Luz: Abordagem baseada no risco para a conformidade com a LGPD

A LGPD em vigor

Temos a LGPD plenamente em vigor há mais de um ano, obrigações e direitos estão estabelecidos, há uma autoridade nacional especializada para zelar pelo tema, que tem, cada vez mais, aparecido como ...ado pela imprensa de grande circulação.

De fato, a LGPD está "na boca do povo" e a conformidade é necessidade inadiável.

Mas como atingir o estado ideal de adequação? Como realizar a implementação na prática?

A lei não dita como isso deve ser feito e tampouco a Autoridade Nacional de Proteção de Dados (ANPD).

E seria esse papel da lei e uma das atribuições da ANPD?

A lei não estabelece — e nem poderia pretender exigir da ANPD — uma "receita de bolo" para a conformidade, com modelo metodológico único, e tampouco faz indicação de solução tecnológica em particular para a sua execução de forma automática, o que poderia inclusive tornar a lei defasada e ineficiente em curto prazo.

Certamente guias orientativos [1] podem ser emitidos no intuito de emitir diretrizes que visem a facilitar o entendimento do assunto e esclarecer dúvidas dos agentes, mas é ponto fixo que a lei é tecnologicamente neutra, ficando a cargo dos agentes de tratamento de dados a responsabilidade por conduzir sua própria trilha.

Com efeito, há na lei alguns pontos bem claros sobre o que deve ser realizado: atendimento aos direitos das pessoas titulares de dados pessoais, verificação de base legal justificante do tratamento, coleta do consentimento quando cabível etc.

Por outro lado, o cumprimento dos princípios legais, sobretudo a garantia da segurança dos dados pessoais, e o endereçamento de riscos nas diferentes operações de tratamento realizadas não revelam de pronto os passos necessários para estar *compliant*.

Há, por exemplo, a obrigatoriedade de os agentes de tratamento adotarem medidas de segurança técnicas e administrativas que sejam aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Medidas diversas podem ser adotadas a depender do setor e porte do negócio em questão. Não serão adotadas as mesmas medidas, por exemplo, à uma instituição de educação infantil e à uma empresa de atuação no modelo B2B, imobiliária ou para um hospital. Medidas técnicas de segurança de vultoso valor não são razoáveis para empresas de pequeno porte que não possuam operações de tratamento de alto risco.

Tal característica da regulamentação não é exclusiva da LGPD, mas está presente também no modelo regulatório europeu estabelecido pelo GDPR/RPGD, *standard* de alto nível reconhecido mundialmente e que serviu de base à formatação da lei brasileira, no que se costumou denominar de *risk-based approach* , isto é, a abordagem baseada no risco.

Segundo a ICO (*Information Commissioner's Office*), autoridade de proteção de dados do Reino Unido, em relação ao que deve ser feito pelas organizações para estar em conformidade, afirma que *"there is no one-size fits-all answer"* e explica que cada organização é diferente e a lei não estabelece muitas regras absolutas, mas utiliza a abordagem baseada no risco, que por sua vez está baseada em alguns princípios-chave [2].

Cumpre esclarecer que não se está a falar aqui da vindoura regulamentação pela ANPD voltada aos chamados "agentes de tratamento de pequeno porte", mas da aplicação prática das obrigações constantes na lei, da forma de realiza-las no plano concreto.

Independentemente do caráter que vier a ter a referida regulamentação, a abordagem baseada no risco será uma constante tanto nos projetos de implementação quanto nos programas de governança de privacidade já em execução.

A abordagem baseada no risco da LGPD

Nas palavras do *Centre for Information Policy Leadership* (CIPL) [3], ao comentar sobre a adequação ao GDPR, ainda em 2016, as obrigações do controlador são calibradas pelo risco, o que permite que as medidas técnicas e organizacionais a serem implementadas sejam moduladas com base nos riscos da operação de tratamento, podendo-se dar atenção às operações que representem maior risco aos direitos fundamentais dos indivíduos. Isso, contudo, não isenta a organização da obrigação geral de cumprir o GDPR [4].

Nas palavras de Claudia Quelle, a abordagem baseada no risco significa trazer o *compliance* da teoria à prática [5].

Disso podemos extrair outra importante característica da abordagem baseada no risco presente na LGPD: o *risco* motivo de preocupação para a lei não é aquele relacionado à eventualidade da aplicação de sanções, judicialização ou de ser alvo da ação de algum grupo criminoso, mas o risco da operação de tratamento de dados ao real dono deles, o *titular*, isto é, a pessoa natural a quem os dados pessoais dizem respeito, que pode ser desde um cliente/consumidor, até um visitante, prestador de serviços, paciente,

colaborador e dependentes.

Riscos de diversas naturezas são cotidianamente considerados pela organização — em especial os de segurança da informação, que podem contemplar dados pessoais, mas a estes não estão limitados — e influenciam na tomada de decisão, mas o risco a que LGPD ocupa-se é aquele voltado ao titular dos dados.

Em que pese não haja expressa previsão do conceito de *risco* na LGPD, e sua acepção possa variar a depender da abordagem da análise, identifica-se que o titular dos dados é o ponto de referência para esta noção.

As previsões da LGPD confirmam esta tendência ao estipular, por exemplo, que o relatório de impacto é a *"documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais"* (artigo 5º, XVII), também que o tratamento será irregular quando não fornecer a segurança que o titular dele pode esperar, considerando o resultado e os riscos que dele razoavelmente se esperam (artigo 44, II) e que os agentes de tratamento poderão formular regras de boas práticas e de governança levando em consideração a gravidade dos riscos (artigo 50, §1º).

Segundo o CIPL, uma das vantagens da adoção dessa abordagem é auxiliar a organização a estabelecer controles apropriados aos riscos, o que assegura a maximização de potenciais benefícios da atividade de tratamento ao mesmo tempo que reduz potencial impacto negativo aos direitos e liberdades dos indivíduos [6].

A preocupação e garantia do tratamento ético e seguro de dados pessoais reverbera positivamente na imagem e reputação da organização perante clientes, colaboradores e parceiros de negócio, que atualmente buscam contratar aqueles que puderem dar garantias de que o tratamento de dados pessoais é realizado de forma adequada.

O papel do Relatório de Impacto à Proteção de Dados Pessoais (RIPD)
Representativo do que se propõe a legislação, o RIPD revela-se ferramenta útil ao *compliance*, auxiliando na identificação e tratamento dos riscos ao mesmo tempo em que opera em favor da responsabilização e da prestação de contas.

Isso porque o RIPD, em que pese a denominação de "relatório" pela lei, configura verdadeiro processo, a ser desenvolvido em etapas, voltado à descrição de determinado projeto que envolva o tratamento de dados pessoais, colocando-o sob enfoque especial, permitindo a identificação preliminar de riscos e o estabelecimento das respectivas medidas para o seu endereçamento e mitigação.

Ao longo desse processo, serão feitos registros do que for identificado e da tomada de decisão em relação aos riscos, dando materialidade à postura da organização quanto às medidas e decisões que forem adotadas.

Para alcançar bons resultados, o RIPD deve contemplar a descrição sistemática e detalhada sobre as operações de tratamento pretendidas que constituem a iniciativa sob análise, em cada etapa do ciclo de vida do dado pessoal, da sua coleta até o seu armazenamento e eliminação, relatando aspectos tais como

a natureza, escopo, finalidade das operações e quaisquer outras informações reputadas úteis ao longo de seu desenvolvimento. Para que o entendimento do projeto seja o mais frutífero possível, será necessário realizar a consulta às partes envolvidas no projeto.

Nesse sentido, o RIPD também auxilia a promover internamente o aculturamento acerca da privacidade e alocá-la como pauta relevante dentro da organização, requerendo a participação efetiva dos envolvidos nos diversos departamentos ou mesmo terceiros que intervenham no processo sob análise.

Assim, mais do que o cumprimento de uma obrigação legal, o controlador poderá realizar esse processo sempre que entender oportuna a identificação de riscos aos titulares em determinada iniciativa ou projeto, podendo então endereça-los antecipadamente ao lado do próprio desenvolvimento da ideia, inserindo a proteção de dados desde a concepção.

Conclusão
A flexibilidade existente na LGPD é vital ao passo que abre margem para a customização de projetos de implementação e do próprio programa de governança de privacidade dentro da organização, sem, contudo, isentá-la do cumprimento de suas obrigações legais.

A abordagem baseada no risco para a adequação à LGPD implica na calibragem para o atendimento às obrigações legais impostas aos agentes de tratamento, afetando como se traz a norma abstrata para a prática.

Os agentes de tratamento, portanto, são responsáveis por cumprir a LGPD com medidas de acordo com o risco das operações que realizam ou pretendam realizar. Nesse sentido, a organização é responsável pelas medidas que escolher adotar para cumprimento das normas de proteção de dados e deverá ser capaz de demonstrar a sua eficácia.

Essa abordagem tecnologicamente neutra garante a longevidade da legislação de modo a não engessar o desenvolvimento da atividade econômica em cada setor e organização, incentivando novas ideias, mas também não retirando a responsabilidade pelo cumprimento da lei e a proteção dos direitos e liberdades fundamentais dos indivíduos.

Uma das demonstrações dessa abordagem está no RIPD, ferramenta que permite ao agente de tratamento compreender em sua própria operação os riscos existentes ao titular em cada etapa, permitindo uma postura proativa e antecipada para a sua mitigação visando a garantir a conformidade com a legislação e o tratamento ético e seguro dos dados pessoais.

[1] Sobre o ponto, vale mencionar que a ANPD já publicou guia orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte, acompanhado de um checklist de medidas, e também um outro relativo à aplicação da LGPD no contexto eleitoral, ambos disponíveis no site da Autoridade.

[2] Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-dpa-2018/some-basic-concepts/#3

. Acesso em 10 dez. 2021.

[3] O CIPL é um think tank global de política de privacidade e de dados que trabalha para promover a política de privacidade e segurança, lei e prática.

[4] Centre for Information Policy Leadership, 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR' 21 December 2016, www.informationpolicycentre.com/eu-gdpr-implementation.html, p. 20.

[5] QUELLE, Claudia. "The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too" in R Leenes, R van Brakel, S Gutwirth and P De Hert (eds), Data Protection and Privacy: The Age of Intelligent Machines (Hart Publishing, forthcoming), p. 4.

[6] Centre for Information Policy Leadership, 'Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR' 21 December 2016, www.informationpolicycentre.com/eu-gdpr-implementation.html, p. 13.

Date Created
05/01/2022