Visão do Direito



Leonardo Corrêa
Sócio do 3C LAW | Corrêa & Conforti Advogados, com LL.M pela University of Pennsylvania (EUA). Cofundador e presidente da Lexum

A reforma que já foi feita sem votação

Tramita no Senado a reforma do Código Civil (Projeto de Lei 4/2025), que trata da responsabilidade civil no ambiente digital. Definir quem suporta o risco cibernético cabe ao Congresso Nacional, não ao Judiciário. Antes da votação, alguns tribunais já construíam, por presunção, regime não previsto em lei.

O Projeto de Lei exige segurança compatível com o risco e condiciona a responsabilidade sem culpa a risco "especial e diferenciado", aferido por estatísticas, prova técnica e classificação regulatória. Não autoriza deduzir responsabilidade do êxito de um ataque. A Emenda 211 do projeto afasta o dever de indenizar quando comprovada a adoção, de boa-fé, das medidas disponíveis para evitar ou mitigar o dano. Já a Emenda 209 exige "falha ou omissão" dos prestadores digitais.

No REsp 2.121.904/SP, relatado pela ministra Nancy Andrighi e julgado por unanimidade, em fevereiro de 2025, pela Terceira Turma do Superior Tribunal de Justiça (STJ), firmou-se que, em seguro de vida, o vazamento de dados sensíveis do segurado gera responsabilidade objetiva da seguradora e dano moral presumido. O acórdão transcreve o artigo 44 da Lei Geral de Proteção de Dados (LGPD): o tratamento é irregular quando não oferece a segurança que o titular pode esperar, considerados os riscos razoáveis e as técnicas disponíveis à época. Mas o dispositivo desaparece da fundamentação, e a conclusão prescinde dele. Esse artigo fixa parâmetro contextual, não absoluto, para aferir a irregularidade.

A seguradora alegou adotar protocolos de segurança. O Tribunal de origem disse que não os esclareceu, embora a prova requerida pela empresa tenha sido indeferida. Indefere-se a prova e depois se cobra a ausência. Falha de segurança é questão técnica, dependente de perícia.

A responsabilidade objetiva não é automática. O Código de Defesa do Consumidor incide na relação securitária e dispensa a prova de culpa, não a do defeito, do dano e do nexo causal. Se o sucesso da invasão "prova" o defeito, a natureza dos dados "prova" o dano e o nexo resulta dessas presunções, chega-se à responsabilidade por risco integral.

A LGPD prevê outra sequência. O artigo 42 da legislação impõe reparação a quem causar dano em violação à lei. O artigo 43 permite demonstrar que não houve violação ou que o dano decorreu de culpa exclusiva do titular ou de terceiro. Já o 44 exige que a ausência de medidas de segurança tenha causado o dano. O nexo continua necessário – e foi o ponto menos examinado. Não se identificou qual informação do segurado foi acessada nem que consequência produziu.

Há controvérsia sobre o conceito de dado pessoal sensível. No AREsp 2.130.619/SP, julgado em 2023 pela Segunda Turma do STJ, afirmou-se que o artigo 5º, II, contém "rol taxativo". Dois anos depois, porém, a categoria passou a abranger informações capazes de gerar discriminação, "sobretudo" as previstas na lista legal. Rol taxativo em 2023, exemplificativo em 2025, sem alteração da lei.

Foram consideradas sensíveis informações fiscais, bancárias e de saúde. As duas primeiras não constam do artigo 5º. Sobre saúde, o comunicado dizia que as propostas poderiam conter tais informações. Uma possibilidade genérica virou fato incontroverso.

Também se confundiram risco e dano. O acórdão afirma que o vazamento expõe o consumidor a riscos e reconhece dano moral presumido. Risco é possibilidade; dano é lesão produzida. O risco reclama comunicação e mitigação; o dano, reparação.

Isso não confere imunidade. Vulnerabilidade negligenciada ou descumprimento de padrões técnicos demonstram falha e contribuição causal – nesses casos, a reparação é devida. O que se pede é investigação. Igualar quem investiu em segurança a quem nada fez transforma o dever de comunicar do artigo 48 da LGPD em armadilha para quem o cumpre.

O desfecho do REsp 2.121.904/SP sintetiza o problema. A sentença condenou a seguradora a informar quais dados haviam sido violados e a pagar R$ 10 mil. O Tribunal de origem afastou a obrigação de informar e elevou a indenização para R$ 15 mil; o STJ manteve ambas. O segurado recebe, mas continua sem saber o que vazou.

Cabe ao Judiciário dizer o que a lei é, não o que deveria ser. A responsabilidade objetiva por vazamento de dados me parece má política legislativa. Essa é uma opinião: em democracia, opiniões precisam conquistar votos. Quem pensa o contrário que submeta a proposta ao Legislativo. Entre a indiferença diante de uma invasão e a responsabilidade integral, há o caminho traçado pela LGPD. Um caminho que os tribunais precisam voltar a percorrê-lo.

Visão do Direito



Patrícia Feitosa
Advogada criminalista

Falsas promoções e golpes na Black Friday: como o consumidor deve agir?

A Black Friday movimenta o comércio e amplia as oportunidades de compra, mas também exige atenção diante do aumento de golpes e fraudes. Falsas promoções, anúncios enganosos, perfis fraudulentos, clonagem de cartões e pedidos de pagamento via Pix estão entre os riscos. Conhecer os sinais de alerta e saber como agir diante de uma fraude é fundamental para evitar prejuízos e tentar recuperar o dinheiro.

Dependendo da forma como a fraude é praticada, a conduta pode configurar estelionato, previsto no artigo 171 do Código Penal. O crime ocorre quando alguém utiliza artifícios para induzir ou manter outra pessoa em erro, com o objetivo de obter vantagem ilícita. É importante diferenciar, porém, uma fraude intencional de problemas relacionados ao descumprimento de uma oferta ou contrato. Nem todo problema em uma compra configura crime, e cada caso deve ser analisado individualmente.

Antes de finalizar uma compra, o consumidor deve verificar se está acessando o site oficial da loja, conferir o endereço eletrônico e desconfiar de ofertas muito abaixo dos preços praticados no mercado. Perfis recém-criados, páginas que imitam marcas conhecidas e links suspeitos também merecem atenção. Nos pagamentos via Pix, é essencial conferir o nome do destinatário e os dados da conta antes de confirmar a transferência. Se as informações não corresponderem às da empresa anunciada, o mais seguro é interromper a operação.

Caso perceba que foi vítima de um golpe, a primeira orientação é reunir provas. Comprovantes de pagamento, conversas, anúncios, notas fiscais, e-mails, números de telefone e dados das contas envolvidas podem ajudar a demonstrar como a fraude aconteceu. Também é importante registrar um boletim de ocorrência, que formaliza o caso e pode contribuir para a investigação e a identificação dos responsáveis.

Nos casos envolvendo Pix, o consumidor deve entrar em contato imediatamente com o banco, pelos canais oficiais, e solicitar a contestação da transação por suspeita de fraude, com acionamento do Mecanismo Especial de Devolução (MED), quando cabível. O pedido pode ser feito em até 80 dias após a transferência, mas a recuperação do dinheiro não é garantida. O procedimento depende da análise da instituição financeira e da disponibilidade de recursos nas contas envolvidas. Quanto mais rápida a comunicação, maiores as possibilidades de adoção das medidas para tentar recuperar os valores.

Outro risco é o golpe da recuperação, em que criminosos prometem devolver o dinheiro perdido mediante o pagamento de taxas ou o fornecimento de dados pessoais e bancários. A vítima deve desconfiar de promessas de recuperação garantida e nunca compartilhar senhas ou códigos de segurança com desconhecidos. O caminho mais seguro é procurar diretamente o banco e os canais oficiais das autoridades.

Além de buscar providências para reduzir o prejuízo, o consumidor deve preservar todas as informações relacionadas à fraude, evitando apagar mensagens ou registros da negociação. Esses materiais podem contribuir para a investigação criminal e para eventuais medidas na esfera do consumidor. A prevenção continua sendo a principal forma de proteção: verificar a procedência das ofertas, utilizar canais oficiais e conferir os dados antes de realizar pagamentos são cuidados essenciais durante a Black Friday.