REFORÇO DA RESPONSABILIZAÇÃO DOS RESPONSÁVEIS PELO TRATAMENTO DE DADOS[1]

Marco Alexandre Saias[2]
Advogado. PRA – Raposo, Sá Miranda & Associados

EXCERTOS

*"Nos últimos anos o conceito de responsabilidade (*accountability*) afirmou-se como um dos alicerces fundamentais para que a proteção de dados fosse efetiva e eficiente"*

"O conceito de responsabilidade engloba aquilo que a maioria dos supervisores espera que sejam as práticas responsáveis das organizações no âmbito das operações de tratamento de dados pessoais que tenham a seu cargo, mas o conceito de responsabilidade reflete igualmente aquilo que muitas legislações incorporaram no que respeita à necessidade de conformidade legal dessas mesmas organizações e das suas operações"

"A ideia central por detrás do conceito de responsabilidade é permitir que os responsáveis pelo tratamento não tenham apenas que cumprir com as regras estabelecidas e previstas na legislação, mas que sejam igualmente capazes de demonstrar a conformidade e como a responsabilidade é exercida"

"O regulamento impõe um conjunto de novos requisitos a serem incluídos em todos os contratos de tratamento de dados"

"O titular de dados que acredite que seus direitos foram violados tem o direito de requerer junto ao responsável pelo tratamento de dados a reparação da situação"

1. As bananas (assim como que a título de introdução)

Abel, nome popular na literatura jurídica, deslocou-se como habitualmente ao supermercado para fazer algumas das compras para o lar. Nesse dia, fatídico nas suas consequências, Abel encontrou Bento (igualmente um nome popular na literatura jurídica) que lhe ofereceu descontos em bananas, apenas bastando para isso que o Abel preenchesse um inquérito. Abel, fascinado e bom apreciador de bananas, decidiu aceitar a proposta e lá preencheu o cupão, conseguindo cinco cêntimos de descontos nas bananas.

As bananas, e outros produtos cuja natureza, perecível ou não, é indiferente, estão no centro da reforma que a União Europeia levou a cabo no que respeita ao regime relativo ao tratamento de dados pessoais e que culminou no Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016[3]. Mas a questão para o leitor permanece no ar: o que tornou esse dia fatídico para Abel?

Abel forneceu os seus dados pessoais a uma empresa e esses seus dados acabaram partilhados com outras empresas sem que Abel tivesse conhecimento. Abel não só começou a receber promoções relativamente a bananas, mas igualmente ofertas de casamento, de investimento e de outras naturezas.

O regulamento pretende criar mecanismos que fortaleçam os direitos fundamentais dos cidadãos, mas, simultaneamente procura facilitar os negócios, e, mais do que criar, reforça os princípios, as regras e as boas práticas já existentes de modo a concretizar esses objetivos.

Partindo de uma solução que é até estranha no quadro habitual da União Europeia, o regulamento inverte o princípio regulatório, estabelecendo um quadro de maior liberdade para os agentes económicos enquanto procura definir de uma forma muito clara e concreta as regras do jogo. Porém, esse maior quadro de liberdade implica um maior grau de responsabilização dos responsáveis pelo tratamento de dados, sendo os quadros gerais desse reforço o objeto de análise das próximas páginas, de uma forma muito breve.

2. *Accountability* / Responsabilidade

Como já referimos, o regulamento traduz uma inversão do princípio regulatório, o que implicou um aprofundamento do princípio da responsabilidade[4] (*accountability*) o qual se afirma ao longo de todo o regulamento, estando presente em toda a sua dimensão como linha condutora no que respeita às obrigações dos responsáveis pelo tratamento e/ou dos subcontratantes, e que nos permitirá compreender de uma forma mais percetível quais os objetivos que o legislador pretendia alcançar.

Nos últimos anos o conceito de responsabilidade (*accountability*) afirmou-se como um dos alicerces fundamentais para que a proteção de dados fosse efetiva e eficiente, fixando-se igualmente como uma tendência dominante no contexto global da privacidade, nomeadamente ao nível de boas práticas organizacionais recomendadas.

Existem vários exemplos desta evolução e tendência, dos quais apontamos, nomeadamente, as orientações da OCDE, o *privacy framework* da APEC e as orientações existentes em países como Canada, Hong Kong, Singapura.

O conceito de responsabilidade engloba aquilo que a maioria dos supervisores espera que sejam as práticas responsáveis das organizações no âmbito das operações de tratamento de dados pessoais que tenham a seu cargo, mas o conceito de responsabilidade reflete igualmente aquilo que muitas legislações incorporaram no que respeita à necessidade de conformidade legal dessas mesmas organizações e das suas operações[5].

Podemos identificar três modalidades de responsabilidade[6]: a responsabilidade política (1), que pode ser descrita como sendo meramente declarativa/enunciativa, ou seja, o responsável pelo tratamento enuncia e compromete-se com um conjunto de práticas, quer junto aos titulares dos dados, quer junto a comunidade em geral. As políticas de privacidade dos websites são um exemplo.

Já a responsabilidade pelo procedimento (2) reflete a natureza e adequação das obrigações organizacionais que o responsável pelo tratamento deve implementar para assegurar e poder demonstrar

que o tratamento é realizado em conformidade com o regulamento, e como tal, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos associados[7].

Por último, a responsabilidade pela prática (3) considera diretamente a necessidade de o responsável pelo tratamento ser capaz de demonstrar a existência de ações concretas relativamente às operações de tratamento e quanto aos dados pessoais, sendo, consequentemente, uma responsabilidade mais ampla e intensa[8].

No caso do regulamento, o princípio da responsabilidade é diretamente aplicável através do número 2 do artigo 5º, o qual exige que o responsável pelo tratamento cumpra com os princípios do regulamento[9], mas igualmente pelo número 1 do artigo 24º.

A responsabilidade torna-se um elemento que percorre o regulamento e está no seu núcleo

Esta introdução reforçada no quadro do regulamento tem como base a opinião[10] e recomendação do Grupo de Trabalho do Artigo 29, o qual indica que o princípio da responsabilidade deve ser uma das medidas a introduzir na revisão do quadro legislativo da proteção de dados da União Europeia, com a finalidade de tornar os responsáveis pelo tratamento responsáveis pela aplicação das medidas necessárias, mas também por assegurarem que os princípios substantivos e obrigações da diretiva sejam efetivamente cumpridos[11]. E igualmente pela necessidade urgente de os incumbidos pelo tratamento aplicarem medidas de proteção que sejam reais e efetivas e dirigidas a uma boa governança da proteção dos dados, promovendo assim a minimização dos riscos legais, económicos e reputacionais que se originam devido às más práticas de proteção de dados[12].

De acordo com a referida opinião do grupo de trabalho, a "arquitetura jurídica" dos mecanismos de responsabilidade contemplaria dois níveis[13]:

a) o primeiro nível consistiria no conjunto dos requisitos legais básicos e obrigatórios para todos os responsáveis pelo tratamento dos dados;

b) o segundo nível incluiria sistemas de responsabilidade voluntários que iriam para lá dos requisitos legais básicos, nomeadamente em termos de implementação ou de garantias da eficácia das medidas.

Assim, a ideia central por detrás do conceito de responsabilidade é permitir que os responsáveis pelo tratamento não tenham apenas que cumprir com as regras estabelecidas e previstas na legislação, mas que sejam igualmente capazes de demonstrar a conformidade e como a responsabilidade é exercida, tornando-se verificável, colocando o regulamento claramente uma especial enfâse nesta capacidade de demonstração.

A responsabilidade torna-se assim um elemento que percorre o regulamento e está no seu núcleo, refletindo um princípio que se traduz em medidas transversais e complementares, mas que também pode ser apoiado através dos instrumentos adequados[14].

O princípio da responsabilidade tem igualmente reflexos que vão para além da mera questão da conformidade legal, permitindo promover claramente uma melhor governança dos dados a nível corporativo, e também práticas eticamente mais corretas[15].

Contudo, é um erro confundir a responsabilidade com a conformidade (*compliance*) e um maior equívoco acreditar que a responsabilidade irá funcionar como um substituto para a conformidade, quando, pelo contrário, a responsabilidade irá permitir atingir e demonstrar a conformidade.

É neste quadro que o reforço das responsabilidades dos responsáveis pelo tratamento está enquadrado e irá operar, responsabilidades essas que iremos analisar de seguida.

3. Responsabilidades dos responsáveis pelo tratamento

Sem prejuízo do que já foi exposto, o reforço das responsabilidades dos encarregados pelo tratamento tem por base o fato de o tratamento de dados ser cada vez mais central na vida das organizações, a vários níveis, quer para gerir os seus clientes, quer para fornecer melhores produtos e serviços a estes, assumindo assim uma relevância central

para as organizações, independentemente de o seu papel ser o de responsável pelo tratamento ou de subcontratante[16].

Como tal, é relevante que uma organização seja capaz de identificar os cenários em que atua enquanto responsável pelo tratamento, de modo a compreender as obrigações que lhe são aplicáveis e, consequentemente, permitir o cumprimento para com essas obrigações, igualmente demonstrando a capacidade de cumprir.

Sem prejuízo das ações e medidas que cada organização deva tomar e implementar para estar conforme e ser responsável perante o regulamento, o que vamos analisar efetivamente são as obrigações, ou seja, o objetivo a atingir, obrigações essas que demonstram esse reforço da responsabilização.

A primeira noção que se deve ter presente é que a obrigação geral que recai sobre os responsáveis pelo tratamento é enganadoramente simples: os onerados pelo tratamento assumem a responsabilidade de garantir que as atividades de processamento sejam compatíveis com a legislação de proteção de dados da União Europeia.

Verificamos assim que o princípio geral não sofre alterações relativamente àquilo que já vinha estabelecido no número 2 do artigo 6º da diretiva: quando uma organização atua enquanto responsável pelo tratamento, é responsável por garantir que suas atividades de tratamento de dados ocorram em conformidade com a legislação.

No entanto, de forma diversa, o regulamento vem fornecer detalhes adicionais sobre a forma como as organizações podem demonstrar a legalidade das suas atividades de tratamento de dados.

Nesse sentido, tanto o Considerando (74) como o artigo 24º estabelecem que o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o regulamento, incluindo a eficácia das medidas, as quais deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares. Ou seja, como referido, ainda que o princípio seja aparentemente simples e idêntico ao que já vinha previsto, o legislador comunitário optou por deixar claro de que forma é que esta conformidade com a legislação é atingida, reforçando

o princípio da responsabilidade, já abordado, através da capacidade de "*ser capaz de comprovar*" essa conformidade para com o regulamento.

Assim, as atribuições do responsável pelo tratamento não são meramente políticas, mas fortemente procedimentais e práticas, através da sua implementação e através da capacidade de as demonstrar.

4. Proteção de dados desde a concepção e por defeito

Este princípio[17] traduz a ideia segundo a qual o cumprimento da legislação comunitária em matéria de proteção de dados deve ser tratado como uma questão fundamental ao longo de todo o processo de desenvolvimento e entrada no mercado de qualquer serviço ou produto, especialmente quando dos mesmos resulte de algum modo uma afetação para os dados pessoais dos utilizadores/consumidores alvo desses serviços e/ou produtos.

O princípio ora em comento, que está estabelecido no Considerando (78) e no artigo 25º, é uma das novidades do novo quadro jurídico comunitário da proteção de dados e obriga a uma especial atenção por parte dos responsáveis pelo tratamento, nomeadamente porque irá articular-se diretamente com os princípios relativos ao tratamento de dados pessoais, em especial a limitação das finalidades, a minimização dos dados ou a limitação da conservação[18].

Por um lado, no que respeita à proteção de dados desde a concepção, há a obrigação de os responsáveis pelo tratamento garantirem que, desde o desenvolvimento, os princípios relativos ao tratamento de dados pessoais sejam respeitados, sobretudo através da adoção de medidas técnicas e organizativas adequadas (como a pseudonimização), sendo destinadas a aplicar com eficácia os princípios da proteção de dados e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do regulamento e proteja os direitos dos titulares dos dados.

Sendo naturalmente consequência da primeira, no que respeita a proteção de dados por defeito, o responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento, o que, associado ao princípio da

minimização dos dados, implica a não recolha exaustiva e abusiva de dados pessoais não adequados à finalidade.

5. Responsáveis conjuntos pelo tratamento

Em relação a qualquer atividade de tratamento, é possível que exista mais do que uma entidade a determinar as finalidades e os meios de tratamento de dados pessoais, traduzindo-se assim na existência de não apenas *um* responsável pelo tratamento mas *vários*.

A diretiva já reconhecia esta possibilidade, ainda que não a consubstanciando tal qual o regulamento faz, numa figura concreta, como acontece no Considerando (79) e artigos 4º, número 7, e 26º.

Assim, quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Esses responsáveis devem, por acordo celebrado entre si, determinar de modo transparente as respectivas responsabilidades pelo cumprimento do regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respectivos deveres de fornecer as informações obrigatórias quando os dados pessoais são (ou não) recolhidos junto do titular dos dados, devendo a essência do acordo ser disponibilizada aos titulares dos dados.

Há que ter noção que, em muitas circunstâncias (particularmente quando o tratamento ocorre num contexto intragrupo), as organizações podem não ter noção de que se encontram numa posição de responsáveis conjuntos. Significa isto que, com estas novas regras, as organizações ficam obrigadas a manterem uma vigilância relativamente a potenciais casos de tratamentos conjuntos de modo a entrarem em acordos adequados.

Como consequência, o titular dos dados pode exercer os direitos que lhe confere o regulamento em relação a cada um dos responsáveis pelo tratamento[19], uma vez que o principal foco do regulamento é garantir a proteção do titular dos dados, sem prejuízo de um responsável ter o direito de reclamar a outros responsáveis envolvidos no mesmo tratamento a parte da indenização correspondente à respectiva parte de responsabilidade pelo dano[20].

6. Representantes dos responsáveis pelo tratamento

Sempre que um responsável pelo tratamento que não se encontre estabelecido na União Europeia efetuar o tratamento de dados pessoais de titulares de dados que se encontrem na União Europeia e as suas atividades de tratamento estiverem relacionadas com a oferta de bens e/ou serviços a esses titulares de dados na União Europeia, o responsável pelo tratamento deverá designar um representante[21], excluindo-se as operações de tratamento de dados que sejam ocasionais, em pequena escala e não envolvam categorias especiais de dados pessoais[22].

O representante deverá ser explicitamente designado por um mandato do responsável pelo tratamento, reduzido a escrito, que permita ao representante agir em nome do responsável pelo tratamento no que diz respeito às obrigações que lhe são impostas pelo regulamento.

A designação de um tal representante não afeta as responsabilidades que incumbem ao responsável pelo tratamento nos termos do regulamento.

O representante deverá executar as suas tarefas em conformidade com o mandato que recebeu do responsável pelo tratamento, incluindo o que toca à cooperação com as autoridades de controlo competentes relativamente a qualquer ação empreendida no sentido de garantir o cumprimento do regulamento.

7. Contratação de subcontratantes

O regulamento impõe um conjunto de novos requisitos a serem incluídos em todos os contratos de tratamento de dados. Implica isto que a seleção de subcontratantes obriga os responsáveis pelo tratamento a contratarem aqueles que ofereçam garantias suficientes, especialmente em termos de conhecimentos especializados, fiabilidade e recursos, quanto à execução de medidas técnicas e organizativas que cumpram os requisitos do regulamento, nomeadamente no que se refere à segurança do tratamento.

Estas operações de tratamento de dados em subcontratação devem ser reguladas por um contrato que vincule o subcontratante ao responsável pelo tratamento e em que seja estabelecido, nomeadamente, o objeto e a duração do contrato, a natureza e as finalidades do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, tendo em conta as tarefas e responsabilidades específicas do subcontratante no contexto do tratamento a realizar e o risco em relação aos direitos e liberdades do titular dos dados. Assim, o subcontratante apenas trata os dados pessoais mediante instruções documentadas do responsável pelo tratamento.

Após concluído o tratamento por conta do responsável por ele, o subcontratante deverá, consoante a escolha do primeiro, devolver ou apagar os dados pessoais, a menos que seja exigida a conservação dos dados pessoais ao abrigo de alguma legislação a que o subcontratante se encontre obrigado.

Por fim, é de referir que o responsável pelo tratamento é responsável pelos danos causados por um tratamento que viole o regulamento quando ocasionados por um subcontratante que tenha seguido as instruções lícitas do responsável pelo tratamento[23].

8. Registos das atividades de tratamento

Ainda que o regulamento elimine o requisito de notificação prévia junto à autoridades de controlo nacionais das atividades de tratamento realizadas pelas organizações, em termos práticos, a informação que teria sido incluída nessa notificação passa a ser simplesmente objeto de registo pelo responsável pelo tratamento (ou pelo seu representante) para disponibilização, a pedido, à autoridade de controlo, sem prejuízo das isenções que o regulamento estabelece[24].

De acordo com o artigo 30º, do registo devem constar as seguintes informações:

a) o nome e os contatos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;

b) as finalidades do tratamento dos dados;

c) a descrição das categorias de titulares de dados e das categorias de dados pessoais;

d) as categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;

e) se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências para organizações internacionais, a documentação que comprove a existência das garantias adequadas;

f) se possível, os prazos previstos para o apagamento das diferentes categorias de dados;

g) se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança.

9. Cooperação com as autoridades de controlo

Em conformidade com o artigo 31º, o responsável pelo tratamento e, sendo caso disso, os seus representantes cooperam com a autoridade de controlo, a pedido desta, na prossecução das suas atribuições.

Assim, o regulamento apenas codifica uma obrigação de fato: de o responsável pelo tratamento dever cooperar com as autoridades de controlo, espelhando essa obrigação ao longo do regulamento.

10. Segurança do tratamento

Se por um lado a diretiva deixava um maior grau de discricionariedade ao responsável pelo tratamento no que respeita às medidas técnicas e organizativas adequadas a aplicar de modo a assegurar um nível de segurança adequado ao risco, o regulamento é mais exaustivo, sendo porém o efeito final muito semelhante, ou seja, a principal obrigação traduz-se no responsável pelo tratamento dever garantir a segurança dos dados pessoais que estão ao seu cuidado. Tal obrigação reflete-se na aplicação das medidas técnicas e organizativas

adequadas para assegurar um nível de segurança condizente ao risco, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares.

Para atingir esse objetivo, o responsável pelo tratamento deve efetuar uma avaliação que determine o nível de segurança adequado, tendo em consideração, nomeadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. Se dessa avaliação de impacto sobre a proteção de dados resultar que o tratamento pode resultar num elevado risco, o responsável pela incumbência consulta a autoridade de controlo antes de proceder à sua efetivação.

11. Notificação de uma violação de dados pessoais

O regulamento tem sobre este tema uma visão muito baseada no risco (*risk approach*) e é claro ao estabelecer a obrigatoriedade de notificar a autoridade de controlo.

A celeridade ou não dessa notificação depende de um elemento fundamental que é "*a possibilidade de*" essa violação dos dados pessoais resultar num risco para os direitos e liberdades das pessoas singulares. Caso resulte nesse risco, há que notificar "*sem demora injustificada e, sempre que possível, até setenta e duas horas após ter tido conhecimento*".

Contudo, no caso da obrigatoriedade de notificar os titulares dos dados, esta ocorre se a violação for suscetível (ou seja, basta criar a possibilidade de) de implicar um elevado risco para os direitos e liberdades das pessoas singulares.

Nessas situações, sem prejuízo da obrigatoriedade de notificar a autoridade de controlo, o responsável pelo tratamento deve, sem demora justificada, comunicar aos titulares dos dados a violação de dados pessoais. Significa isto que, na análise do incidente, deve ser

feita uma ponderação sobre a probabilidade de a violação de dados pessoais afetar os direitos, e existindo essa probabilidade deve a mesma ser suficiente para realizar essa notificação.

Assim, se da análise e dos resultados e medidas tomadas pelo responsável pelo tratamento se concluir pela inexistência de probabilidade de risco, devem existir registos e essas conclusões têm que estar documentadas e fundamentadas para consulta pela autoridade de controlo[25].

12. Responsabilidade

12.1 Direito à ação judicial

O titular de dados que acredite que seus direitos foram violados tem o direito de requerer junto ao responsável pelo tratamento de dados a reparação da situação, e, caso não receba uma resposta adequada do responsável pelo tratamento em questão, é-lhe garantido o direito de apresentar uma queixa junto à autoridade de controlo, a qual pode ser a autoridade de controlo do Estado-membro em que vive ou trabalha, ou a autoridade de controlo do Estado-membro em que ocorreu a alegada infração.

Na sequência dessa queixa, a autoridade de controlo é obrigada a manter o titular dos dados devidamente informado sobre a situação, nomeadamente a evolução da queixa, bem como sobre o resultado dela.

O regulamento deixa bem claro a possibilidade de os titulares dos dados poderem apresentar as referidas queixas em autoridades de controlo diferentes, nunca deixando de ter presente que, no âmbito do mecanismo "*one-stop-shop*", a autoridade de controlo junto ao qual a queixa é apresentada poderá não ser necessariamente a autoridade de controlo interessada pelo responsável pelo tratamento em questão.

Caso o titular dos dados não fique satisfeito com a resposta da autoridade de controlo à sua queixa, é-lhe garantido o direito de apresentar uma queixa junto a um órgão judicial, obtendo assim um recurso judicial efetivo contra:

a) decisões de uma autoridade de controlo que os afete;

b) qualquer falha de uma autoridade de controlo para lidar com uma queixa ou dar resposta a ela em três meses; e

c) qualquer tratamento ilícito dos seus dados pessoais por um responsável pelo tratamento.

Assim, o regulamento consegue fornecer uma maior clareza e segurança jurídica relativamente às queixas que podem ser apresentadas contra responsáveis pelo tratamento.

12.2 Obrigação de indenizar

Tem sido entendimento da legislação comunitária e dos Estados-membros que os responsáveis pelo tratamento devem indenizar os titulares dos dados no caso de qualquer tratamento ilícito dos seus dados pessoais. Já a diretiva, no seu artigo 23º, refletia esse entendimento, o qual foi mantido e desenvolvido pelo regulamento.

Como tal, um titular de dados que tenha sofrido danos como resultado do tratamento ilícito dos seus dados pessoais tem o direito de receber uma indenização por parte do responsável pelo dano sofrido.

Consequentemente, dispõe o regulamento que qualquer responsável pelo tratamento que se encontre envolvido no tratamento é responsável pelos danos causados, o que abre a porta à responsabilidade solidária entre responsáveis conjuntos pelo tratamento e entre o responsável pelo tratamento e o subcontratante, estabelecendo o regulamento que, de modo a que se consiga obter uma compensação efetiva, cada responsável pelo tratamento será responsável pela totalidade do dano causado.

Assim, e tendo em atenção o seu âmbito de aplicação territorial, o regulamento expande o âmbito de responsabilidade em matéria de proteção de dados tanto para os responsáveis pelo tratamento comunitários como extracomunitários.

12.3 Isenções de responsabilidade

Em conformidade com os princípios gerais de responsabilidade, um responsável pelo tratamento está isento de responsabilidade na

medida em que não seja responsável pelo dano relevante, ou seja, se provar que não é responsável pelos fatos ou atos que originaram os danos causados ao titular dos dados.

Uma alteração relevante face à diretiva respeita aos casos de força maior. Enquanto a diretiva isenta os responsáveis pelo tratamento da responsabilidade por danos resultantes de casos de força maior, o regulamento não contém tal isenção, o que significa que o responsável pelo tratamento terá necessariamente de gerir o risco em situações derivadas de casos de força maior.

13. Sanções

13.1 Coimas

Como acontece com outras áreas da legislação regulatória, no âmbito da legislação de proteção de dados existe um sistema de sanções e coimas estabelecido para garantir o cumprimento da legislação, sendo competência das autoridades de controlo nacionais a decisão sobre a (não) aplicação da referida coima, e, em caso afirmativo, a determinação do seu montante.

Nesse sentido, dispõe o regulamento que cada autoridade de controlo deve assegurar que a aplicação de coimas a violações do regulamento é, em cada caso *individual, efetiva, proporcionada e dissuasiva*[26].

Sem prejuízo de o conceito de coimas ou sanções administrativas por violações da legislação da União Europeia em matéria de proteção de dados apenas ser objeto de ligeiras alterações no âmbito do regulamento, existem contudo mudanças significativas tanto no montante de quaisquer coimas quanto nos fatores relevantes para a determinação desses montantes.

O regulamento estabelece um montante de coimas máximas com o objetivo de garantir que as coimas sejam aplicadas numa escala consistente e proporcional. Assim, a coima máxima que pode ser objeto de aplicação por infrações graves do regulamento é de vinte milhões de euros, ou, 4% do volume de negócios mundial de uma empresa relativamente ao exercício anterior, mudando assim de uma forma bastante ampla as possíveis consequências financeiras

derivadas de uma violação da legislação de proteção de dados da União Europeia[27].

Torna-se pois fundamental saber de que modo as autoridades de controlo irão determinar se existem fundamentos para a (não) aplicação de uma coima, e, em caso afirmativo, qual o montante dessa mesma coima, de modo a garantir uma aplicação consistente da legislação de proteção no espaço da União Europeia.

O legislador comunitário procurou garantir esta aplicação consistente, estabelecendo um conjunto de elementos a serem objeto de ponderação, nomeadamente aqueles estabelecidos no número 2 do artigo 83º.

Assim, ao clarificar quais os fatores que são relevantes para determinar a aplicação e o montante da coima, o regulamento consegue fornecer aos responsáveis pelo tratamento um maior grau de certeza e confiança jurídica e operacional quanto ao risco de lhes ser aplicada uma sanção.

13.2 Sanções penais

O regulamento permite por fim que os Estados-membros possam especificar sanções adicionais por infração que não se encontre sujeita a sanções de natureza administrativa.

Desse modo, os Estados-membros podem também prever, aplicar e punir através do seu direito interno as suas próprias normas penais para infrações no âmbito do regulamento.

Significa isto que, a nível prático, existe uma forte probabilidade de continuarem a existir diferenças no que respeita à aplicação das sanções, em consequência das variações nas legislações nacionais originadas pela possível introdução de sanções penais para o tratamento ilícito de dados pessoais, o que representa um risco significativo para os responsáveis pelo tratamento[28].

14. Conclusões

Ainda que, dada a extensão do documento, o regulamento apresente-se como um conjunto normativo extenso, na prática ele traduz um conjunto de princípios e ideias já existentes tanto na

Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108 do Conselho da Europa) quanto na Carta dos Direitos Fundamentais da União Europeia. Traduz igualmente um conjunto de boas práticas no âmbito da privacidade e proteção de dados, governança organizacional e da informação, mas também da segurança da informação.

Existe efetivamente um reforço da imputação dos responsáveis pelo tratamento, mas esse reforço resulta do maior grau de liberdade que o legislador comunitário oferece a esses responsáveis.

As regras do jogo são claras (sem prejuízo das dúvidas e discussões que irão surgir nos próximos anos), e, citando uma frase conhecida, grandes poderes trazem grandes responsabilidades.

Assim, não há que encarar o regulamento com medo e receio, mas como uma ferramenta que irá permitir uma maior segurança no desenvolvimento operacional das organizações, e que também irá cumprir com a proteção das pessoas singulares relativamente ao tratamento de dados pessoais, o qual, nunca devemos deixar de ter presente, é um direito fundamental.

Notas

1. O presente artigo tem por base a conferência proferida no dia 9 de março de 2017, nas VII Jornadas de Direito do Consumo que tiveram lugar na Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria.
2. Marco Alexandre Saias. Advogado. PRA – Raposo, Sá Miranda & Associados.
3. Revogando assim a Diretiva 95/46/CE.
4. Podemos encontrar referências ao princípio da responsabilidade ao longo do regulamento, mas mais concretamente nos seguintes considerandos e artigos:
   a) "(74) Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade com o presente regulamento, incluindo a eficácia das medidas";
   b) "Artigo 5º
   Princípios relativos ao tratamento de dados pessoais
   (...)
   2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n. 1 e ***tem de poder comprová-lo ('responsabilidade')****"*; e,

a) *"Artigo 24º*
Responsabilidade do responsável pelo tratamento
1. 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, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e ***poder comprovar que o tratamento é realizado em conformidade com o presente regulamento****"*

5. VRANAKI, Asma; HEYDER, Markus; and BELLAMY, Bojana, "Implementing and Interpreting the GDPR: Challenges and Opportunities", Centre for Information Policy Leadership, p. 10, 2016.
6. LE MÉTAYE, Daniel, "Whom to Trust? Using Technology to Enforce Privacy" in, Enforcing Privacy - Regulatory, Legal and Technological Approaches (editado por, David Wright e Paul De Hert), p. 414 e ss, 2016; V. BENNETT, Colin, "International privacy standards: can accountability be adequate?", Privacy Laws and Business International, August 2010.
7. V. artigo 24º do Regulamento (todas as referências legais, a menos que de outro modo indicado na nota, são para o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016.
8. LE MÉTAYE, *ibid*.
9. "Licitude, lealdade e transparência"; "Limitação das finalidades"; "Minimização dos dados"; "Exatidão"; "Limitação da conservação"; e, "Integridade e confidencialidade" (artigo 5º, n. 1).
10. Opinion 3/2010 *on the principle of accountability*.
11. WONG, Rebecca, "Data Security Breaches and Privacy in Europe", p. 20, 2013.
12. ARTICLE 29 WORKING PARTY, Opinion 3/2010, p. 5.
13. ARTICLE 29 WORKING PARTY, Opinion 3/2010, p. 6.
14. LE MÉTAYE, *ibid*.
15. LE MÉTAYE, *ibid*.
16. Sem prejuízo de cada um desses papéis ter responsabilidades diferentes.
17. Este conceito, vertido agora em princípio da legislação de proteção de dados, tem origem num relatório conjunto do Information and Privacy Commissioner de Ontário, Canada, e da Registratiekamer dos Países Baixos, *Privacy-Enhancing Technologies: The Path to Anonymity* (Volume I), 1st August 1995. Disponível em: http://tinyurl.com/yenjgns.
18. V. artigo 5º.
19. Artigo 26, número 3.
20. Artigo 82, número 5.
21. V. Considerando 80, artigo 4º, número 17, e artigo 27º.
22. Tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento, não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares.

23. V. artigo 82, número 2, *a contrario*, sem prejuízo do segundo parágrafo do número 3 do artigo 28º, o qual dispõe que o subcontratante deve informar imediatamente o responsável pelo tratamento se, no entender do subcontratante, alguma instrução violar o regulamento ou outras disposições do direito da União ou dos Estados-membros em matéria de proteção de dados.
24. Artigo 30º, número 5.
25. V. artigo 33º, número 5.
26. Considerandos (150), (152) e artigo 83º.
27. Considerando (150) e artigo 83º, números 5 e 6.
28. No caso nacional, resulta que a Secção III do Capítulo IV da Lei n. 67/98, de 26 de Outubro, manter-se-á em vigor.