A recente multa que a autoridade de proteção de dados francesa aplicou ao Google

Reflexões sobre os parâmetros da avaliação da legalidade das políticas de privacidade

Ana Frazão

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

Em 21 de janeiro deste ano a Comissão Nacional de Proteção de Dados da França multou o Google em 50 milhões de euros por violação às regras de privacidade da União Europeia. Ao que se sabe, é a maior penalidade imposta contra uma companhia de tecnologia norte-americana.

Ao examinar a decisão[1], observa-se que a autoridade francesa considerou que o Google falhou no seu dever de informar, especialmente no que diz respeito aos requisitos de acessibilidade, clareza e compreensão. Ponto importante da decisão foi o de que a própria arquitetura geral de informação escolhida pela plataforma impede que os objetivos legais sejam alcançados, uma vez que as informações estão excessivamente dispersas em vários documentos e algumas delas ainda são difíceis de serem encontradas.

O problema torna-se mais grave, segundo a autoridade francesa, diante do fato de que pelo menos 20 serviços oferecidos pelo Google são suscetíveis de serem implicados para efeitos do tratamento de dados. Diante da multiplicidade de fontes, a conclusão a que se chegou é que, do resultado da observação do conjunto de elementos, falta acessibilidade do ponto de vista global.

[1] https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1. Acesso em 20.02.2019.

A autoridade francesa também ressaltou a variedade e diversidade de dados que são objeto de tratamento, o que inclui desde históricos de utilização de aplicativos e de navegação até dados estocados no equipamento, dados de geolocalização e vários outros. A partir daí, sistematizou os três tipos de dados que estariam envolvidos em tratamentos diversos pelo Google: (i) os produzidos pelo próprio usuário, (ii) os gerados pela atividade do usuário e (iii) os derivados ou inferidos a partir dos dois primeiros.

Se a utilização de cada um desses dados já seria preocupante, o resultado da combinação de todos eles reforçaria, segundo a autoridade francesa, o caráter massivo e invasivo do tratamento de dados, especialmente porque as informações geradas não permitem que os usuários compreendam suficientemente as consequências particulares dos tratamentos.

A autoridade francesa ainda se referiu ao fato de que o Google procura justificar o tratamento de dados a partir de finalidades excessivamente genéricas, tais como propor serviços personalizados ou garantir a segurança de produtos e serviços, o que igualmente não permite ao usuário mensurar a amplitude dos tratamento e o grau de instrusão em sua vida privada.

Como se pode observar, a decisão da autoridade francesa, embora ainda não seja final, pode ser utilizada como importante referencial para analisarmos vários dos problemas relacionados às políticas de privacidade que atualmente imperam no mundo digital. A decisão chama a atenção para o fato de que os tratamentos de dados precisam respeitar o princípio da finalidade - que precisa ser legítima, clara, expressa e específica - e o princípio do acesso à informação - que impõe que a informação seja clara, fácil e acessível.

Tais princípios não podem ser afastados pelo simples fato de que o usuário consentiu com determinada política de privacidade. Por mais que o GDPR, assim como a LGPD brasileira, tenha atribuído grande valor ao consentimento, é inequívoco que ele precisa ser entendido dentro do contexto maior da proteção de dados.

Com efeito, ainda que se entendesse que os dados pessoais são meros bens patrimoniais, suscetíveis de amplas negociações pelos seus titulares, haver-se-ia que concordar que tal negociação, considerando os problemas de racionalidade limitada dos usuários e a sua vulnerabilidade e assimetria do ponto de vista técnico, apenas seria válida se baseada na ampla informação sobre os dados coletados e as

finalidades específicas do tratamento desses dados. Tais requisitos seriam ainda mais necessários diante de serviços importantes para o usuário, em que não lhe resta outra opção, para ter acesso ao serviço, que não concordar com as cláusulas unilateralmente impostas pelo prestador - as chamadas cláusulas *take it or leave it*.

Acresce que o cenário atual em que essas transações ocorrem é muito próximo ao *one way mirror* descrito por Pasquale[2] no artigo da semana passada, em que os agentes do meio digital sabem tudo dos usuários enquanto estes não sabem nada dos primeiros, o que reforça ainda mais a assimetria informacional.

Aliás, foi por esse motivo que a autoridade francesa rejeitou a defesa do Google baseada no consentimento, assim como muitos autores defendem hoje que termos de serviço na internet são menos políticas de privacidade e mais contratos por meio dos quais os usuários abrem mão de todos os seus direitos em prol do prestador do serviço[3].

Por outro lado, há que se lembrar que os valores e objetivos reconhecidos pelo GDPR europeu e também pela LGPD brasileira representam um importante contraponto à tendência atual de monetização dos dados e da consideração destes como meras *commodities* que podem ser objeto de livre negociação. De forma contrária, os referidos atos normativos ressaltam a importante dimensão existencial dos dados pessoais e a sua vinculação aos valores mais importantes da pessoa humana, tais como liberdade, igualdade, dignidade e cidadania.

Daí por que Danilo Doneda[4] aponta com muita propriedade que a adoção da solução de mercado para o problema dos dados não é adequada, motivo pelo qual a disciplina do consentimento não deve ser tratada sob viés meramente negocial, mas sim a partir do poder de autodeterminação e a consideração dos direitos fundamentais em questão.

Tal perspectiva não implica a negação da importância do consentimento ou da existência de desdobramentos patrimoniais dos dados que podem ser objeto de livre negociação. O que o arcabouço valorativo do GDPR e da LPGD impede é a redução dos dados ao aspecto patrimonial e negocial, o que reforça a existência de limitações ao consentimento, assim como da necessidade de atendimento a requisitos

---

[2] PASQUALE, Frank. *The black box society. The secret algorithms that control money and information*. Cambridge: Harvard University Press, 2015.
[3] Ver, por todos, Pasquale (Op.cit., pp. 143-144).
[4] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio: Renovar, 2006, p. 410.

indispensáveis para a sua validade, dentre os quais a observância aos princípios fundamentais do tratamento de dados, como a finalidade e o acesso à informação.

Assim, observa-se claramente que a decisão da autoridade francesa transcende o caso Google e a França, sendo uma excelente oportunidade para refletirmos com maior alcance sobre as políticas de privacidade atualmente existentes e como podem e devem ser adaptadas para se tornarem compatíveis com com o GDPR e a LGPD.