Por quê o Relatório de Impacto da LGPD ainda é frágil?

Instrumento da lei para controle dos efeitos sobre direitos e liberdades é aquém do necessário num cenário de alta complexidade

Esther Külkamp Eyng Prete, advogada brasileira radicada no Porto (Portugal), Mestre e Doutoranda em Direito (UFMG), pesquisadora associada ao "LegisLab" - Laboratório de Legislação e Políticas Públicas. esther.eke@gmail.com.br

Rodrigo Élcio Marcelos Mascarenhas, advogado, analista legislativo na Assembleia Legislativa de Minas Gerais, mestre em Administração Pública (Fundação João Pinheiro), Doutorado em Direito (UFMG), pesquisador do Observatório para a Qualidade da Lei (UFMG), rodmarcelos@gmail.com.

O aprofundamento e a expansão do processo da digitalização da vida social, ocorrida especialmente na última década, colocam o Direito diante de novos e grandes desafios. A "digitalização profunda" (*deep digitalization*), impulsionada por avanços tecnológicos como *big data*, aprendizado de máquina (*machine learning*), algoritmos inteligentes, inteligência artificial e soluções avançadas de interação em rede, desafia o jurista contemporâneo a conseguir discernir como promover a proteção do núcleo essencial dos direitos fundamentais diante dos potenciais usos e efeitos daquelas tecnologias. Isso é especialmente desafiador perante infraestruturas digitais "semi-autônomas" dotadas de uma funcionalidade cada vez menos acessível e transparente ao grande público (e até às autoridades governamentais).

Trata-se de um cenário de alta complexidade, cujos efeitos são transversais a quase todas as dimensões da vida humana, desde a distribuição do poder político, econômico, chegando até aos níveis psicológico e antropológico. Por isso, a digitalização da vida social pede de forma ainda mais contundente a aplicação de metodologias da Ciência da Legislação (Legística) para a regulamentação dessas novas searas, especialmente a aplicação de mecanismos de *avaliação de impacto,* tanto previamente à feitura da lei quanto posteriormente à sua aplicação concreta. É nesse sentido que se compreende a inserção de mecanismos como o "relatório de impacto" (XVII do Art. 5º c/c o parágrafo único do art. 38) e "análise de impacto regulatório" (§ 2º do Art. 55-J) na Lei de Proteção de Dados Pessoais (LGPD, Lei 13709 de 14 de agosto de 2018, alterada pela lei 13853 de 2019), a qual parece indicar uma crescente e bem-vinda adesão ao uso de ferramentas de avaliação de impacto, observada desde as leis Lei 13.848 e 13.874, ambas de 2019.

Todavia, tal como desenhado o mecanismo do "relatório de impacto" na LGPD - e sem ainda se poder levar em conta a futura regulamentação da recém-criada Autoridade Nacional de Proteção de Dados - ele estabelece deveres *aquém* do necessário para prevenir ofensas aos direitos fundamentais das pessoas naturais, tendo em conta o contexto

atual de grande complexidade e periculosidade, alta concentração de poder tecnológico e informacional[1] e a evolução regulatória internacional.

O "Relatório de Impacto" da LGPD e a "Avaliação de Impacto" do Regulamento 2016/6791 da União Europeia.

Uma forma de melhor iluminar algumas fragilidades do Relatório de Impacto é compará-lo ao instrumento de "Avaliação de Impacto de Proteção de Dados" (*Data Protection Impact Assessment*, DPIA) do Regulamento Geral de Proteção de Dados[2], por ser tratar do arcabouço normativo mais desenvolvido até o presente no que tange proteção de direitos. Seu tratamento é dado pelo art. 35 c/c o art. 36 (dever de consulta prévia), devendo-se ainda observar os considerandos 84, 90 ao 94, e as orientações da Diretriz[3] sobre Avaliação de Impacto do Grupo de Trabalho Artigo 29 (*Working Party 29*).

Ao compararmos a descrição dos dois institutos das respectivas legislações, depreendem-se diferenças importantes na *natureza*, *alcance*, *finalidades* e *procedimento:*

Art. 35 RGPD (UE)	XVII do art. 5º do LGPD
"Quando um certo tipo de tratamento, ***em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades***, *for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*, o responsável pelo tratamento procede, ***antes de iniciar o tratamento***, a uma ***avaliação*** de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação."	"relatório de impacto à proteção de dados pessoais: ***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, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Da forma como redigida, **a descrição do mecanismo da LGPD destaca como finalidade principal do Relatório de Impacto *a atividade de simples registro* ("documentação") das atividades potencialmente danosas e das eventuais medidas mitigadoras do risco tomadas.** Sendo assim, o instrumento da LGPD tende a ser executado *após* os tratamentos de dados potencialmente lesivos aos direitos, de forma que não há também a possibilidade de a Autoridade Nacional fazer um controle *prévio* desses tratamentos. A palavra "relatório", escolhida para designar o instituto, reforça essa conclusão: derivada da palavra "relato", caracteriza-se pelo objetivo principal de narrativa

[1] Sobre o isso, ver *"A Era do Capitalismo de Vigilância: a Disputa por um Futuro Humano na Nova Fronteira do Poder"* (2020), da socióloga norte-americana Shoshana Zuboff.
[2] Em vigor desde 25 de maio de 2018, revogando a Diretiva 95/46/CE
[3] *Guidelines on Data Protection Impact Assessment* (DPIA) (wp248rev.01)

objetiva e *descritiva* de fatos, eventos, motivos. Mesmo quando culmine numa opinião (como num parecer), um relatório volta-se sempre para o passado.

Por sua vez, o DPIA deverá ser sempre realizado *antes* do processamento se este apresentar alto risco latente aos direitos e liberdades das pessoas naturais, tendo em vista o contexto, âmbito, finalidade e alcance. Seu objetivo é uma *avaliação,* ou seja, *um julgamento:* o apurar e avaliar os riscos aos direitos e liberdade, sopesá-los com a proporcionalidade, necessidade e legitimidade das operações; verificar as possíveis medidas de mitigação de riscos, existentes ou a serem criadas pelo controlador, incluídas garantias aos titulares e medidas de segurança. Se mesmo diante da adoção de medidas de mitigação de risco este ainda subsista, deverá a autoridade competente (no caso, a *European Data Protection Board*) ser consultada para autorizar ou não o processamento (art. 36). Em resumo, a DPIA é tanto um mecanismo de *gestão do risco* aos direitos fundamentais quanto um meio de demonstração de conformidade regulatória. Foi concebido como *processo* para auxiliar na *tomada de decisões* relativas ao processamento potencialmente lesivo, com ou sem a participação da autoridade pública competente, ficando o registro das atividades num plano relativamente secundário àquele.

No caso da lei brasileira, para além do dever genérico dos controladores em adotar medidas de segurança aptas à proteção e à segurança dos dados pessoais (art. 46), o único momento em que se menciona expressamente "avaliação de impacto" para mitigação de riscos é na alínea "d", art. 50, mas elencado apenas como uma das boas práticas de governança, ou seja, não obrigatória. Outra lacuna da lei que induz os controladores a uma posição passiva frente aos riscos latentes é a ausência de uma obrigação de comunicar a ANPD dos mesmos quando constatados, cabendo prioritariamente à ANPD a iniciativa de exigir relatórios de impacto dos controladores. A Lei cita situações específicas nas quais a Autoridade Nacional possui ora o dever, ora a prerrogativa de exigir a sua feitura por parte do controlador, entre elas: a) quando o tratamento de dados é excetuado da aplicabilidade da LGPD (§ 3º do art. 4º.), referente a certas atividades executadas pelo Poder Público, dispostas no inciso III do art. 4º; b) mesmo diante do "interesse legítimo" do controlador que justifica o tratamento de dados (§ 3º do art.10); c) possibilidade de solicitação de publicação de relatórios de impacto a agentes públicos no caso de violação da lei (art. 31 c/c 32); d) por fim, conforme art. 38, nos termos de futura regulamentação. Ao controlador, exige-se informar a ANPD quando *já ocorrido* um evento danoso ("incidente de segurança"), especificamente ligado à segurança dos dados (art. 48).

A análise sistemática dos dois regulamentos (LGPD e RGPD europeu) parece indicar uma diferença de escopo entre esses que pode explicar a maior ênfase na avaliação prévia de riscos da normativa europeia. Os mecanismos da LGPD, tomados em conjunto, voltam-se primordialmente à proteção da idoneidade, privacidade e sigilo dos dados

pessoais, priorizando a ausência de incidentes com esses direitos. O RGPD também parte desse objetivo, mas esse é englobado pelo âmbito mais amplo da proteção dos direitos e liberdades frente *à inovação tecnológica*, visando evitar que, por exemplo, o poder de processamento de dados pessoais em larga escala (considerando 91) possa enfraquecer o núcleo de direitos como "liberdade de expressão, liberdade de pensamento, liberdade de movimento, proibição de discriminação, direito à liberdade, consciência e religião"[4].

E é justamente nesse ponto que nossa lei parece estar aquém da complexidade do cenário atual apesar dela ter sido fortemente inspirada no arcabouço normativo europeu[5]: faltam mecanismos com critérios precisos que, à semelhança da exaustiva regulamentação comunitária europeia, leve em conta também os riscos *latentes* das novas tecnologias ao exercício efetivo das liberdades e direitos, para além de medidas que garantam prioritariamente o sigilo e privacidade - alinhando assim globalmente a normativa nacional aos fundamentos elencados pelo artigo 2 da própria LGPD. Além disso, que essa tarefa de verificação dos riscos latentes de novas tecnologias seja *compartilhado* com os controladores – tal como se depreende das funções do DPIA - não devendo recair o encargo de tal monitoramento antecipatório exclusivamente sobre o Estado, no caso, sobre a Coordenação-Geral de Tecnologia e Pesquisa da ANPD (art. 18 do seu Regimento Interno).

No curto prazo, a tarefa de sanar as lacunas em torno do instrumento do relatório de impacto caberá, muito provavelmente, à própria ANPD (pois ao seu Conselho Diretor cabe ainda regulamentar com maiores detalhes o Relatório de Impacto) a partir dos elementos que a própria LGPD já fornece para aperfeiçoar em sede infralegal os instrumentos de mitigação de risco; o que poderá ser realizado já tendo em conta as experiências práticas tanto nacionais quanto internacionais, e ajustando-as às realidades e necessidades nacionais.

---

[4] *Guidelines on Data Protection Impact Assessment* (DPIA) (wp248rev.01), pg. 6.

[5] Ver o processo da Comissão Especial destinada a proferir parecer ao projeto de Lei no. 4060, disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=PRL+1+PL406012+%3D%3E+PL+4060/2012