conservados. Esta avaliação deverá também ter em conta as operações de tratamento de dados no seu todo. Tal pressuposto obriga a que os responsáveis pelo tratamento tenham em conta um conjunto de considerações éticas no momento de conceção do próprio processo de tratamento, devendo interromper o mesmo, caso os riscos aos direitos e liberdades dos indivíduos inerentes ao processo sejam elevados[38].

Por outro lado, o RGPD veio estabelecer, a título exemplificativo, casos em que o tratamento de dados é "suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares": (i) "avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares baseada no tratamento automatizado, incluindo a definição de perfis", para servir de base a decisões que produzem efeitos jurídicos na esfera de uma pessoa singular ou que a afetem significativamente[39]; (ii) operações de tratamento em grande escala[40] de categorias especiais de dados ("dados pessoais sensíveis[41]"); ou que (iii) requeiram o "controlo sistemático de zonas acessíveis ao público" (art. 35.º, n.º 3 do RGPD).

---

[38] Neste sentido, Quelle, Claudia. *The Data Protection Impact Assessment, or: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing* (November 25, 2015). Disponível em: <https://ssrn.com/abstract=2695398> (acedido a 10/12/2017).

[39] Por exemplo, quando o tratamento é suscetível de conduzir à exclusão ou à discriminação de indivíduos.

[40] O G29 recomenda a adoção dos seguintes critérios para a determinação se um tratamento de dados é conduzido em grande escala: (i) o número de titulares de dados em causa, (ii) o volume dos dados e/ou variedade de tipo de dados que estão a ser tratados, (iii) a duração ou a continuidade da atividade de tratamento dos dados, (iv) o âmbito geográfico da atividade de tratamento. V. G29, *Guidelines on Data Protection Officers ('DPOs')*, 16/EN-WP 243, p. 7. Disponível em: <http://ec.europa.eu/newsroom/document.cfm?doc_id=43823> (acedido a 10/12/2017).

[41] Dados pessoais sensíveis incluem as categorias especiais de dados previstos no art. 9.º do RGPD (entre outros aí previstos, dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, dados relativos à saúde), bem como os dados pessoais referentes a condenações penais e infrações, conforme previsto no art. 10.º do RGPD.

O G29, com base em várias disposições do RGPD, veio também publicar algumas orientações para determinar se o tratamento é "suscetível de implicar um elevado risco" no âmbito do RGPD[42].

Adicionalmente, nos casos em que a avaliação de impacto indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco, deve ser consultada a autoridade de controlo competente antes do início do tratamento dos dados (art. 36.º, n.º 1 do RGPD). De acordo com o G29, estão em causa casos em que os riscos identificados não podem ser suficientemente endereçados pelo responsável pelo tratamento (*i.e.* quando os riscos residuais se mantêm elevados), como, por exemplo, situações em que os titulares dos dados se podem deparar com consequências significativas ou, até mesmo, irreversíveis, que não podem ultrapassar, e/ou quando parece óbvio que o risco ocorrerá[43].

No caso da autoridade de controlo considerar que o tratamento viola o previsto no RGPD, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, deverá, no prazo de oito semanas a contar da receção do pedido de consulta, emitir orientações ao responsável pelo tratamento ou, quando aplicável, ao subcontratante, podendo aplicar uma variedade de medidas para mitigação ou eliminação do risco (art. 36.º, n.º 2 do RGPD), incluindo, por exemplo, a imposição da limitação temporária ou definitiva do tratamento de dados, ou mesmo a respetiva proibição (art. 58.º, n.º 2, alínea f) do RGPD).

Importa ainda salientar que, apesar da obrigação jurídica de avaliação de impacto sobre a proteção de dados incidir sobre o responsável pelo tratamento, no contrato a celebrar com o subcontratante deverá resultar expressamente que este se obriga a prestar todo o suporte necessário e fornecer qualquer informação relevante para a realização da referida avaliação, sempre e quando o tratamento for realizado, no todo ou em parte, pelo subcontratante (art. 28.º, n.º 3, alínea f) do RGPD).

---

[42] V. G29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, cit., p. 7-11

[43] V. G29, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, p. 19.

7. O registo das atividades de tratamento e notificação de violação de dados pessoais

Não obstante o RGPD suprimir a obrigação de notificação prévia das operações de tratamento de dados pessoais às autoridades de controlo, prevista no art. 18.º da Diretiva 95/46/CE, este diploma vem estabelecer novas obrigações de registo para os responsáveis pelo tratamento de dados e subcontratantes (art. 30.º do RGPD).

Pretende-se, com efeito, que, a fim de comprovar a observância do RGPD, o responsável pelo tratamento ou o subcontratante conserve registos de atividades de tratamento sob a sua responsabilidade[44]. Acresce ainda que os responsáveis pelo tratamento e subcontratantes estarão obrigados a cooperar com a autoridade de controlo, facultando-lhe os referidos registos, sempre que solicitado, para fiscalização dessas operações de tratamento (art. 30.º, n.º 4 do RGPD).

Cumpre também mencionar que, com o intuito de atender às especificidades das micro, pequenas e médias empresas[45], o RGPD prevê uma derrogação da obrigação de conservação deste registo para as organizações com menos de 250 trabalhadores, salvo se o tratamento em apreço implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional, ou abranja os já mencionados "dados pessoais sensíveis" (art. 30.º, n.º 5 do RGPD).

Por outro lado, o responsável pelo tratamento deve notificar à autoridade de controlo a violação de dados pessoais, no prazo máximo de 72 horas após ter tido conhecimento da mesma, a menos que seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada (art. 33.º do RGPD).

Adicionalmente, se a violação dos dados pessoais implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deverá notificar o titular dos dados (art. 34.º, n.º 1 do RGPD).

---

[44] V. considerando 82 do RGPD.

[45] V. considerando 13 do RGPD.

Nesta matéria, importa salientar que, de acordo com o RGPD, por violação de dados pessoais deverá entender-se qualquer 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 objeto de tratamento (art. 4.º, alínea 12 do RGPD). Com base na mencionada definição, o G29 identificou três tipos de violação de dados pessoais que poderão observar-se, isolada ou cumulativamente: violação de confidencialidade (divulgação ou acesso não autorizado ou acidental a dados pessoais), violação da disponibilidade dos dados (perda de acesso ou destruição não autorizada ou acidental dos dados pessoais) e violação da integridade dos dados (alteração não autorizada ou acidental de dados pessoais)[46]. Neste âmbito, veio também definir critérios de avaliação do nível de risco[47].

8. O encarregado da proteção de dados

O encarregado da proteção de dados surge no RGPD como um elemento chave no novo modelo de governação das instituições, assumindo um papel crucial no cumprimento por parte destas das disposições legais relativas à proteção de dados pessoais[48].

No âmbito do RGPD, torna-se obrigatória a nomeação de um encarregado da proteção de dados por parte do responsável pelo tratamento e do subcontratante, sempre que um tratamento de dados pessoais for efetuado por uma autoridade ou organismo público[49] (excetuando os tribunais no exercício da sua função jurisdicional), ou nos casos em que as atividades principais do responsável pelo tratamento ou do

---

[46] V. G29, *Guidelines on Personal data breach notification under Regulation 2016/679, 17/EN WP250*, de 3 outubro de 2017, p. 6 e 7. Disponível em: <http://ec.europa.eu/newsroom/document.cfm?doc_id=47741> (acedido a 10/12/2017).

[47] *Idem*, pp. 19-22.

[48] A designação do encarregado de proteção de dados não constitui em si uma inovação, encontrando-se já prevista, a título facultativo, na atual Diretiva 95/46/CE e constituindo já prática corrente em alguns Estados- Membros, tais como a Alemanha, a França e a Holanda.

[49] De acordo com o G29, o conceito de autoridade ou organismo público deverá ser aferido de acordo com a legislação local. V. G29, *Guidelines on Data Protection Officers (*'DPOs'), cit., p. 6.

subcontratante[50] consistirem em operações de tratamento de dados em grande escala que exijam um controlo regular e sistemático[51] dos titulares dos dados ou o tratamento de dados sensíveis (art. 37.º, n.º 1 do RGPD)[52].

O mencionado encarregado da proteção de dados pode ser um trabalhador do responsável pelo tratamento ou do subcontratante, bem como um prestador de serviços contratado por qualquer um deles (art. 37.º, n.º 6 do RGPD).

Por outro lado, um único encarregado da proteção de dados poderá ser designado para um grupo empresarial ou um conjunto de autoridades ou organismo públicos, desde que seja facilmente acessível a partir de cada estabelecimento (art. 37.º, n.º 2 e 3 do RGPD) e tenha conhecimento especializado no domínio do direito e das práticas aplicáveis em matéria de proteção de dados (art. 37.º, n.º 5 do RGPD).

De forma a assegurar que o encarregado da proteção de dados se encontra acessível, tanto interna como externamente, é importante que os seus contactos estejam publicamente disponíveis (art. 37.º, n.º 7 do RGPD). Por

---

[50] De acordo com considerando 97 do RGPD, as "atividades principais" dizem respeito às "atividades primárias e não estão relacionadas com o tratamento de dados pessoais como atividade auxiliar". O G29 veio, contudo, salientar que tal conceito não deverá excluir aquelas atividades em que o tratamento de dados é uma parte indissociável da atividade do responsável pelo tratamento ou subcontratante. Por exemplo, a atividade principal de um hospital é prestar serviços de saúde. Contudo, um hospital não poderá assegurar cuidados de saúde de uma forma segura e eficaz sem o tratamento dos dados de saúde dos pacientes. Desta forma, o tratamento destes dados deverá ser considerado parte integrante das atividades principais do hospital. V. G29, *Guidelines on Data Protection Officers ('DPOs')*, cit., pp. 6 e 7.

[51] A noção de "controlo regular e sistemático" não se encontra definida no RGPD. De acordo com o G29 esta definição inclui todo o tipo de monitorização e definição de perfis na Internet. Contudo, não se restringe apenas ao ambiente on-line. v. G29, *Guidelines on Data Protection Officers ('DPOs')*, pp. 8 e 9.

[52] Da análise do n.º 4 do art. 37.º do RGPD resulta ainda que a UE e/ou os Estados-Membros terão a discricionariedade de fixar outos casos em que seja obrigatória a nomeação de um encarregado da proteção de dados para além das circunstâncias previstas no RGPD, permitindo assim a fixação, a nível dos Estados-Membros, de requisitos ainda mais exigentes no que respeita à nomeação do encarregado da proteção de dados. Adicionalmente, nos casos em que não é legalmente exigível a nomeação de um encarregado da proteção de dados, os responsáveis pelo tratamento, subcontratantes ou as associações e outros organismos que os representam poderão optar voluntariamente por tal designação. Neste caso, deverão ser igualmente aplicáveis os requisitos previstos no RGPD relativamente ao encarregado da proteção de dados.

conseguinte, o encarregado da proteção de dados, com o suporte de uma equipa, se necessário, deverá encontrar-se numa posição que lhe permita comunicar eficazmente com a sua organização, com os titulares dos dados e com as autoridades de controlo. Tal significa que esta comunicação deve ser realizada no idioma (ou idiomas) utilizados por estas entidades[53].

O encarregado da proteção de dados assume assim um papel fundamental na promoção de uma cultura de *compliance* na área de proteção de dados dentro da organização para a qual trabalha. Em especial, incumbe-lhe, nos termos do RGPD, controlar o cumprimento das obrigações legais e políticas internas em matéria de proteção de dados, incluindo assegurar a repartição de responsabilidades, dar formação, sensibilizar, informar e prestar aconselhamento, designadamente sobre as obrigações do responsável pelo tratamento ou do subcontratante, coordenar auditorias, assim como cooperar e ser o ponto de contacto com as autoridades de controlo (art. 39.º do RGPD) e com os titulares dos dados (art. 38.º, n.º 4 do RGPD).

Estas funções deverão ser exercidas com a máxima independência[54]. O próprio RGPD estabelece alguns mecanismos para garantir que o encarregado da proteção de dados exerça as suas funções com um suficiente grau de autonomia dentro da organização: (i) obrigação do responsável pelo tratamento e do subcontratante assegurarem que o encarregado da proteção de dados não recebe instruções relativamente ao exercício das suas funções, (ii) proibição de destituição ou penalização do encarregado da proteção de dados devido ao exercício as suas funções, (iii) proibição de conflito de interesses com outras funções exercidas pelo encarregado da proteção de dados (art. 38.º, n.º 3 e n.º 6 do RGPD). O G29 veio elencar algumas funções que poderão consubstanciar um conflito de interesses com o cargo de encarregado da proteção de dados, tais como funções que tipicamente envolvam a determinação das finalidades e meios de

---

[53] Neste sentido, G29, *Guidelines on Data Protection Officers ('DPOs')*, cit., p. 10.

[54] Neste sentido, veja-se o previsto no considerando 97 do RGPD: "Estes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência". Sobre boas práticas que ajudam a assegurar a independência do encarregado da proteção de dados ver também Network of Data Protection Officers of the EU Institutions and Bodies, *Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/20011*, 14 October 2010, pp. 5-7. Disponível em: <https://edps.europa.eu/sites/edp/files/publication/10-10-14_dpo_standards_en.pdf> (acedido a 10/12/2017).

tratamento de dados, como, por exemplo, posições de direção na gestão de negócios, ou funções que envolvam a representação em juízo do responsável pelo tratamento ou subcontratante em ações que envolvam a proteção de dados[55].

É importante salientar que, não obstante o encarregado da proteção de dados seja responsável por zelar pela implementação e cumprimento das regras de proteção de dados, tal não significa, contudo, que seja pessoalmente responsável em caso de incumprimento. Na verdade, ao abrigo do princípio da responsabilidade, a designação do encarregado da proteção de dados não exonera a própria instituição da responsabilidade em assegurar e demonstrar a conformidade com o RGPD[56].

9. Códigos de conduta, certificação e selos de proteção

Por último, cumpre ainda salientar que o RGPD vem também incentivar a criação de códigos de conduta pelas associações ou outras entidades representativas de categorias de responsáveis pelo tratamento ou de subcontratantes (arts. 40.º e 41.º do RGPD).

Os referidos códigos de conduta apresentam-se como mecanismos de autorregulação suscetíveis de conferir orientação sobre a aplicação efetiva das regras de proteção de dados, tendo em conta as especificidades de cada sector e as necessidades das micro, pequenas e médias empresas[57]. Neste sentido, aquando da elaboração dos códigos de conduta, as associações e os demais organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes devem consultar as partes interessadas e procurar ter em conta os contributos recebidos e as opiniões expressas em resposta a essas consultas[58].

Adicionalmente, o RGPD promove ainda a criação de mecanismos de certificação na área da proteção de dados e de selos e marcas de proteção, para efeitos de comprovação da conformidade das operações de tratamento de dados com o próprio Regulamento (arts. 42.º e 43.º do RGPD).

---

[55] V. G 29, *Guidelines on Data Protection Officers ('DPOs')*, p. 24.

[56] *Ibidem*, p. 4.

[57] Neste sentido, v. considerando 98 do RGPD.

[58] Neste sentido, v. considerando 99 do RGPD.

Estes instrumentos, além de constituírem um elemento determinante na demonstração do cumprimento das obrigações do responsável pelo tratamento (art. 24.º, n.º 3 do RGPD), assumem-se como fator atenuante na determinação das coimas a aplicar em caso de violação das regras de proteção de dados (art. 83.º, n.º 2, alínea j) do RGPD).

Conclusões

Face ao exposto, cumpre concluir que o RGPD se apresenta como um instrumento essencial para a modernização e harmonização das regras de proteção de dados na UE, baseando-se, essencialmente, na garantia dos direitos e liberdades fundamentais dos cidadãos, perante os novos desafios da era digital.

As novas tecnologias, a globalização, o fenómeno do *big data* permitem, nos dias de hoje e cada vez mais, a utilização de dados pessoais em larga escala, o que exige um quadro de proteção de dados mais sólido e eficaz, que confira uma maior segurança ao tratamento dos dados pessoais.

Este regulamento tem como principais características a especial ênfase no *compliance*, através da consagração dos princípios da responsabilidade e de *data protection by design* e *by default*, bem como do estabelecimento de novas medidas organizativas e técnicas que recaem sobre os responsáveis pelo tratamento e subcontratantes.

A responsabilidade pela verificação prévia do cumprimento das normas de proteção de dados passa, pois, a incidir, essencialmente, sobre os responsáveis pelo tratamento e subcontratantes e não tanto sobre as autoridade de controlo, ficando os primeiros obrigados a implementar mecanismos eficazes que assegurem tal cumprimento, sob pena da aplicação de pesadas sanções, que podem ascender a 20.000.000 EUR ou, tratando-se de uma empresa, até 4% do volume de negócios anual a nível mundial.

Por conseguinte, torna-se fundamental adaptar a estrutura organizacional das empresas e fomentar uma cultura de *compliance*, de molde a promover, internamente, a implementação e a aplicação dos princípios e das novas obrigações desta reforma europeia da proteção de dados, favorecendo o desenvolvimento de uma economia cada vez mais aberta, transparente e responsável.