Valéria Reani: A GDPR e o compliance de medidas protetivas

15/06/2018

Em 27 de abril de 2016, foi adotado pela União Europeia a lei europeia sobre proteção de dados (conhecida como GDPR, na sigla em inglês para *General Data Protection Regulation*)[1], mais de quatro anos após ter sido apresentada pela Comissão Europeia[2] a proposta para a sua implementação. Esse regulamento entrou em vigor em maio de 2016 e passou a ser diretamente aplicável a todos os Estados-membros em 25 de maio deste ano (artigo 99º da GDPR).

A GDPR, 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 a 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.

Isto posto, a GDPR é um diploma europeu (EU 2016/679) que estabelece as regras referentes à proteção, tratamento e livre circulação de dados pessoais das pessoas singulares/físicas em todos os países-membros da União Europeia e que vem obrigar a implementação de regras dentro de empresas e entidades públicas, visando garantir a privacidade dos dados dos cidadãos da União Europeia.

Importante salientar que esse regulamento surgiu com o objetivo de reforçar a proteção de dados, prevista no artigo 8º da Carta dos Direitos Fundamentais da União Europeia, e harmonizar a legislação existente nos Estados-membros, criando as bases para o mercado único digital.

Seguramente, a medida deve ter impacto também nas empresas brasileiras, além dos 28 países-membros da União Europeia. Por conta disso, ela vem sendo chamada de “padrão ouro” na proteção de dados pessoais. Isso porque a medida tem aplicação extraterritorial, ou seja, alcança empresas brasileiras com filiais na União Europeia ou que ofertem serviços ao mercado europeu para coletar dados de cidadãos europeus.

Por conseguinte, essa 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 “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, o *compliance*, sendo consagradas medidas mais rigorosas a nível de

governança, responsabilidade e documentação para os responsáveis pelo tratamento ou subcontratantes.

A GDPR 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.

Ressalta-se como uma das suas a consagração do princípio da responsabilidade, bem como o estabelecimento de novas medidas corporativas e técnicas que recaem sobre os responsáveis pelo tratamento e subcontratantes. Por outro lado, é prevista a aplicação, por parte das autoridades de controle, de sanções mais exigentes em caso de descumprimento que impactam a nível organizacional.

Outrossim, as novas tecnologias, a globalização, o fenômeno 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.

Por conseguinte, este regulamento tem ainda como principais características a especial ênfase no *compliance*, através da consagração dos princípios da responsabilidade e de *data protection by design,* ou seja, as medidas protetivas da privacidade e dos dados pessoais deverão ser inseridas nos equipamentos desde sua concepção (também previsto no projeto de lei brasileiro) e *by default*, isto é, assegurar que são colocados em prática, dentro de uma organização, mecanismos padrão de garantia de privacidade, bem como novas medidas organizacionais e técnicas que recaem sobre os responsáveis pelo tratamento de dados pessoais 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 controle, ficando os primeiros obrigados a implementar mecanismos eficazes que assegurem tal cumprimento, sob pena da aplicação de pesadas sanções, que podem chegar a 20 milhões de euros, ou, tratando-se de uma empresa, até 4% do seu faturamento anual, a nível mundial.

Glossário da GDPR[4]
***Accountability*:** exige que seja implementado um programa de conformidade capaz de monitorar a conformidade em toda a organização e demonstrar às autoridades de proteção de dados e aos titulares dos dados que toda essa informação pessoal está em segurança.

Consentimento do titular dos dados pessoais: qualquer manifestação de vontade, livre, específica, informada e explícita, nos termos da qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os seus dados pessoais sejam objeto de tratamento.

Dados pessoais: qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (“titular dos dados”); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um identificador como o

nome, número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, mental, econômica, cultural ou social.

Destinatário: a pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo a quem sejam comunicados dados pessoais, independentemente de se tratar ou não de um terceiro.

Encarregado de proteção de dados (DPO – *Data Protection Officer*): Pessoa designada pela organização que estará envolvida em todas as questões relacionadas com a proteção de dados pessoais. Esta função deve ser atribuída sempre que o processamento for levado a cabo por uma entidade pública; se verifique a monitorização constante de indivíduos em larga escala; ou exista processamento de dados sensíveis em larga escala. As principais funções do encarregado de proteção de dados envolvem informar e aconselhar a empresa sobre a conformidade da proteção de dados; aconselhar sobre a avaliação do impacto da proteção de dados; monitorar a conformidade da proteção de dados, que inclui, por exemplo, formar a equipe e realizar auditorias relacionadas com essa área; e cooperar e atuar como ponto de contato com as autoridades de proteção de dados.

Limitação do tratamento: inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro.

Minimização dos dados (*Data Minimisation*): significa que os dados pessoais recolhidos devem ser limitados ao que é necessário relativamente às finalidades para as quais são tratados.

Oposição ao *profiling*: os titulares dos dados têm direito a opor-se ao uso de *profiling*, ou seja, qualquer forma automatizada de processamento de informação pessoal, com o objetivo de avaliar e tipificar indivíduos com base nos seus dados pessoais.

Privacidade desde a concepção (*Privacy by Design*): significa levar o risco de privacidade em conta em todo o processo de concepção de um novo produto ou serviço em vez de considerar as questões de privacidade apenas posteriormente. Tal significa avaliar cuidadosamente e implementar medidas e procedimentos técnicos e organizacionais adequados desde o início para garantir que o tratamento está em conformidade com a GDPR e protege os direitos dos titulares dos dados em causa.

Privacidade por defeito (*Privacy by Default*): significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por defeito, apenas será recolhida/coletada, utilizada e conservada para cada tarefa a quantidade necessária de dados pessoais. Esta obrigação aplica-se à extensão do seu tratamento, ao prazo de conservação e à sua acessibilidade de forma a assegurar que os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

***Privacy Impact Assessments*:** permite que a organização encontre problemas nas fases iniciais de qualquer projeto, reduzindo os custos associados e danos à reputação que poderiam acompanhar uma violação das leis e regulamentos de proteção de dados.

Pseudonimização: o recurso à pseudonimização (substituição de material pessoalmente identificável por identificadores artificiais) e à cifragem (codificação de mensagens para que apenas as pessoas autorizadas as possam ler). Tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

Responsável pelo tratamento dos dados pessoais: a pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais.

Subcontratante (*Data Processor*): a pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

Tratamento de dados pessoais: qualquer operação ou conjunto de operações efetuados sobre dados pessoais, com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, bem como a limitação, apagamento ou destruição.

Terceiro: pessoa singular ou coletiva, autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular de dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratante, esteja autorizado a tratar os dados.

Violação de dados pessoais: violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

Violação de segurança (incidentes de segurança): evento com um efeito adverso real na segurança das redes e dos sistemas de informação, tal como um acesso não autorizado ao sistema de informação.

Conclusão

Por conseguinte, e por se tornar fundamental adaptar a estrutura organizacional das empresas à GDPR, que proporciona, oportunamente uma cultura de *compliance*, de maneira a promover, internamente, a implementação e a aplicação dos princípios e das novas obrigações desta reforma europeia da proteção de dados, perante a UE, com impacto relevante internacional, sobretudo para os países da América Latina, favorecendo o desenvolvimento de uma economia cada vez mais aberta, transparente e responsável.

[1] Aprovado pelo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho em 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 (GDPR).

[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 (GDPR), de 25 de janeiro de 2012. Disponível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a633XIII.doc&Inline=true (acesso em 24/5/2018).
[3] Nesse 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.
[4] REANI, Valéria Rodrigues Garcia – Glossário RGPD – 2018 – Comentários com base no Material Intelectual do Curso Presencial Completo Capacitação RGPD – feita pela autora na Universidade Nova Lisboa – em Portugal – no Primeiro Semestre 2018.