A nova Lei Geral de Proteção de Dados Pessoais

Principais repercussões para a atividade empresarial: perspectivas a respeito da eficácia do direito à explicação e à oposição diante de decisões totalmente automatizadas

Parte XVII

Ana Frazão

Advogada. Professora de Direito Civil e Comercial da UnB. Ex-Conselheira do CADE.

Como se pode perceber pelos artigos anteriores, existem consideráveis controvérsias em torno do direito à explicação e à oposição diante de decisões automatizadas, o que pode comprometer a compreensão do seu real alcance e, consequentemente, a sua efetividade.

Não obstante, a interpretação sistemática dos referidos direitos diante de outras soluções previstas pela LGPD, a exemplo do disposto igualmente no GDPR, pode oferecer cenário mais promissor a respeito da sua eficácia.

É o que sustentam, em recente e instigante artigo, Bryan Casey, Ashkon Farhangi e Roland Vogl[1], segundo os quais, embora os direitos ora discutidos não obriguem a total transparência, no sentido de uma completa e individualizada explicação das decisões automatizadas, os seus efeitos sinergéticos se projetariam quando combinados com a auditoria dos algoritmos e a metodologias de "data protection by design". Daí a conclusão dos autores de que a mais revolucionária modificação do GDPR foi a relacionada aos poderes conferidos as autoridades e às previsíveis repercussões deles decorrentes.

---

[1] Rethinking explainable machines: the GDPR's "right to explanation" debate and the rise of algorithmic audits in enterprise". https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143325

Por essa razão, é preocupante que, no contexto brasileiro, até hoje não tenha sido resolvido o problema da autoridade nacional, uma vez que, diante do veto presidencial à sua instituição, nada foi feito para suprir essa grave lacuna da LGPD.

Outro ponto crucial, destacado pelas *Guidelines on Automated Individual Decision Making and Profiling*[2], já mencionadas no artigo anterior, diz respeito à importância das medidas e procedimentos para prevenir erros, inacurácias e discriminações que podem resultar de decisões totalmente automatizadas, o que impõe a todos que delas se utilizam a realização de constantes avaliações sobre os seus resultados.

Tais conclusões casam-se perfeitamente com aquelas previstas no relatório do governo Barack Obama *Preparing for the future of artificial intelligence*[3], no qual fica claro que, diante das dificuldades de se realizar uma regressão perfeita das decisões totalmente automatizadas, há necessidade ao menos de se proceder a testes exaustivos sobre os seus resultados.

Outra medida de segurança repetidamente invocada pelas *Guidelines* é o relatório de impacto à proteção de dados, previsto no art. 35 do GDPR, por meio do qual se pode construir e demonstrar o *compliance* com a proteção de dados por meio do exame sistemático de técnicas de processamento automatizado e as medidas necessárias para gerenciar os riscos e as liberdades das pessoas naturais envolvidas.

De fato, de acordo com o GDPR, tais avaliações precisam conter minimamente a descrição sistemática das operações de processamento e seus propósitos, incluindo o legítimo interesse do controlador, a avaliação da necessidade e da proporcionalidade do processamento em relação aos seus objetivos, a avaliação dos riscos aos direitos dos titulares de dados e as medidas visando a endereçar tais riscos, incluindo as salvaguardas, medidas de segurança e mecanismos para garantir a proteção dos dados pessoais.

No Brasil, a LGPD define, em seu art. 5º, XVII, o relatório de impacto à proteção de dados pessoais como a "documentação do controlador que

---

[2] file:///D:/Users/User/Downloads/wp251rev01_enpdf.pdf
[3]https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

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."

Entretanto, não fica claro qual é o grau de comprometimento dos controladores com a referida obrigação, uma vez que o art. 38, da LGPD - "A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial" - poderia sugerir que o relatório dependeria da iniciativa da autoridade nacional, hipótese que se confirmaria com a previsão do art. 4º, § 3º, segundo o qual "A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais."

Verdade seja dita que, ao tratar da questão da governança e do *compliance*, a própria LGPD, em seu art. 50, § 2º, I, "d", determina a existência de "políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade". Entretanto, não são claras as consequências do desrespeito a tais determinações.

De toda sorte, diante das controvérsias sobre as decisões automatizadas, é inequívoco que a autoridade tem o papel central de determinar o que pode ser considerado uma política adequada de proteção de dados e o que pode ser considerado uma avaliação idônea dos impactos e riscos para os usuários. Assim, qualquer que seja a interpretação, a ausência da autoridade nacional causa diversos problemas.

Com efeito, Bryan Casey, Ashkon Farhangi e Roland Vogl[4] mostram que o que se chama de *data protection by design* precisa levar em consideração diversos fatores complexos, tais como o estado da arte da tecnologia, os custos de implementação, a natureza, o escopo, o contexto e o propósito do tratamento de dados, assim como os riscos da probabilidade de violações aos direitos dos titulares e a gravidade dessas violações.

---

[4] Op.cit.

Por mais que isso envolva uma atitude proativa dos controladores e possam existir hipóteses nas quais os altos riscos tornariam os relatórios de impactos obrigatórios – e não meramente recomendáveis -, é inequívoco que a autoridade responsável tem importante papel para aclarar essas dúvidas.

Não obstante, as *Guidelines on Automated Individual Decision Making and Profiling* delimitam alguns exemplos de atividades consideradas de alto risco, dentre as quais (i) avaliações ou scorings, (ii) decisões automatizadas com efeitos jurídicos ou similares, (iii) monitoramento sistemático, (iv) dados sensíveis, (v) dados processados em larga escala, (vi) datasets que forem combinados ou misturados, (vii) uso inovativo ou aplicação tecnologica ou souções organizacionais, (viii) transferência de dados entre fronteiras fora da União Eueopeia e (ix) processamentos que impedem titulares de dados de exercerem direitos ou usarem determinado serviço ou poderem contratar.

Por essa razão, faz sentido o argumento de Bryan Casey, Ashkon Farhangi e Roland Vogl[5] de que, até para demonstrar que determinada atividade nao gera risco suficiente para justificar o relatório de impacto, será necessária a existência deste. Vale ainda ressaltar que, do ponto de vista das *Guidelines on Automated Individual Decision Making and Profiling*, as avaliações são necessárias não somente nos casos de decisões totalmente automatizadas.

Todas essas questões são aqui trazidas para se mostrar que os direitos ora em discussão, interpretados sistematicamente com as demais previsões do GDPR e da LGPD, não são apenas reativos, mas geram grande dever de cuidado aos agentes de processamento.

Afinal, ao direito do titular de entender a lógica do processo decisório e o significado e as consequências pretendidas, contrapõe-se o dever dos controladores de se utilizarem de procedimentos matemáticos e estatísticos apropriados, que sejam capazes de corrigir inacurácias e minimizar os riscos de erro, submetendo-os aos devidos controles, por meio dos relatórios de impacto e dos procedimentos de testagem e avaliação.

Sob essa perspectiva, o GDPR e a LGPD acabam impondo aos controladores o ônus da prova da legitimidade do tratamento totalmente

[5] Op.cit.

automatizado, uma vez que caberá a eles demonstrar, dentre outras questões (i) os dados que são coletados, de que fonte e de que maneira, (ii) quais as linhas gerais de programação dos algoritmos e seus objetivos, (iii) como se deu a programação e o desenvolvimento do algoritmo, (iv) se o algoritmo pode ou não modificar seu próprio código, (v) se tais modificações são previsíveis ou ao menos verificáveis, (vi) quais as categorias relevantes dos perfis e os critérios para cada uma delas, (vii) quais são os outputs do processo decisório e como avaliar a sua adequação e acurácia, (viii) se há mecanismos de feedback, (viii) se há intervenção humana e em que nível, (ix) quais são os principais impactos e riscos para os titulares de danos, (x) que medidas foram tomadas para conter tais riscos.

Dessa maneira por mais que os direitos à explicação e à oposição não exijam que as companhias abram suas *black boxes* algorítmicas, certamente exigem que os controladores avaliem cuidadosamente os interesses dos titulares de dados, escolham com cuidado seus sistemas de processamento de dados e possam compreendê-los, assim como estabelecem políticas para documentar e justificar os aspectos centrais do *design* do sistema e todas as salvaguardas adotadas.

Não há dúvidas de que, apesar de todos os desafios apontados, tem-se que tanto o GDPR como a LGPD pavimentaram o caminho em busca da *accountability* algorítmica, o que se projeta inclusive na adoção, pelos controladores, de tecnologias compatíveis e dos investimentos necessários para tal fim.