Migalhas Patrimoniais

Hackeamento de dados pessoais e responsabilidade do fornecedor: releitura do CDC pela óptica da LGPD

Aline de Miranda Valverde Terra

sexta-feira, 9 de julho de 2021

O ano de 2021 tem sido profícuo em megavazamentos de dados, no Brasil e no exterior. Em janeiro deste ano, noticiou-se o mais grave vazamento em território nacional causado pela invasão de sistemas por *hackers*, com a exposição de dados pessoais de mais de 220 milhões de brasileiros (incluindo falecidos).[1] Em junho, ganhou as manchetes mundiais a notícia do que tem sido designado o maior vazamento da história: mais de 8,4 bilhões de senhas foram compartilhadas em fórum de *hackers*, episódio que ficou conhecido como *RockYou2021*, em alusão ao incidente ocorrido em 2009 que expôs 32 milhões de senhas, designado *RockYou*.[2]

Nesse cenário, assume inegável relevância a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18), cujo artigo 2º elenca entre seus fundamentos, além da defesa do consumidor, o direito à *autodeterminação informativa*, assim entendido o direito fundamental do titular "de manter controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".[3] Busca-se, desse modo, conferir ao sujeito a posição de protagonista acerca das decisões relativas ao uso e à circulação dos seus dados pessoais. O mesmo artigo 2º, em evidente dialética normativa, também estabelece como fundamentos da novel legislação a inovação e o desenvolvimento econômico e tecnológico. E não poderia ser diferente. O artigo 1º da Constituição de 1988 crava, entre os fundamentos da República Federativa do Brasil, a livre iniciativa (inciso IV).

Com efeito, embora a LGPD tenha sido editada com o objetivo precípuo de conferir proteção qualificada aos dados pessoais, tanto mais necessária diante do inexorável incremento das situações lesivas impulsionado pelo crescente desenvolvimento tecnológico, não descuidou de ratificar a necessidade de compatibilizar referida tutela com a promoção de outros valores constitucionalmente relevantes. A harmonia entre fundamentos e valores aparentemente antagônicos é alcançada, entre outras formas, com a opção legislativa em favor do regime de responsabilidade subjetiva do agente de tratamento pelos danos sofridos pelo titular.[4]

No âmbito de relações de consumo, no entanto, a LGPD remeteu as hipóteses de "violação do direito do titular () às regras de responsabilidade previstas na legislação pertinente" (art. 45), ou seja, no Código de Defesa do Consumidor, que estabelece regime de responsabilidade *objetiva*. Nesse cenário, o desafio do intérprete reside em superar a insidiosa tentação de aplicar as regras da legislação consumerista mecânica e isoladamente, como se fossem microssistema encapsulado e imune aos influxos das demais leis do ordenamento jurídico.

A evolução da ciência e da tecnologia desde a edição do CDC, há exatos 30 anos, produziu intenso impacto na sociedade brasileira e, especificamente, no mercado de consumo, tornando, por vezes, anacrônica a legislação consumerista, a requerer o seu cotejo com regulamentações elaboradas para setores específicos, a exemplo da LGPD. Por isso mesmo, há de se atribuir aos artigos 12 e 14 do CDC sentido condizente com todos os fundamentos da LGPD bem como com todas as especificidades envolvidas no tratamento de dados no meio digital, de modo a garantir a máxima proteção aos direitos do consumidor sem comprimir ilegitimamente a livre iniciativa e o desenvolvimento econômico e tecnológico.

Nos termos do CDC, a responsabilidade pelo fato do produto ou do serviço pressupõe *acidente de consumo*, com danos efetivos para o consumidor, cuja reparação se impõe; trata-se de reflexo da atribuição, ao fornecedor, do *dever de segurança* quanto aos produtos e serviços que coloca no mercado. Já a responsabilidade pelo vício se verifica quando o produto ou o serviço se revela inadequado às suas finalidades e à sua função, a conferir ao consumidor o direito de exigir o conserto do produto, a troca por outro em perfeitas condições ou a devolução do preço.

Cuidando-se de tratamento de dados, aplica-se a mesma classificação oferecida pelo CDC. Há mero *vício do serviço* quando o consumidor, por falha no sistema, não consegue, por exemplo, alterar seus dados em cadastro anteriormente realizado com a finalidade de realizar compras *online*. De outro lado, há *acidente de consumo* quando certo laboratório de análises clínicas permite acesso indiscriminado, por sua página na *internet*, aos resultados dos exames de seus pacientes.

A LGPD, por sua vez, traz o conceito de *incidente de segurança*, definido pelo Glossário de Segurança da Informação como "qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança dos sistemas de computação ou das redes de computadores".[5] Portanto, parece correto afirmar que *incidente de segurança* não se confunde com *acidente de segurança*. O *incidente de segurança* encerra gênero, a abarcar, repita-se, qualquer eventos relacionados a segurança dos dados, a exemplo da perda de dados pessoais dos consumidores. Já o *acidente de segurança*, espécie de *incidente de segurança*, configura-se sempre que referido evento causar danos aos consumidores, como pode se verificar, a depender das circunstâncias, quando há acesso não autorizados por terceiros a determinados dados pessoais. Referida compreensão é corroborada pela letra do artigo 48 da LGPD, segundo o qual "o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de *incidente de segurança que possa acarretar risco ou dano relevante aos titulares*" (grifou-se).[6] Nota-se, assim, que há incidentes de segurança que não acarretam danos aos titulares, pelo que não se qualificam como *acidente de segurança* e tampouco geram o dever de indenizar.

O Código de Defesa do Consumidor exige a presença de elemento específico para a configuração da responsabilidade do fornecedor, o *defeito* do produto ou do serviço, que se relaciona à sua *desconformidade com a legítima expectativa do consumidor*. Não se trata, todavia, da expectativa de segurança daquele específico consumidor que sofreu os danos, mas da expectativa de segurança do *consumidor médio* nas mesmas circunstâncias.

Ademais, a expectativa de segurança há de ser *razoável*. Não há, com efeito, expectativa legítima de segurança absoluta. Existem variados graus de segurança, e apenas alguns deles podem ser legitimamente esperados pelo consumidor. O desafio do intérprete está em identificar os graus de segurança que estão abarcados pela expectativa legítima do consumidor e cuja violação configura defeito do produto ou serviço. A análise, que já não é simples, torna-se ainda mais tormentosa quando se cuida de tratamento de dados no ambiente digital. Para tanto, os parágrafos 1º e 2º dos artigos 12 e 14 do CDC bem como os incisos do artigo 44 da LGPD oferecem relevantes parâmetros a serem considerados.

Em primeiro lugar, há de se levar em conta o meio empregado para o tratamento dos dados. Parece não haver dúvidas de que o tratamento de dados por meio digital oferece riscos diversos daqueles verificados no tratamento desses mesmos dados fora do ambiente virtual. O consumidor que guarda seus documentos em papel, por exemplo, sabe que eles podem se perder ou se deteriorar, o consumidor que guarda seus documentos em nuvem ou mesmo no seu computador sabe que está sujeito a vírus, ainda que adquira o melhor antivírus disponível no mercado - aliás, as periódicas atualizações do *software* voltadas a combater os novos vírus em permanente desenvolvimento ratificam a afirmação.

A suscetibilidade a violações do meio digital é amplamente conhecida pelo mercado consumidor, sobretudo em sociedades tecnológicas, como corrobora pesquisa realizada entre agosto e setembro de 2017, pela PricewaterhouseCoopers (PwC), que revelou que 69% dos consumidores acreditam que as companhias estão *vulneráveis* a ciberataques.[7] É verdade, todavia, que o fornecedor deve buscar superar as vulnerabilidades do seu sistema, mas se a própria NASA e o FBI foram vítimas de *hackers*,[8] nenhum consumidor pode ter a *legítima* expectativa de proteção total e absoluta de seus dados, quem quer que seja o agente de tratamento.

De todo modo, embora o *consumidor médio* conheça a vulnerabilidade insita ao meio digital, em situações específicas nas quais a natureza dos dados tratados ou a própria atividade exercida pelo agente suscite expectativa legítima de maior segurança do que a ordinariamente esperada, a divulgação de dados decorrente de fontes externas poderá não configurar defeito se o fornecedor houver informado adequadamente o grau de segurança oferecido no tratamento, parametrizando, assim, a legítima expectativa do consumidor.

Note-se, ainda, que o § 1º do artigo 46 prevê a possibilidade de a Autoridade Nacional de Proteção de Dados estabelecer padrões técnicos mínimos de segurança levando em consideração "as características específicas do tratamento" e "*o estado atual da tecnologia*". Em cotejo com o inciso III do artigo 44, extrai-se do dispositivo que, ao menos no que tange a incidentes de segurança, o *risco de desenvolvimento* afasta a responsabilidade do fornecedor, já que ausente o defeito do serviço.

O legislador reconhece, assim, que o meio digital está exposto a acelerado e ininterrupto desenvolvimento tecnológico, o que potencializa os riscos de acesso não autorizado de terceiros aos dados tratados pelo agente. Desse modo, se o fornecedor adotar a tecnologia disponível naquela época no mercado e ainda assim sobrevier ataque *hacker* que, valendo-se de tecnologia nova, quebre a segurança do sistema, restará configurado o *risco de desenvolvimento*, afastando-se a configuração do defeito e, consequentemente, o dever de indenizar.

No que tange ao nexo de causalidade, segundo elemento da responsabilidade civil, é possível que no decurso de cadeia causal dirigida à produção do dano outra causa autônoma a interrompa e provoque, ela própria, o dano. Nesse caso, o agente deflagrador da primeira cadeia causal não será obrigado a indenizar, pois o outro evento alterou o curso dos acontecimentos e rompeu o nexo de causalidade original. É exatamente o que ocorre na hipótese de fato de terceiro, expressamente previsto como excludente de responsabilidade tanto nos artigos 12, § 3º, III e 14, § 3º, II do CDC quanto no artigo 43, III da LGPD.

O fato de terceiro rompe o nexo de causalidade porque o dano resulta direta e imediatamente da atuação desse terceiro, não já da atividade do agente. Terceiro é pessoa estranha à relação original, cujo comportamento implica a realização autônoma do fato danoso. No entanto, tem-se entendido que para afastar o dever de indenizar, o fato de terceiro há de ser *externo*, isto é, *estranho* à atividade exercida pelo agente, de modo a não se inserir no seu campo de influência e atuação. O fato de terceiro *interno*, ligado aos riscos da atividade desenvolvida pelo agente, não exclui a responsabilidade do fornecedor.

Veja-se, por exemplo, o teor da Súmula 479 do Superior Tribunal de Justiça, segundo a qual "as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros *no âmbito de operações bancárias*" (grifou-se). A partir da dicção da Súmula, reconhece-se como fortuito interno a atuação de terceiros desde que decorrente da atividade fim prestada pela instituição financeira, a exemplo da clonagem de cartão de crédito ou da emissão de cheque com assinatura falsa. Em todos esses casos, a atuação do terceiro ocorre no âmbito da própria atividade exercida pela instituição financeira, vale dizer, a fraude é meio para obtenção de vantagem extraída diretamente da atividade fim desempenhada pela instituição financeira. É justamente por isso que se considera que a atuação do terceiro se qualifica como fortuito interno, a ensejar a responsabilidade da instituição financeira pelos danos causados aos correntistas.

De outro lado, "sequestro relâmpago" iniciado fora da agência bancária, seguido de saques de valores no interior de agência bancária, tem sido considerado fortuito externo.[9] Nesse caso, a agência bancária figura como mera *oportunidade* para a atuação criminosa, pelo que a ação do terceiro não se liga diretamente à atividade da instituição financeira. Pela mesma lógica, se há divulgação de dados de correntista em razão de atuação *hacker*, mas essa exposição não resulta em qualquer fraude bancária naquela instituição ou outro benefício auferido da atividade fim prestada por essa mesma instituição financeira, sua responsabilidade não poderá ser aferida com base na Súmula 479, e o ataque de terceiro deverá ser considerado fortuito externo se não houver defeito no tratamento desses dados.

De regra, portanto, há de se reconhecer que se o fornecedor não presta serviço de tratamento de dados pessoais com atividade fim, realizando-o como meio para executar o serviço precípuo a que se destina, a divulgação de dados provocada por *hacker* se qualifica, de regra, como fato de terceiro externo, rompendo o nexo de causalidade entre a atividade do prestador de serviço e o dano porventura sofrido pelo consumidor, desde que não configurado defeito no tratamento.

Por fim, duas observações derradeiras se impõem. Em primeiro lugar, não existe responsabilidade sem dano, nem responsabilidade por mero *risco de dano*, como se poderia pretender extrair do *caput* do já mencionado artigo 48. Se o incidente de segurança não causar danos, não se deflagra a atuação da responsabilidade civil, sem prejuízo do cabimento de outras medidas a fim não só de restabelecer a segurança necessária, mas, sobretudo, de prevenir a própria ocorrência de danos aos consumidores. Ademais, se a indenização se mede pela extensão do dano (art. 944, Código Civil), todas as medidas adotadas pelo agente de tratamento capazes efetivamente de mitigar os danos (art. 48, § 2º) devem ser consideradas para a quantificação da indenização: quanto mais eficazes forem as medidas, maior a redução do dano e, consequentemente, menor a indenização devida.

Não há dúvidas de que o Código de Defesa do Consumidor representou divisor de águas na proteção dos direitos dos consumidores, erigindo-se como verdadeiro marco civilizatório nas relações entre consumidores e fornecedores. Cuida-se, todavia, de legislação marcada pelo seu tempo. Por essa razão, afigura-se fundamental reler os artigos do CDC com cotejo com as disposições da LGPD, que incorpora a seus conceitos as peculiaridades do meio digital. Não se trata, em definitivo, de vulnerar os direitos dos consumidores cujos dados são tratados digitalmente, mas de lhes conferir a máxima proteção possível em cenário de desenfreado desenvolvimento tecnológico sem, com isso, descurar de outros valores igualmente caros à ordem jurídica. Ao que parece, apenas assim se alcança o necessário equilíbrio entre os princípios fundantes da República Federativa do Brasil.

---

1 Disponível em: clique aqui. Acesso em 05 jul. 2021.

2 Disponível em: clique aqui. Acesso em 05 jul. 2021.

3 Stefano Rodotà, *A vida na sociedade de vigilância*: a privacidade hoje, org. Maria Celina Bodin de Moraes, trad. Danilo Doneda e Luciana Cabral Doneda, Rio de Janeiro: Renovar, 2008, p. 15.

4 A propósito, seja consentido remeter a Aline de Miranda Valverde Terra; Gustavo Tepedino; Gisela Sampaio da Cruz Guedes, *Fundamentos do direito civil*: responsabilidade civil, 2ª ed. rev. atual. e ampl., Forense: Rio de Janeiro, p. 287 *et. seq.*

5 Disponível em clique aqui. Acesso em 05 fev. 2021.

6 No mesmo sentido, confira-se a definição oferecida pela Autoridade Nacional de Proteção de Dados: "um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais". Disponível em: clique aqui. Acesso em 05 jun. 2021.

7 Disponível em clique aqui. Acesso em 02 fev. 2021.

8 Disponível em clique aqui. Acesso em 02 fev. 2021.

9 TJ/SP, 11ª CDPriv, AC 1009442-85.2019.8.26.0008, Rel. Des. Gil Coelho, julg. 10.06.2020.

Atualizado em: 9/7/2021 10:58

COORDENAÇÃO

Thamis Dalsenter é coordenadora acadêmica do Instituto de Direito da PUC-Rio. Doutora em Direito Civil pela UERJ. Mestre em Teoria do Estado e Direito Constitucional da PUC-Rio. Professora de Direito Civil do Departamento de Direito da PUC-Rio.

outras edições

MIGALHAS PATRIMONIAIS - MAIS LIDAS

1 Força maior e caso fortuito: o efeito de fatos incontroláveis pelas partes nos negócios jurídicos patrimoniais

2 O conflito de competência em tempos de coronavírus: Entre um federalismo que está nu e um constitucionalismo pragmático

3 Uma releitura do direito real de habitação na sucessão hereditária

4 Usucapião familiar, composse e condomínio: um cotejo necessário

5 O planejamento sucessório e a proteção de herdeiros menores ou com deficiência pelo testamento