Daniele Marcon: Dano moral e vazamento de dados

Em 7 de março de 2023, a 2ª Turma do Superior Tribunal de Justiça entendeu que o vazamento de dados pessoais não gera dano moral presumido (*in re ipsa*), *"sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações"* [1]. A decisão foi proferida nos autos do Agravo em Recurso Especial nº 2.130.619/SP e reformou acórdão do Tribunal de Justiça de São Paulo que havia condenado a Eletropaulo Metropolitana Eletricidade de São Paulo S.A. ao pagamento de indenização por dano moral diante do vazamento de dados pessoais da autora (que incluíam, dentre outros, data de nascimento, números de CPF e RG, endereço e

A conclusão do STJ foi delineada a partir de duas premissas.

A primeira, que se revela uma tese, é a de que o artigo 5º, II, da LGPD traria *"um rol taxativo daquilo que seriam dados pessoais sensíveis"*. Consequentemente, dados que não estão expressamente listados em tal inciso, como dados de geolocalização, não poderiam ser considerados dados sensíveis. Contudo, essa conclusão, que não foi fundamentada no voto do ministro relator, está longe de ser óbvia. A professora Caitlin Mulholland referiu, por exemplo, que o rol seria exemplificativo pois *"não somente o conteúdo dos dados previsto neste inciso merecerão a qualificação como dados sensíveis, podendo abarcar outras situações não previstas"* [2].

A segunda premissa adotada pelo STJ é de que dados pessoais "comuns", fornecidos em qualquer tipo de cadastro, não são *"acobertados por sigilo, e o conhecimento por terceiro em nada violaria o direito de personalidade"*. Daí a necessidade de provar um dano pela sua exposição. Porém, o acórdão refere logo em seguida que *"diferente seria se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural"*. O trecho é ambíguo e dá a entender que haveria espaço para reconhecer um dano moral *in re ipsa* se o vazamento envolvesse dados que a LGPD considera sensíveis (pelo artigo 5º, II).

Ocorre que a natureza dos dados não deveria ser um critério para reconhecer se há um dano moral (presumido ou não) em uma situação de vazamento de dados. A reflexão aqui proposta busca questionar as premissas adotadas pelo acórdão, elencando alguns motivos que podem justificar a conclusão do STJ está amparada, na verdade, em uma falácia.

Primeiro, porque a LGPD tem entre seus fundamentos a privacidade, a intimidade e a autodeterminação informativa, direitos fundamentais que abarcam todo tipo de dado pessoal, sensível ou não. A distinção entre as categorias indica apenas que alguns dados, como a orientação sexual, estado de saúde e convicções religiosas e políticas [3], podem gerar algum tipo de discriminação e representam, por isso, uma vulnerabilidade [4]. Categoriza-se para restringir as hipóteses que autorizam o tratamento de dados sensíveis — e afastar, por exemplo, a possibilidade de justificativa no legítimo interesse do controlador — a fim de limitar o uso de tais dados.

Porém, quando trata do dano, a LGPD não diferencia situações envolvendo dados sensíveis e "comuns". Se um incidente de segurança puder causar risco ou dano relevante, o artigo 48, §1º, I, da LGPD indica que a comunicação a ser encaminhada à autoridade nacional deve descrever a "natureza dos dados pessoais afetados". O envolvimento de dados sensíveis no incidente não é um requisito para reconhecer o risco ou dano relevante, apenas um elemento da análise.

Segundo, porque a fronteira entre um dado pessoal "comum" e um "sensível" não é evidente e não se limita às hipóteses elencadas pelo artigo 5º, II, da LGPD, que o acórdão entendeu como taxativas. Em artigo recente, Daniel Solove, professor na *George Washington University Law School*, critica leis de proteção de dados que estabelecem dois níveis de proteção, um para dados "comuns" e outro para dados "sensíveis", pois essa separação não faz sentido no contexto de *Big Data Analytics*, em que grandes quantidades de dados podem ser analisadas rapidamente para extrair outras informações. Algoritmos são capazes de fazer inferências e descobrir a orientação sexual e o posicionamento político de alguém a partir de suas interações nas redes sociais, uma gravidez por hábitos de compra e a religião pela alimentação ou vestuário [5].

O fato de que inferências baseadas em fatos triviais [6] podem revelar tanto sobre alguém torna a delimitação do que se entende por dado sensível complicada — até mesmo arbitrária. Mas não só isso: se dados sensíveis podem ser extraídos das mais simples informações cotidianas, então praticamente todas as interações que fazemos colocam em risco o seu sigilo e, consequentemente, dificultam a sua efetiva proteção.

Terceiro, porque dados que a LGPD considera "comuns" podem ser sensíveis para algumas pessoas. A sensibilidade de uma informação depende do contexto em que o titular a quem ela se relaciona está inserido. Para vítimas de perseguição e violência doméstica, juízes e médicos que realizam abortos, por exemplo, o endereço onde residem ou a escola onde seus filhos estudam podem ser informações sensíveis. Por outro lado, a orientação sexual e a religião de políticos são dados sensíveis que podem se tornar públicos para fins de identificação das pautas que tais políticos defendem, mas o acesso a sua geolocalização, um dado "comum" para a LGPD, pode causar um assassinato [7].

Quarto, porque, como já referido, alguns dados sensíveis são compartilhados com o público pelo próprio titular ou com a sua concordância. Nesses casos, não é o rompimento do sigilo que fere direitos fundamentais do titular, mas o uso dos dados sensíveis em contrariedade à finalidade, a boa-fé ou ao interesse público que justificaram a disponibilização (artigo 7º, §3º). Apesar de tratar de hipótese distinta da que ocorre em um vazamento, que representa uma publicização não autorizada, o artigo 7º, §§3º, 4º e

7º, indica que o que importa, para fins de proteção de dados, é o uso inadequado da informação, não propriamente o seu sigilo.

Feitas tais ponderações, a conclusão do STJ no sentido de que não se pode presumir que há um dano pelo simples fato de alguém ter sido notificado a respeito de um incidente de segurança da informação parece correta. São fatores individuais, relacionados à pessoa do titular e ao contexto em que está inserido, que determinam a gravidade de um vazamento de dados e permitem identificar que tipo de informação é
ou não sensível para a proteção da intimidade e da integridade moral (e física) daquela pessoa.

A individualização é necessária não apenas para assegurar que as
particularidades de cada pessoa sejam levadas em conta — inclusive para a determinação de outras medidas de proteção eventualmente necessárias —, mas também para que se possa arbitrar uma indenização compatível com a dimensão do dano moral configurado. Ademais, o raciocínio não afasta a possibilidade de se reconhecer, em sendo o caso, que de fato há uma situação de dano moral presumido, como ocorre com a inscrição indevida em cadastro de inadimplentes associada à fraude de identidade.

Mas essas mesmas ponderações permitem confrontar as premissas adotadas pelo STJ para sustentar a conclusão. Se dados sensíveis podem ser inferidos a partir de informações comuns e se uma informação comum pode ser sensível a depender do contexto de uma pessoa, então a primeira premissa adotada pelo acórdão é falsa, pois o rol do artigo 5º, II, da LGPD não pode ser considerado taxativo. Da mesma forma, se o
vazamento de um dado "comum" pode representar mais risco a alguém do que a publicidade de um dado sensível em razão do uso que dele pode ser feito, então também a segunda premissa do acórdão é falsa, pois não é a natureza do dado vazado que permitirá presumir ou não a existência de um dano moral.

Portanto, é o uso que determina a relevância de uma informação. Esse uso pode ser positivo ou negativo, caso em que pode originar um dano [8]. Assim, o critério para se aferir a ocorrência de um dano moral não deve considerar simplesmente a categoria do dado para a LGPD, mas, sim, o uso e os riscos que o vazamento representa a um titular específico — daí a necessidade de demonstrar o dano caso a caso.

---

[1] BRASIL. Superior Tribunal de Justiça. Agravo em Recurso Especial nº 2.130.619/SP. Agravante: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Agravada: Maria Edite de Souza. Relator: ministro Francisco Falcão, 07 mar. 2023.

[2] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. São Paulo, Revista do Advogado, ano XXXIX, nº 144, nov. 2019, p. 48.

[3] O artigo 5º, inciso I, da LGPD define "dado pessoal" como *"informação relacionada a pessoa natural identificada ou identificável"*; o artigo 5º, inciso II, define "dado pessoal sensível" como *"dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"*.

[4] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3 ed. Rio de Janeiro: Forense, 2021, p. 83-84.

[5] SOLOVE, Daniel J. *Data is what data does: regulating use, harm, and risk instead of sensitive data. Northwestern University Law Review*, v. 118, jan. 2023, p. 35-36. Disponível em: https://ssrn.com/abstract=4322198.

[6] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3 ed. Rio de Janeiro: Forense, 2021, p. 84.

[7] SOLOVE, Daniel J. *Data is what data does: regulating use, harm, and risk instead of sensitive data. Northwestern University Law Review*, v. 118, jan. 2023, p. 35-36.

[8] SOLOVE, Daniel J. *Data is what data does: regulating use, harm, and risk instead of sensitive data. Northwestern University Law Review*, v. 118, jan. 2023, p. 43.

Meta Fields