DATA PROTECTION

NUNO SALDANHA

NOVO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

O QUE É? A QUEM SE APLICA? COMO IMPLEMENTAR?

FCA

Edição
FCA – Editora de Informática, Lda.
Av. Praia da Vitória, 14 A – 1000-247 Lisboa
Tel: +351 213 511 448
fca@fca.pt
www.fca.pt

Distribuição
Lidel – Edições Técnicas, Lda.
Rua D. Estefânia, 183, R/C Dto. – 1049-057 Lisboa
Tel: +351 213 511 448
lidel@lidel.pt
www.lidel.pt

Livraria
Av. Praia da Vitória, 14 A – 1000-247 Lisboa
Tel: +351 213 511 448 * Fax: +351 213 522 684
livraria@lidel.pt

ISBN edição impressa: 978-972-722-889-8
1.ª edição impressa: março 2018

Paginação: Carlos Mendes
Impressão e acabamento: Tipografia Lousanense, Lda. – Lousã
Depósito Legal n.º 438714/18
Capa: José M. Ferrão – *Look-Ahead*

ÍNDICE

O AUTOR

Licenciado em Direito pela Universidade Católica Portuguesa, tem diversas formações em diferentes áreas, nomeadamente Gestão Empresarial e Financeira, Gestão de Informação, Sustentabilidade, Auditoria Interna, Controlo de Gestão, Proteção de Dados, Fraude, Risco, Controlos Informáticos, Técnicas de Apresentação e Marketing.

Exerceu no Grupo Impresa (televisão e imprensa escrita) funções de Adjunto do Diretor Financeiro durante 2 anos, de Diretor de Controlo de Gestão durante mais de 15 anos, tendo sido o seu primeiro diretor, e criou e dirigiu durante 8 anos a Direção de Auditoria Interna, acumulando essas funções com as de Membro do Gabinete de Risco e Membro do Gabinete de Sustentabilidade. Foi ainda Secretário da Sociedade Suplente durante 12 anos.

É atualmente consultor independente, professor de Estratégia Empresarial no ISAL – Instituto Superior de Administração e Línguas da Madeira na Pós-Graduação em Gestão, e responsável pela implementação de soluções de *compliance* com o novo Regulamento Geral de Proteção de Dados na consultora Bi4all.

INTRODUÇÃO

Quando apresento a temática do Regulamento Geral de Proteção de Dados (RGPD) tenho por hábito frisar que este não é um tema da moda, mas sim um tema do momento. Com efeito, o RGPD não foi algo que apareceu do nada nem tão-pouco será algo que desaparecerá rapidamente, ao contrário da ideia que todos nós temos do que é "moda".

Mais do que uma moldura legal, o RGPD traduz uma mudança na abordagem às questões relacionadas com a segurança e privacidade dos dados pessoais.

O presente regulamento, que cria um conjunto de novos direitos do cidadão, novos procedimentos e novas obrigações para todas as entidades públicas e privadas, demorou cerca de 4 anos a ser elaborado e é fruto de inúmeras discussões, avanços e retrocessos, pressões e imposições, tendo finalmente visto a luz, com a aprovação no Parlamento Europeu e do Conselho Europeu (CE), no dia 27 de abril de 2016.

Ao contrário de uma qualquer diretiva da União Europeia (UE), a escolha da forma legislativa "regulamento" implica, por si só, uma mudança no paradigma regulatório, uma vez que, na data aprazada, esta legislação entra em vigor em toda a UE e, desse modo, no ordenamento jurídico português, não necessitando de ser transposta (como é o caso da diretiva).

Ficou desde logo estabelecido que o regulamento entraria em vigor no 20.º dia seguinte à sua publicação no "Jornal Oficial da União Europeia" e que seria aplicável a partir de 25 de maio de 2018. Portanto, foi dado um período de 2 anos para que as organizações que tratam dados pessoais se preparassem para a sua efetiva aplicabilidade. Existiram, assim, 6 anos entre a "primeira pedra" e a "entrega da obra".

O RGPD será diretamente aplicável, na mesma data, em todos os países da UE e também no Espaço Económico Europeu (Islândia, Liechtenstein, Noruega e Suíça).

Também este não será, ao contrário da moda, um tema que deixará de estar na ordem do dia pouco tempo depois da sua entrada em funcionamento.

Efetivamente, será no dia 25 de maio de 2018 que tudo começa, ou seja, será esta a data que marca o início de uma nova relação entre as organizações que tratam dados pessoais e os titulares desses dados, e será da relação que conseguirem estabelecer entre eles que o sucesso do regulamento, ou, mais propriamente, o sucesso da implementação do conjunto de direitos e obrigações constantes desse regulamento, se fará sentir com maior ou menor acuidade.

De qualquer forma, convém notar que este regulamento, em termos de efeitos práticos, e apesar de entrar em vigor em 2018, estende todos os seus efeitos ao passado, daí se dizer que é um documento normativo de efeito triplo: passado, presente e futuro. Toda a informação que as organizações europeias tratam, relativa a dados pessoais e que esteja na sua posse, vai ter de estar conforme este regulamento, vai ter de estar em *compliance*.

A "bola" já começou a rolar e, apesar de existir, e existirá sempre, quem discorde do nível de regulação ou da forma como esta é consubstanciada nesta peça, tanto as imposições para as organizações como a regulação dos direitos para as pessoas já não têm reversão.

Se procedermos à comparação deste regulamento com a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e livre circulação dos mesmos, ou seja, a diretiva que antecedeu este regulamento, e que foi transposta para a legislação portuguesa através da Lei n.º 67/98, de 26 de outubro, mais facilmente se compreendem as diferenças e as razões da nova regulamentação.

Diria que, face ao que se estava a passar na realidade europeia e mundial e ao modo como as organizações tratavam os dados pessoais, as autoridades europeias tiveram uma tripla preocupação:

- Como fazer com que os Estados-Membros se tornassem mais participantes e mais conscientes dos problemas relacionados com esta questão?
- Como chamar as pessoas, os titulares dos dados, para esta discussão?
- Como fazer com que as empresas e restantes organizações, responsáveis pelos tratamentos de dados, estivessem atentas às novas realidades de defesa dos direitos dos cidadãos?

A realidade globalizante da economia europeia, em todos os aspetos e também na questão dos dados pessoais, aliada à descoberta, já não tão recente, de que os

dados pessoais possuem um valor económico intrínseco, têm levado as organizações a fazerem grandes investimentos na recolha e tratamento de dados de milhões de consumidores europeus. Os Estados-Membros têm acompanhado esta questão e foram percebendo que não existe uma forma de "controlarem" e imporem sozinhos as obrigações que decorrem das leis nacionais, mais ainda quando a transferência de dados dentro da UE, portanto, dentro de "Espaço Comum", aliada ao novo mundo digital, é uma realidade diária e acima das suas próprias iniciativas legislativas.

A compreensão dessas duas novas realidades – os dados com valor económico e a inexistência de fronteiras digitais – levou os Estados-Membros da UE a decidirem que estava na hora de adotar uma legislação mais adequada aos novos tempos, mas também que a nova forma não poderia ser baseada numa diretiva europeia que, como sabemos, teria de ser transcrita por cada Estado-Membro, provavelmente em tempos diferentes e com *nuances* e aplicações diferentes. Era necessário um regulamento europeu. Os Estados-Membros perceberam que só com legislação, regras, períodos e sanções comuns seria possível adequarem a temática dos dados pessoais à realidade da Europa, cada vez mais ligada política, social e economicamente. Curiosamente, esta ideia ficou também vincada no modo como o regulamento trata, posteriormente, todas as questões relacionadas com países terceiros, na forma de tratamento de dados pessoais, levando, portanto, ao reconhecimento de que este tipo de questão já não pode ser só regulado num espaço como o europeu, sendo também necessário pensar num espaço realmente global.

A segunda preocupação que passou pelas mentes dos responsáveis europeus foi encontrar uma forma de chamar os cidadãos a envolverem-se nesta temática. É certo que já existia um conjunto de direitos na legislação anterior que protegia os titulares dos dados, e que os mais informados iam exercendo. Mas era preciso ir mais além. Era necessário informar os titulares dos dados de que esta era uma legislação pensada e estruturada para eles e com consequências para quem os não respeitasse. O regulamento, ao considerar 12 tipos diferentes de direitos, autónomos uns dos outros, fez a sua parte. Estamos a atender ao direito à proteção dos dados pessoais (artigo 1.º), direito à informação (artigo 13.º), de acesso (artigo 15.º), de retificação (artigo 16.º), ao apagamento dos dados (artigo 17.º), à limitação do tratamento (artigo 18.º), à notificação (artigo 19.º), de portabilidade dos dados (artigo 20.º), de oposição (artigo 21.º), a não ficar sujeito a decisões automatizadas (artigo 22.º), a ser avisado em caso de uma violação de dados pessoais (artigo 34.º) e, claro, os direitos relacionados com os princípios do tratamento de dados pessoais (e constantes do artigo 5.º), nomeadamente que os dados sejam objeto

de tratamento lícito, leal e transparente, recolhidos com finalidades determinadas, adequados, pertinentes, limitados, exatos, atualizados, etc.

A declaração deste conjunto de direitos é a prova de que é realmente um regulamento para os cidadãos europeus, ou seja, são eles que estão na primeira linha de preocupação das autoridades europeias e são a razão desta regulamentação.

Não valia a pena trazer os Estados-Membros e as pessoas para este debate se não se conseguissem trazer também as organizações. Com efeito, a cada direito atribuído a um cidadão cabe uma obrigação por parte de cada organização.

Se repararmos nos efeitos da anterior legislação, nomeadamente nas sanções por incumprimento, percebe-se que a melhor forma que as organizações europeias encontraram de trazer para o debate as entidades que tratam dados pessoais foi mexendo no valor das coimas.

E as entidades europeias fizeram-no de uma forma eficaz, talvez até em demasia. Ao estabelecerem um valor sancionatório mais elevado, com coimas que podem chegar aos 20 milhões de euros ou 4% do valor de faturação anual das empresas ou do grupo de empresas a que pertencem, obrigaram estas instituições a perceber que, afinal, desta vez tinham mesmo de prestar muita atenção ao tema. Foi, sem dúvida, o meio mais eficaz de trazer ao debate aqueles que efetivamente fazem o tratamento de dados pessoais.

Como é do conhecimento geral, há muito que os dados pessoais deixaram de ser apenas isso – "dados pessoais". Inicialmente, as organizações faziam recolha de dados dos seus clientes, fornecedores e público em geral sem terem ainda a perceção da importância dessa informação. Consideravam mesmo, muitas vezes, que arquivavam informação desnecessária, com custos excessivos e não rentabilizáveis.

No entanto, rapidamente se aperceberam do valor económico dessa informação. Vivemos hoje numa sociedade de informação que é já o resultado de uma enorme transformação digital e, nesse sentido, numa sociedade que assenta em dados, principalmente em dados pessoais. Vivemos numa sociedade de motores de busca digitais, de *cloud*, de Internet das Coisas (*Internet of Things* – IoT), de *Big Data*, de BYOD (*Bring Your Own Device*) de comunicações digitais móveis, enfim, hoje conhecer hábitos de consumo, tendências, gostos e necessidades é uma vantagem competitiva muito importante para as organizações.

Hoje, as empresas são ávidas na recolha de informação dos seus clientes e potenciais clientes e não poupam esforços ou investimentos para conseguirem esse

objetivo. É necessário convencer as pessoas a voluntariamente confiarem os seus dados e para isso é também preciso oferecer-lhes vantagens em troca.

Alguém, em tempos, comparou uma qualquer organização que recolhe e processa dados pessoais a uma entidade bancária. O titular dos dados "deposita" a sua informação numa organização, confiando em três pressupostos:

- Os dados estão seguros;
- Os dados são trabalhados para que a organização lhe proporcione um melhor serviço;
- A informação contida nos seus dados irá trazer-lhe vantagens diretas e imediatas.

No fundo, o que a atividade bancária proporciona aos clientes é:

- A segurança dos seus depósitos, em termos físicos e de valor;
- A certeza de que o banco proporciona um conjunto de serviços bancários;
- O pagamento de juros em resultado desse mesmo depósito.

É, sem dúvida, uma comparação feliz e que obriga as organizações que recolhem e tratam dados pessoais a terem um cuidado extremo na forma como recolhem, tratam e armazenam a informação que lhes é confiada.

Ao longo das próximas páginas, preparei uma espécie de resumo dos temas presentes no RGPD, na pretensão de ajudar as organizações a implementarem novos procedimentos técnicos de tratamento de dados pessoais, assim como a adotarem novos sistemas de gestão operacional da proteção de dados. Dividiu-se o livro em capítulos, maioritariamente coincidentes com os capítulos do regulamento. Em algumas situações autonomizaram-se temas. Utilizou-se essencialmente o texto do próprio regulamento, seja do articulado, seja das considerações iniciais, por vezes com outra organização, mas sempre com a vontade de facilitar a leitura do texto oficial, principalmente a pessoas menos familiarizadas com temas jurídicos ou com as sistematizações próprias destas temáticas.

Este é um ponto de partida. O conhecimento detalhado da regulamentação constante no RGPD permite compreender o que as organizações têm de fazer para se colocarem em *compliance*. No último capítulo deste livro dou 14 dicas para iniciar a implementação do regulamento nas organizações. Poderiam ser mais ou menos, não interessa o número ou os passos a dar, mas sim a necessidade imperiosa

de o fazer. Quando se passa para uma atitude mais prática face ao regulamento, acredito que é necessário apresentar uma abordagem sistemática do problema. O RGPD não é só uma questão legal, não se trata apenas de processos internos nem de uma questão de tecnologia. A implementação de uma solução de *compliance* obriga a uma abordagem integrada destas questões. O RGPD é uma questão legal, processual e tecnológica e tal não deve ser esquecido nem facilitado.

Espero que estas notas e resumos lhes sejam úteis, e que se transformem num verdadeiro guia prático.

Nuno Saldanha

1

A **HISTÓRIA EUROPEIA** DA **PROTEÇÃO** DE **DADOS**

A história europeia da proteção de dados começa logo após a Segunda Guerra Mundial, com a criação do Conselho da Europa (CdE), que reuniu 10 países europeus com o objetivo de promover o Estado de direito, a democracia e os direitos humanos. Em 1950, foi adotada a Convenção Europeia dos Direitos do Homem (CEDH), que entrou em vigor em 1953 no ordenamento jurídico de todos os países signatários do CdE. Em 1959, com a criação do Tribunal Europeu dos Direitos do Homem (TEDH), garantiu-se que todos os Estados cumpriam as suas obrigações, cabendo ao TEDH apreciar as queixas apresentadas por cidadãos, grupos de cidadãos, organizações não governamentais (ONG) ou pessoas coletivas que alegassem violações dessa mesma convenção.

Atualmente, todos os Estados-Membros da UE pertencem ao CdE.

O direito à proteção de dados pessoais faz parte dos direitos consagrados na CEDH, nomeadamente no artigo 8.º, que garante o direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência.

Artigo 8.º

1. *Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.*
2. *Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.*

O TEDH, no âmbito da sua atividade jurisdicional, esclareceu que este artigo 8.º não só obriga os Estados a absterem-se de praticar atos suscetíveis de violarem os direitos aí consagrados, como impõe uma atitude positiva de garantir de forma ativa o respeito efetivo pela vida privada e familiar. De certa maneira, precisamente o que a legislação da UE procurou desenvolver.

Mais tarde, em 1981, e em consequência do surgimento, nos anos 60 do século XX, das tecnologias de informação e da necessidade, na década seguinte, da existência de um conjunto de resoluções sobre proteção de dados, com base precisamente no artigo 8.º, foi estabelecida a Convenção 108.

2

A **HISTÓRIA PORTUGUESA** DA **PROTEÇÃO** DE **DADOS**

A Constituição Portuguesa de 1976, no seu artigo 35.º, foi o primeiro texto jurídico que, de uma forma sistematizada, abordou a temática da proteção de dados. Ainda ligando muito o tema às questões da informática, atribuía já um conjunto de direitos aos titulares dos dados, desde logo o direito à proteção dos dados pessoais, à informação, ao acesso aos seus dados pessoais e à retificação.

Na senda da proteção das pessoas e na atribuição de direitos e garantias, afirmava a proibição de utilização dos dados para fins discriminatórios, nomeadamente no que se referia a convicções políticas, religiosas ou vida privada.

Esta é a versão inicial do artigo 35.º da Constituição Portuguesa:

Artigo 35.º (Utilização da informática)

1. *Todos os cidadãos têm o direito de tomar conhecimento do que constar de registos mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.*
2. *A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos.*
3. *É proibida a atribuição de um número nacional único aos cidadãos.*

Atualmente, o mesmo artigo 35.º vai um pouco mais longe, mas não esconde as origens:

Artigo 35.º (Utilização da informática)

1. *Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos previstos na lei.*
2. *A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.*
3. *A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.*

– Continua –

O QUE É O RGPD

3

O RGPD é um regulamento europeu, aprovado pelo Parlamento Europeu e pelo CE, que considera a proteção das pessoas singulares, relativamente ao tratamento dos seus dados pessoais, um direito fundamental, independentemente da nacionalidade ou local de residência, contribuindo, assim, para a realização de um espaço de liberdade, segurança e justiça e para uma união económica e social dos cidadãos do espaço europeu.

O que o regulamento pretende é não só harmonizar e assegurar a defesa dos direitos e liberdades fundamentais das pessoas singulares, mas também garantir a livre circulação de dados pessoais entre os Estados da UE.

Um regulamento europeu, ao contrário de uma diretiva, uma outra forma legislativa da UE, é de aplicação direta no sistema jurídico dos diferentes Estados-Membros, sem necessidade de ser transposto para o direito interno, algo que acontece com a diretiva.

Verifica-se, portanto, um triplo objetivo que a UE procurou alcançar através deste regulamento: harmonização da legislação, coerência do tratamento de dados pessoais em todo o espaço europeu e segurança jurídica, que só com uma aplicação uniforme em toda a UE se torna mais fácil de assegurar.

Apesar de se aplicar a toda a UE, este regulamento deixou ainda algum espaço para que, em certas situações, os Estados-Membros possam legislar, como as questões ligadas à aplicação prática do regulamento, nomeadamente a organização interna da autoridade de controlo.

3.1 PORQUÊ A NECESSIDADE DE UM RGPD?

A necessidade que a UE sentiu de legislar em matéria de proteção de dados pessoais resultou de vários fatores, nomeadamente o aumento dos fluxos transfronteiriços e, em consequência, uma cada vez maior integração económica, fruto, sem dúvida, da criação do mercado único, mas também em resultado de um intercâmbio de dados que se verifica cada vez mais entre sectores público e privado, de uma evolução tecnológica contínua, uma globalização já imparável, uma cada vez maior recolha e partilha de dados, tidos já como um valor económico muito real e mensurável, e a utilização, por todas as organizações, sejam públicas ou privadas, de dados pessoais em larga escala.

Toda esta evolução exigiu, por parte da UE, uma tomada de posição, nomeadamente através da criação de um quadro legal de proteção dos dados pessoais e

de uma aplicação rigorosa dessas mesmas regras, de forma a gerar a confiança necessária quer aos cidadãos, para disponibilizarem os seus dados, já que poderão ter um controlo sobre os mesmos, quer às organizações, no que respeita ao desenvolvimento da economia digital no mercado interno da UE.

3.2 PORQUE VEM O RGPD SUBSTITUIR A ANTIGA DIRETIVA?

Pode invocar-se que muitas destas questões já estavam endereçadas pela antiga Diretiva n.º 95/46/CE, transposta para a legislação portuguesa através da Lei n.º 67/98. No entanto, um facto é inegável: pelo carácter próprio da forma de legislar, a Diretiva possibilitou que cada país transcrevesse com alguma liberdade o seu conteúdo, o que acabou por se traduzir numa produção avulsa de legislação acerca desta temática, originando uma aplicação pouco uniforme pelos países da UE, e o que gerou uma insegurança jurídica pouco favorável ao desenvolvimento económico, com as consequentes distorções da concorrência entre os Estados e a dificuldade, por parte das autoridades nacionais, de cumprirem as obrigações de controlo.

Tudo isto gerou a necessidade de harmonização numa nova legislação: o RGPD.

Apesar da importância deste regulamento e do espaço central que irá ocupar em todo o edifício legislativo da UE, no que concerne à regulação do tratamento de dados pessoais, este não será o único instrumento jurídico aplicável nesta matéria.

Para além do RGPD, haverá que ter em conta qualquer outra regulamentação da UE, nomeadamente aspetos mais temáticos, descritos no Capítulo 30 deste livro, a legislação dos Estados-Membros, sendo de realçar, em Portugal, os temas relacionados com a CNPD, todas as ações e indicações desenvolvidas pelas autoridades de controlo da UE e dos Estados-Membros e, claro, em última análise, mas de importância extrema, a interpretação que os tribunais nacionais e da UE irão fazer deste regulamento.

4

A **QUEM** E **QUANDO** SE **APLICA** O **RGPD**

O RGPD não se aplica:

- A questões de defesa dos direitos e liberdades fundamentais;
- À livre circulação de dados pessoais relacionados com atividades fora do âmbito de aplicação do direito da UE, nomeadamente segurança nacional;
- A atividades relacionadas com a política externa e de segurança comum da UE;
- Ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades pessoais ou domésticas;
- Ao tratamento de dados pessoais relativos a pessoas coletivas, nomeadamente a sua denominação, forma jurídica e os seus contactos;
- A atividades de tratamento para efeitos de proteção das pessoas singulares no que respeita à prevenção, investigação, deteção e repressão de infrações penais ou execução de sanções penais.

Como se pode observar, existe um conjunto alargado de sujeitos jurídicos a quem se aplica o regulamento e que estão todos em contacto com o titular dos dados, ou seja, aquele que é a razão essencial deste documento normativo.

Falamos, então, de quem?

- **Do responsável pelo tratamento e do subcontratante** – aquele que efetivamente recolhe e trata dados pessoais;
- **Das autoridades nacionais** – essencialmente as autoridades de controlo, responsáveis por fiscalizar o cumprimento deste regulamento, mas também de o dar a conhecer, de o "evangelizar";
- **Dos destinatários** – aqueles que recebem comunicações de dados pessoais;
- **De terceiros** – todos aqueles que não sendo titulares de dados, responsáveis pelo tratamento de dados ou subcontratantes, estão autorizados a tratar dados pessoais.

9

PRINCÍPIOS DO RGPD

Artigo 5.º e seguintes / Considerando n.º 39 e seguintes

O artigo 5.º enumera vários princípios relativos ao tratamento de dados pessoais, o que se consubstancia num conjunto de direitos que acrescem aos que constam dos artigos 12.º e seguintes, Capítulo III do RGPD:

- Princípio da livre circulação;
- Princípio da licitude, lealdade e transparência;
- Princípio do propósito limitado;
- Princípio da minimização dos dados;
- Princípio da precisão;
- Princípio do limite à retenção dos dados;
- Princípio da segurança dos dados;
- Princípio da responsabilidade.

9.1 PRINCÍPIO DA LIVRE CIRCULAÇÃO

Está presente no artigo 1.º do RGPD e é a condição *sine qua non* para a sua existência. O regulamento existe para proteger o tratamento de dados pessoais das pessoas singulares e a livre circulação desses dados. Numa sociedade democrática, baseada na economia de mercado e cada vez mais alicerçada na economia digital, proteger a circulação da informação e, por isso, proteger a circulação dos dados pessoais torna-se essencial, com vista a preservar os direitos e as liberdades das pessoas singulares.

9.2 PRINCÍPIO DA LICITUDE, LEALDADE E TRANSPARÊNCIA

É a base de todo o sistema consagrado no regulamento. Os dados pessoais, na sua relação com o titular dos dados, têm de ser objeto de um tratamento lícito, leal e transparente.

9.2.1 Tratamento lícito

Ser objeto de um tratamento lícito implica a existência, desde logo, de uma recolha lícita, portanto, baseada no consentimento do titular dos dados, e para uma finalidade específica, ou, em certas ocasiões, de um fundamento legítimo previsto na lei – nacional ou comunitária – ou no regulamento que permita esse tratamento.

As pessoas singulares a quem os dados dizem respeito devem ser avisadas dos riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais e devem ser também alertadas para os meios de que dispõem para exercer esses direitos.

Para o regulamento existe licitude:

- Se o titular tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
- Se o tratamento for necessário para a execução de um contrato, no qual o titular dos dados é parte, ou para diligências pré-contratuais, a pedido do titular dos dados;
- Se o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito. É o caso das entidades patronais, no que respeita aos dados dos seus funcionários;
- Se o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- Se o tratamento for necessário para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento;
- Se o tratamento for necessário para defender os interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. Por aqui se verifica que o titular dos dados pode não ser a única pessoa com interesses legítimos.

18

AVALIAÇÃO DE **IMPACTO** SOBRE A **PROTEÇÃO** DE **DADOS** (***DATA PROTECTION IMPACT ASSESSMENT*** – **DPIA)**

Artigo 35.º / Considerando n.º 89 e seguintes / "WP 248 rev.01" e "WP 251 rev.01"

Quando um responsável pelo tratamento tiver a noção de que, face a uma necessidade da sua organização, vai ter de utilizar uma nova tecnologia, ou perceba que, tendo em conta a natureza, âmbito, contexto ou finalidade do tratamento de dados que vai ou pretende iniciar, é suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, esse responsável deve proceder, ainda antes do início do tratamento de dados, a uma avaliação do impacto dessas operações de tratamento sobre esses direitos e liberdades, devendo, inclusivamente, solicitar o parecer do DPO, nos casos em que este exista. A Avaliação de Impacto sobre a Proteção de Dados (AIPD ou DPIA, em inglês) é, portanto, um processo que ajuda as organizações a identificar e a minimizar riscos, a avaliar as necessidades e proporcionalidades do tratamento a efetuar, a gerir os riscos para os direitos e liberdades das pessoas e a determinar as medidas necessárias para fazer face a esses riscos.

As avaliações de impacto são instrumentos de responsabilização, de demostração de conformidade, e são obrigatórias, nos termos do regulamento (artigo 35.º), quando:

- O tratamento de dados for suscetível de implicar um risco elevado para os direitos e liberdades das pessoas singulares;
- Existe uma avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseados em tratamento automatizado, incluindo a definição de perfis, ou seja, *qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações* (número 4 do artigo 4.º). E, com base nessa avaliação, produzem-se efeitos na esfera jurídica das pessoas singulares;
- Existem operações de tratamento de dados sensíveis (número 1 do artigo 9.º) ou relacionados com condenações penais, em larga escala;
- Existe um controlo sistemático de zonas acessíveis ao público em larga escala.

24

AUTORIDADES DE CONTROLO

A criação, por este regulamento, da entidade "autoridade de controlo", obrigatória nos diferentes Estados-Membros, é o elemento essencial para uma proteção eficaz das pessoas singulares no que respeita ao tratamento de dados pessoais. Os Estados podem, inclusivamente, criar mais do que uma autoridade de controlo, desde que fique claro qual vai ser a principal.

Nos termos do número 21 do artigo 4.º, *Autoridade de Controlo é uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51.º e, de acordo com o número 22 do mesmo artigo 4.º, Autoridade de Controlo Interessada é uma autoridade de controlo afetada pelo tratamento de dados pessoais pelo facto de*:

a) O responsável pelo tratamento ou o subcontratante estar estabelecido no território do Estado-Membro dessa autoridade de controlo;

b) Os titulares de dados que residem no Estado-Membro dessa autoridade de controlo serem substancialmente afetados, ou suscetíveis de o ser pelo tratamento de dados; *ou*

c) Ter sido apresentada uma reclamação junto dessa autoridade de controlo.

Nos termos da definição apresentada, cabe aos Estados-Membros criar uma ou mais entidades, com um estatuto de independência, que terão por missão:

- Zelar pela fiscalização do RGPD e, dessa forma, defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados e, nos termos do artigo 1.º, facilitar a livre circulação dos dados pessoais na UE;
- Contribuir para a aplicação coerente do RGPD em toda a UE.

A principal característica das autoridades de controlo é a independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos, uma vez que os seus membros não estão sujeitos a influências externas, diretas ou indiretas, no desempenho das funções e no exercício dos poderes, não solicitando nem recebendo instruções de ninguém.

29

SANÇÕES

Artigos 58.º (número 2), 83.º e 84.º / Considerando n.º 148 e seguintes / "WP 253"

A imposição de sanções é geralmente uma condição *sine qua non* para a efetiva observância e execução de regras estabelecidas. O regulamento, no artigo 84.º, refere que cabe aos Estados-Membros estabelecer as regras relativas a outras sanções (para além das coimas), aplicáveis em caso de violação do disposto no RGPD. Estas deverão ser efetivas, proporcionadas e dissuasivas. Os Estados-Membros estão obrigados, após o estabelecimento das novas sanções, a notificar e a comunicar à Comissão o conteúdo dessas normas internas.

No sentido de ajudar as autoridades de controlo a identificar as melhores medidas corretivas por forma a sanar a infração, o "WP 253" apresenta a utilização de quatro princípios:

- As infrações ao regulamento devem conduzir à imposição de sanções equivalentes;
- Como todas as medidas corretivas escolhidas pelas autoridades de controlo, as coimas devem ser *efetivas, proporcionadas e dissuasivas*;
- A autoridade de controlo competente fará uma avaliação *em cada caso individual*;
- *A abordagem harmonizada das coimas no domínio da proteção de dados exige a participação ativa e o intercâmbio de informações entre autoridades de controlo*.

No RGPD pode encontrar-se três tipos de sanções:

- **Sanções penais** – deverão ser definidas pelos Estados-Membros quais as sanções penais, aplicáveis por violação do RGPD e por violação de normas nacionais, adotadas em conformidade com o regulamento. O regulamento, nos seus considerandos, propõe mesmo, a título de exemplo, a privação dos lucros auferidos em virtude dessa violação, chamando, no entanto, a atenção para o princípio de que ninguém pode ser condenado mais do que uma vez pelo mesmo delito;
- **Sanções administrativas** – nomeadamente as que advêm dos poderes de correção das autoridades de controlo, ou seja, o poder de advertir, repreender, ordenar ou impor uma certa atuação;

31 FORMULÁRIOS

Um dos aspetos práticos da implementação de um sistema de *compliance* nas diferentes organizações é a necessidade de estas se munirem de um conjunto de formulários que regulem a sua relação com os titulares dos dados.

Este é realmente um aspeto prático de grande importância, porque é aqui, no primeiro contacto com os cidadãos titulares dos dados, que se verifica a forma como as organizações incorporam os princípios deste regulamento.

O RGPD define o consentimento, no número 11 do artigo 4.º, como *uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento*.

Estes formulários irão ser usados em situações diferentes, consoante as necessidades do responsável pelo tratamento e os canais utilizados. Referimo-nos, naturalmente, aos formulários utilizados em *sites* da Internet, em redes sociais, como *Facebook*, *Instagram* ou *Twitter*, ou em aplicações móveis, ou seja, numa multiplicidade de opções que a economia digital hoje nos oferece.

Cada uma das situações apresenta desafios diferenciados, no entanto, acreditamos que existe um conjunto de princípios que deverão constar em todos, daí incluirmos aqui algumas orientações que podem/devem ser seguidas na construção dos formulários:

- Deve ser utilizada uma linguagem muito simples, compreensível e de fácil acesso. Os titulares dos dados, ao darem o seu consentimento, não devem precisar de dicionários ou de ler duas vezes o texto para perceberem qual é a mensagem. A linguagem tem de ser simples, sem segundos sentidos, clara e inequívoca;
- Tem de existir uma ação positiva, uma opção de aceitação, não basta uma decisão por exclusão. O titular dos dados tem de demonstrar claramente a sua opção por fornecer os dados. O responsável pelo tratamento tem de criar um formulário que dê a iniciativa ao titular e, por exemplo, não criar apenas "caixas pré-marcadas ou de exclusão". Existe um termo inglês, *opt-in*, que significa isso mesmo, uma expressão da vontade do utilizador, afastando-se a sua presunção de aceitação pelo silêncio;
- Os formulários devem pretender obter consentimentos caso a caso. Não deve ser aproveitado um formulário de *marketing* para também obter consentimento para outros efeitos. Cada situação deve ser tratada individualmente e o consentimento nunca deverá ser condicionado ou condicionar a uma qualquer inscrição,

32

CONCLUSÃO: COMO SE **PREPARAR** PARA **ESTAR** ***COMPLIANCE***

Com a aproximação do dia 25 de maio de 2018, data oficial a partir de qual o regulamento se torna aplicável, e mesmo depois desse dia, muitas empresas não saberão o que fazer para estar em conformidade com o regulamento. Como começar? Qual o primeiro passo? E o segundo?

Existe muita literatura disponível, principalmente em *sites* da Internet, na qual se tenta calendarizar, elencar, disponibilizar e ajudar a conseguir este desiderato. Estes são os nossos 14 passos:

1. Informação e formação, ou seja, ainda antes de qualquer procedimento mais direto, as organizações devem procurar informar e formar os seus colaboradores da existência do novo regulamento. Qualquer que seja o nível do colaborador, ele deve saber que algo mudou, que os titulares dos dados já não são apenas sujeitos passivos, que a organização é responsável pela prática de qualquer um dos colaboradores. A organização tem de antecipar o impacto do RGPD.
2. Saber que dados pessoais existem na sua organização, onde estão localizados, quem são os "donos" desses dados, qual o fluxo de recolha, de uso e de processamento. Também é conveniente saber se os dados estão em papel ou em formato informático, e o modo como são partilhados. A organização deve documentar todos esses fluxos e criar um sistema de registo de dados que tenha em conta a categoria dos dados, a finalidade do tratamento, o prazo de conservação e o âmbito geográfico.
3. Faça o *assessment* da tecnologia e verifique até que ponto ela já responde às exigências do regulamento.
4. A organização já tem políticas de segurança? Políticas de privacidade? Então é tempo de revisitar essas políticas e adequá-las ao novo regulamento.
5. Prepare a sua organização para fazer face aos direitos dos titulares dos dados. Crie procedimentos internos para responder em tempo útil aos pedidos. Lembre-se de que a informação dos titulares dos dados é essencial à sua atividade.
6. Reveja o consentimento dos titulares dos dados, adeque ao regulamento e atualize essa informação.
7. Reveja e atualize os formulários dentro da sua organização. Adeque-os à nova realidade e aos novos direitos dos titulares dos dados.
8. Verifique se a sua organização recolhe e trata dados sensíveis e dados de crianças, e proceda de acordo com o regulamento.

9. Verifique se a sua organização necessita de proceder ao registo de atividades de tratamento de dados e atue em conformidade.
10. Analise todos os contratos com subcontratantes.
11. Verifique se a sua organização necessita de designar um DPO para assumir a responsabilidade pela conformidade da proteção de dados.
12. Verifique se a organização adotou medidas técnicas e organizativas para garantir a segurança dos dados que possui, nomeadamente encriptação e mascaramento de dados. Confirme se a proteção dos dados é efetuada desde a conceção e por defeito.
13. Verifique se necessita de proceder a qualquer tipo de avaliação de impacto sobre a proteção de dados ou a uma consulta prévia.
14. Certifique-se de que adotou procedimentos para detetar, denunciar, reportar e investigar violações de dados.

E a seguir pode "descansar"…

DATA PROTECTION

A aprovação de um Regulamento Geral de Proteção de Dados (RGPD) relativo à proteção das pessoas singulares (tratamento de dados pessoais e livre circulação desses mesmos dados) produziu uma rutura no modo como a proteção de dados tem sido entendida nos diferentes contextos legislativos dos estados-membros da União Europeia (UE).

A centralização normativa, conseguida através da aprovação de um regulamento europeu, obriga, por si só, todos os estados da UE, no mesmo momento e da mesma forma, a capacitar os seus cidadãos de um conjunto alargado de direitos: desde a proteção da sua informação, o acesso aos seus dados, à retificação, ao apagamento, ao direito de oposição e até de portabilidade.

Da mesma forma, obriga todas as organizações, públicas ou privadas, que tratam de dados pessoais, a respeitar e fazer cumprir os direitos dos titulares. O seu incumprimento poderá levar a um conjunto de sanções que, no pior cenário, podem atingir os 20 milhões de euros ou 4% do volume de negócios anual ao nível mundial! São motivos mais do que suficientes para se olhar para este regulamento europeu com uma atenção muito especial.

Este livro destina-se a apoiar juristas, encarregados de proteção de dados, implementadores de processos de *compliance*, assim como todos os gestores de topo nas diferentes organizações.

TEMAS:

- **O que é o Regulamento Geral de Proteção de Dados?**
- **A quem se aplica?**
- **Qual a evolução histórica da regulação da proteção de dados em Portugal e na Europa?**
- **Quais são os princípios consagrados no RGPD?**
- **Que direitos são atribuídos aos titulares dos dados?**
- **Quais são as obrigações das organizações no tratamento de dados pessoais?**
- **Que tipo de sanções pode ser aplicado? E por quem?**
- **Que processo deve implementar para colocar a sua organização em conformidade com o RGPD?**

Um guia prático que resume os principais temas do RGPD, comentados de forma simples, clara e útil! Inclui 14 passos para iniciar a implementação do regulamento nas organizações.

NUNO SALDANHA

Licenciado em Direito, com diversas formações nas áreas da Gestão Empresarial e Financeira. Professor no Ensino Superior e responsável pela implementação de processos de *compliance* no âmbito do RGPD numa importante consultora nacional.

Aceda de forma fácil ao **RGPD** através da nossa página www.fca.pt.

ISBN 978-972-722-889-8

9 789727 228898

FCA

GRUPO LIDEL

www.fca.pt