Conhecer não é demonstrar nem explicar. É aceder à visão. A. Saint-Exupéry

2017, ANO V, N.º 7

AB INSTANTIA

REVISTA DO INSTITUTO DO CONHECIMENTO AB

ALMEDINA

ABREU ADVOGADOS
INSTITUTO DO CONHECIMENTO AB

OS CONCEITOS DE *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT* NO ÂMBITO DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS*

FILIPA IGLÉSIAS**

1. Depois de quatro anos de negociações, o Novo Regulamento Geral de Proteção de Dados – Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (RGPD) – foi publicado no dia 4 de maio de 2016 no Jornal Oficial da União Europeia. O RGPD revoga a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 (a Diretiva), relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

A Diretiva, que se manteve em vigor durante quase 23 anos, começou a ser redigida no início dos anos 90 com o duplo objetivo de assegurar a livre circulação de dados pessoais de um Estado-membro para outro, ao mesmo tempo que se garantia a proteção dos direitos fundamentais das pessoas. Assim, se por um lado se proclamava que o respeito dos direitos e liberdades fundamentais deve ser assegurado, nomeadamente o direito à vida privada (reconhecido não só no artigo 8.º da Convenção europeia para a proteção dos direitos do Homem e das liberdades fundamentais como nos princípios gerais do direito comunitário), por outro, o estabelecimento e o funcionamento do mercado interno exigia, nos termos do artigo 7.º A do Tratado, a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais.

A Diretiva já preconizava nos seus Considerandos que a integração económica e social provocaria necessariamente um aumento sensível dos fluxos transfronteiriços de dados pessoais entre todos os intervenientes, privados ou públicos, na vida económica e social dos Estados-membros, sendo que o intercâmbio de dados pessoais entre empresas estabelecidas em diferentes Estados-membros tenderia a intensificar-se. Preconizava ainda que as administrações dos Estados-membros

* O texto corresponde, em síntese, à conferência proferida no Seminário *Privacidade e Compliance nas entidades privadas e públicas – A contagem decrescente do Regulamento Geral de Proteção de Dados*, organizado pelo *Instituto do Conhecimento Abreu Advogados* no dia 4 de maio de 2017 (Lisboa, Câmara de Comércio e Indústria Portuguesa).

** Mestre em *Gestão das Indústrias Criativas*. Pós-Graduada em Propriedade Intelectual
Advogada AB (2007-2017)

seriam chamadas, por força do direito comunitário, a colaborar e a trocar entre si dados pessoais a fim de poderem desempenhar as suas atribuições ou executar tarefas por conta de uma administração de outro Estado-membro, no âmbito do espaço sem fronteiras internas que o mercado interno havia constituído. Com esse pano de fundo, estabeleceu-se então um conjunto de Princípios segundos os quais o tratamento de dados pessoais deve sempre processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais.

Porém, tratando-se de uma Diretiva, esta vinculava os Estados-membros destinatários quanto ao resultado a alcançar, deixando às instâncias nacionais a competência quanto à forma e aos meios (artigo 249º do Tratado de Roma). No processo de transposição para a ordem interna que uma Diretiva impõe, os Estados-membros dispõem de uma certa margem de liberdade na implementação das regras adotadas a nível comunitário.

A transposição da Diretiva em diferentes momentos resultou assim, em matéria de proteção de dados pessoais, num *puzzle* legislativo com diversos graus de exigências e diferenças significativas de país para país na interpretação e atuação das autoridades locais.

Já o Regulamento, nos termos do artigo 288.º do Tratado da União Europeia, é obrigatório em todos os seus elementos e diretamente aplicável em todos os 28 Estados-membros, tornando-se assim parte integrante do ordenamento jurídico interno sem necessidade de um ato que formalmente o receba. A opção por este ato legislativo da União Europeia neste âmbito da proteção de dados pessoais pretendeu reduzir a fragmentação jurídica e proporcionar uma maior segurança, introduzindo um conjunto harmonizado de regras de base, melhorando a proteção dos Direitos Fundamentais das pessoas singulares e contribuindo para o bom funcionamento do mercado interno.

Para a construção do novo Regulamento pesou ainda o facto de a data da Diretiva ter coincidido, não só com o alargamento da União Europeia, como com o advento das novas tecnologias e o uso generalizado de computadores pessoais com acesso à Internet, o que conduziu a uma rápida desatualização do texto face à realidade do uso e da circulação de dados em grande escala, que não podia então ser previsto e regulado em igual medida.

De facto, a rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados, cuja recolha e partilha atingiram uma escala sem precedentes, movimentando-se com uma rapidez tal que suplanta a capacidade de adaptação e controlo por parte dos seus titulares (se não tiverem forma de os gerir de início e por defeito, como adiante veremos).

A circulação transfronteiriça de dados pessoais já era, porém, antevista na Diretiva, ao destacar o reforço da cooperação científica e a introdução coordenada de novas redes de telecomunicações na Comunidade que se adivinhavam para breve.

O novo Regulamento, além de atualizar as questões levantadas pela realidade tecnológica entretanto surgida, vem finalmente garantir uma verdadeira harmonização legislativa ao nível da proteção de dados em todos os países na União Europeia, estabelecendo para tal um período transitório de 2 anos de adaptação até à sua total aplicação a 25 de maio de 2018.

2. O RGPD introduz alterações significativas às regras de proteção de dados, preconizadas pela Diretiva, impondo às organizações novas obrigações, cujo incumprimento é punido por elevadas coimas que podem ascender a 4% da faturação anual global ou a €20.000.000,00, consoante o valor mais elevado.

O Regulamento introduz, ainda, outras novidades importantes a nível organizacional tais como a introdução dos deveres de *Accountability*, a realização de avaliações de impacto sobre a proteção de dados (*Privacy Impact Assessments* – PIA), a notificação obrigatória às Autoridades de Proteção de Dados (CNPD) em caso de violações de segurança (*data breaches)*, a nomeação de Encarregados de Proteção de Dados (*Data Protection Officers* – DPO), ou o reforço da segurança dos dados.

O conceito de dados pessoais, além de clarificado, é alargado a qualquer informação relativa a uma pessoa singular identificada ou identificável, com um maior nível de alcance na interpretação daquilo que se entende por dado pessoal. Resultam ainda novos direitos para os titulares dos dados, como o direito à portabilidade dos dados, o direito ao esquecimento e o direito de oposição ao *profiling*.

As regras para obtenção do consentimento dos titulares passam a ser muito mais exigentes, não podendo aquele ser tácito e devendo ser demonstrável, exigindo-se o consentimento explícito para o tratamento de dados sensíveis.

Outra novidade é a introdução de novos princípios e conceitos que devem nortear o tratamento dos dados como o *Privacy by design* and *by default*, ou a pseudonimização dos dados.

Os grandes Princípios já estabelecidos na Diretiva mantiveram-se, tais como a obrigação de tratar os dados pessoais de forma lícita e com respeito pelo princípio da boa fé; proceder à sua recolha somente para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma

incompatível com essas finalidades; garantir que os dados recolhidos e tratados são adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados; garantir ainda que os dados pessoais sejam exatos e, se necessário, atualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou retificados os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente; e finalmente que sejam conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior.

Porém, o Regulamento, tendo em conta a nova dimensão social e económica de utilização de dados pessoais em grande escala, e reconhecendo as mudanças drásticas dos últimos 23 anos, veio identificar a parte mais vulnerável (as pessoas individuais, titulares dos dados pessoais) concedendo-lhes mais e novos direitos. Com os novos direitos vieram maiores responsabilidades para quem trata os dados – sejam os responsáveis que determinam as finalidades do tratamento, sejam os subcontratantes.

3. Entre as novidades estão alguns conceitos novos na legislação europeia de proteção de dados, dirigidos às organizações, que devem implementar medidas técnicas e organizativas capazes de mostrar o cumprimento com o Regulamento, entre as quais destacamos aqueles já enunciados:

- *Privacy by Design*, ou proteção de dados desde a conceção, que começa antes do tratamento e incorpora esse cuidado numa fase de planeamento;
- *Privacy by Default*, ou proteção de dados por defeito, que sustenta esse mesmo cuidado na fase de tratamento, limitando-o.

Por defeito, um produto ou serviço deve apenas tratar os dados que sejam necessários. Ao aderir a uma nova ferramenta tecnológica, os utilizadores/ /clientes/ titulares dos dados devem optar, através das definições, pelas funções que pretendem usufruir, podendo excluir alguma função que apresente maiores riscos ou que simplesmente não pretendam, se não for necessária para o serviço em causa.

Passa assim a haver uma abordagem baseada no risco. Além da implementação da proteção de dados desde a conceção e por defeito (antes e na fase de tratamento), para avaliar o impacto do tratamento de dados nos direitos e liberdades dos titulares e quando se prevê que aquele representa um risco,

há agora outro instrumento que o Regulamento vem trazer e tornar obrigatório em diversos casos (como será o do tratamento de dados em grande escala): os PIA (*Privacy Impact Assessments* – Avaliações de Impacto sobre a proteção de dados).

As avaliações de impacto têm como principais razões de ser ajudar a incorporar as medidas de proteção de dados no planeamento da organização e demonstrar o cumprimento com o Regulamento e representam mais uma medida no novo paradigma de auto-regulação imposto às organizações.

Resulta como conclusão que a rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados. O regime da Diretiva vigente entre 1995 a 2016, centrado numa perspetiva reativa e *"de controlo"* por parte da autoridade local, dá lugar a um compromisso de conformidade preventiva, no qual ganham destaque os novos conceitos de *privacy by design* e *privacy by default*.

A recolha e a partilha de dados pessoais no mundo digital tornam imperativo que as organizações incorporem a proteção de dados proativamente numa fase inicial de planeamento, de modo a garantir, na fase de tratamento, condições para que o titular dos dados seja capaz de gerir e ter controlo sobre a informação que lhe diz respeito. Os novos conceitos (PbD, Pbd e PIA) concretizam assim a atitude pró-ativa e preventiva que corresponde à principal marca imposta pelo Regulamento.

4. O Regulamento aplicar-se-á não apenas a responsáveis pelo tratamento dos dados (*controllers*), como também aos subcontratantes (*processors*), preconizando uma partilha de responsabilidade que não acontecia no âmbito da Diretiva. O âmbito de aplicação é igualmente alargado, aplicando-se às operações de tratamento que incidam sobre titulares de dados pessoais europeus, independentemente de o responsável pelo tratamento (ou o subcontratante) se encontrar ou não localizado na União Europeia.

Este novo diploma introduz, ainda, o conceito de *"one stop shop"*, o que beneficia as organizações que tenham estabelecimentos em diferentes países da União Europeia e que, tendencialmente, passarão a reportar apenas à autoridade de controlo principal, que, regra geral, corresponde à localizada no país do estabelecimento principal do responsável pelo tratamento.

Finalmente, a previsão de um período transitório de 2 anos para a total aplicação do Regulamento vem de encontro à mudança de paradigma que este significa, tornando os dados pessoais uma nova camada de *compliance* e risco a ter em conta pelas organizações.

Mais do que cumprir com as novas regras do Regulamento Geral de Proteção de Dados, uma nova atitude poderá representar um posicionamento competitivo para as organizações alinhadas com as diretrizes de transparência e segurança nas quais estes conceitos inovam.