RESPONSALIDADE CIVIL POR ATAQUE HACKER NA LGPD

LIABILITY FOR HACKER ATTACK IN THE LGPD

Amanda Israel Fraga[*]

Kadur Albornoz Da Rosa[**]

Resumo: A LGPD é legislação recente, que visa a proteger os titulares de dados e garantir sua privacidade. Para tanto, a lei estabelece princípios e regras a serem seguidos pelas empresas a fim de manter a segurança das informações. No entanto, não se pode olvidar a possibilidade de ocorrência de lesão a bem jurídico, ou seja, à privacidade dos titulares de dados. Com isso, a lei apresentou o instituto da responsabilidade civil, sem especificar sua aplicação em formato objetivo ou subjetivo, bem como trouxe excludentes de responsabilidade que permitem ao agente de tratamento se eximir da obrigação de ressarcir. Nos casos de ataques hacker, é necessário observar a segurança que era esperada nos sistemas do agente de tratamento, e as regras de privacy by design para garantir ao titular o respeito aos seus direitos.

Palavras-chave: responsabilidade civil; análise econômica do direito, privacidade, ataque hacker, LGPD.

Abstract: The Brazilian's LGPD is recent legislation, which aims to protect data subjects and guarantee their privacy. To this end, the law establishes principles and rules to be followed by companies in order to maintain information security. However, the possibility of harm to legal interests, that is, to the privacy of data subjects, cannot be forgotten. With this, the law introduced the institute of civil liability, without specifying its application in objective or subjective format, as well as bringing liability exclusions that allow the treatment agent to exempt himself from the obligation to reimburse. In cases of hacker attacks, it is necessary to observe the security that was expected in the systems of the processing agent, and the privacy by design rules to guarantee the data subject respect for their rights.

Keywords: liability; economic analysis of law; privacy; hacker attack.

1 INTRODUÇÃO

[*] Coordenadora de Compliance e LGPD da J&T Express Brasil. MBA em Auditoria e Compliance pela Universidade LaSalle e especialista em Direito Digital, Proteção de Dados e Cibersegurança pela PUCPR.

[**] Advogado sócio do escritório Albornoz Jordão Advogados Associados. Mestre em Direito da Empresa e dos Negócios pela UNISINOS.

A responsabilidade civil é instituto que visa a evitar lesões aos direitos de outrem, bem como a reparar quando se concretiza, trazendo equilíbrio para a relação. A lei n. 13.709/2018 (LGPD) (Brasil, 2018) trouxe a responsabilidade civil decorrente de violações aos direitos do titular, sem especificar, sua classificação entre responsabilidade objetiva ou subjetiva.

Nesse contexto, surgem dúvidas sobre a forma de aplicação da responsabilização pelo ilícito civil, a ser desvendado, corroborando a legislação em pauta, em conjunto com o Código de Defesa do Consumidor e o Código Civil. Diante da solidariedade entre os agentes de tratamento, surgem novos contornos a serem analisados, especialmente quando se trata de ataques hacker sofridos por corporações e a forma de reparar os danos aos titulares.

Ainda, necessário avaliar as excludentes de responsabilidade, especialmente no que tange à culpa exclusiva de terceiro, que nos casos de ataque hacker deve ser devidamente observada no que toca à análise econômica do direito e ao que era esperado dos agentes de tratamento, em termos de segurança da informação, para proteção dos dados pessoais.

A análise econômica do direito é mecanismo que permite aos juristas a análise dos fenômenos jurídicos observando os princípios das ciências econômicas. Através desta avaliação é possível identificar, de forma racional econômica, aquele agente diligente, do negligente. A aplicação desse instrumento, permite que se vislumbre a aplicação, pela empresa, de formas adequadas para garantia da privacidade desde a concepção do produto (*privacy by design*), trazendo ao titular de dados a segurança esperada para a prestação do serviço.

Considerando que o titular de dados tem expectativas acerca da segurança aplicada aos produtos e serviços, cabe aos agentes de tratamento identificarem formas de prevenir ataques hacker e ações de engenharia social, visando a evitar fraudes e violações aos seus sistemas, investindo o que se é esperado e proporcional para evitar o dano. No entanto, ocorrendo a lesão, necessário analisar, a responsabilidade do agente de tratamento em relação à segurança de seus sistemas, para eventual aplicabilidade de excludente de responsabilidade, por culpa exclusiva de terceiro.

2 RESPONSABILIDADE CIVIL NA LGPD

O instituto da responsabilidade civil permite um olhar único, contemporâneo e compreensivo, refletindo as mudanças contínuas da sociedade. Observando-se sociedades plurais e complexas, nas quais os sistemas jurídicos são formados não apenas por regras, mas também por princípios, a responsabilidade civil tem o papel de traçar contornos dos caminhos que seguiremos (Farias; Netto e Rosenvald, 2019).

A responsabilidade civil está baseada no pilar que visa a evitar as lesões aos direitos de outrem. No entanto, quando a lesão se concretiza, é necessário buscar uma forma de compensação do dano causado, com o objetivo de restabelecer o equilíbrio.

A lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018), apresentou o instituto da responsabilidade civil, demonstrando as situações nas quais o Controlador e o Operador, agentes de tratamento, devem indenizar o titular de dados pessoais, pessoa a quem se referem os dados pessoais objeto do tratamento.

O artigo 42 desta legislação declarou a solidariedade entre os agentes de tratamento que causarem dano aos titulares de dados, sendo que, o operador responderá quando descumprir as obrigações da legislação de proteção de dados ou, quando desviar das orientações lícitas prestadas pelo controlador. Os controladores que, por sua vez, atuarem na relação jurídica diretamente, responderão solidariamente, salvo nos casos de excludentes de responsabilidade.

Destaca-se ainda, o fato de a legislação permitir a reparação civil em pluralidade de espécies de danos, sejam eles patrimoniais, morais, individuais ou coletivos. Visando a evitar os danos aos titulares de dados, em seu artigo 44, ressaltou-se a necessidade de o tratamento de dados pessoais ocorrer de forma regular, ou seja, oferecendo a segurança a qual o titular deve esperar, consideradas circunstâncias relevantes como, o modo de tratamento e as técnicas disponíveis a época em que foi realizado.

Observa-se, portanto, que o artigo 44 da LGPD apresenta uma versão adaptada do "defeito de serviço", constante no art. 14, § 1º, do Código de Defesa do Consumidor. Nesse ponto, embora a LGPD não explicite o conceito de tratamento defeituoso, cabe uma construção análoga à legislação consumerista para aplicação da responsabilidade do fornecedor de produtos ou serviços, que ensejaria a responsabilização objetiva, que trataremos a seguir (Schreiber, 2021).

Dentre as diversas obrigações previstas na legislação, evidencia-se o dever de os agentes de tratamento adotarem medidas de segurança técnicas e administrativa, para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

As medidas técnicas são aquelas adotadas no âmbito da tecnologia da informação, com utilização de recursos informáticos dotados de funcionalidades que permitam a segurança da informação, tais como softwares, ferramentas de autenticação de sistemas, criptografias, detectores de invasões de sistemas. As medidas administrativas, por sua vez, são aquelas aplicadas em questões administrativas gerenciais, dentre as quais se destacam as medidas jurídicas, como a alteração de cláusulas contratuais e a elaboração de políticas de privacidade (Maldonado e Blum, 2019).

Em relação à adoção de medidas de segurança, o legislador foi categórico ao impor aos agentes de tratamento sua realização, visto que se utilizou da expressão “devem”. A imposição legal da obrigação apresentada pelo legislador é ressaltada no parágrafo único do art. 44, afirmando que os agentes de tratamento responderão por danos decorrentes de violações de segurança, quando não observarem as medidas previstas no art. 46 da lei.

Para a aplicação da responsabilidade civil é sabida a necessidade de se comprovar a conduta, o dano e o nexo de causalidade entre ambos. Mais do que isso, em determinados casos, se faz imperioso demonstrar a culpa ou o dolo do agente para sua responsabilização, questão controversa na LGPD.

2.1 Responsabilidade Civil Objetiva e Subjetiva

O artigo 42 da LGPD não identificou de forma clara o regime aplicável à responsabilidade civil por danos causados aos titulares de dados pessoais. O referido artigo não menciona expressamente a culpa, ou a expressão “independentemente de culpa”, como se vislumbra no Código Civil e no Código de Defesa do Consumidor, de forma que, pela omissão, poderia presumir-se uma preferência pela responsabilização subjetiva.

Nesse sentido, a parte final do artigo 42, que se refere ao dano causado por “violação à legislação de proteção de dados pessoais” sugere a responsabilização fundamentada na

desobediência a deveres jurídicos, que ensejaria a culpa normativa, e que expressa redação similar ao disposto no regulamento europeu, com defesa da responsabilização subjetiva. Sabe-se que a responsabilidade subjetiva é fundamentada na culpa do agente, ou seja, na violação a um dever jurídico, de forma que, uma leitura inicial ao artigo 42 corresponderia a responsabilidade subjetiva (Schreiber, 2021).

No entanto, os dispositivos legais não podem ser analisados isoladamente, devem corroborar o conjunto legislativo, não apenas do conteúdo da Lei Geral de Proteção de Dados, mas também das demais normas jurídicas que integram o ordenamento, especialmente, o Código Civil e o Código de Defesa do Consumidor, que tratou da proteção dos dados pessoais antes mesmo da promulgação de legislação específica sobre o tema. Nesse ponto, tem-se a questão referente ao defeito do serviço, uma vez que, pela análise do disposto no artigo 44, se observa a analogia com as disposições previstas na legislação consumerista que motivam a responsabilização objetiva, que independe de culpa do agente.

Nesse contexto, nota-se que o objetivo central da LGPD foi contemplar o titular de dados com ampla proteção, garantindo sua autodeterminação informativa e resguardando a segurança no tratamento dos dados pessoais. Com isso, o disposto no parágrafo único do artigo 44 visa a apresentar nova hipótese de responsabilidade civil aos agentes de tratamento, qual seja, pela ausência de medidas protetivas indicadas no artigo 46, que alude à previsão de serviço defeituoso, contida na legislação consumerista e que provoca a responsabilização objetiva do agente causador do dano, fundada sobre o risco, como se observa no inciso II do artigo 44 (Schreiber, 2021).

O diálogo com a legislação de proteção ao consumidor se destaca pelo artigo 45, que dispõe sobre a aplicabilidade da legislação pertinente e das regras referentes à responsabilização, nos casos de relação de consumo. Ademais, a regra geral de responsabilidade objetiva, prevista no parágrafo único do artigo 927 do Código Civil também poderia ser aplicada, diante da hiperconectividade que vivenciamos a suscitação do risco inerente às atividades de tratamento de dados.

Assim, tem-se que a análise conjunta das legislações e as interpretações trazidas na LGPD ensejam regimes distintos de responsabilização, comportando a análise da responsabilidade subjetiva e objetiva, a depende do caso concreto e da avaliação judicial. No

entanto, importante ressalvar que, independentemente do regime de responsabilização adotado, imprescindível será a comprovação do nexo de causalidade.

2.2 Nexo de causalidade e a inversão do ônus da prova

Para fins da responsabilização civil, indispensável se torna a comprovação da conduta do agente de tratamento, do dano e do nexo de causalidade, ressalvada a aplicabilidade do regime da responsabilidade, que poderá ensejar a demonstração de culpa ou não. A relação de causalidade, ou seja, a demonstração de causa e consequência é imprescindível para configuração do dever de indenizar.

Em relação ao tratamento de dados pessoais, a comprovação do nexo causal é algo de extrema complexidade, especialmente porque os vazamentos de dados, em uma sociedade amplamente conectada, podem decorrer de sucessivas transferências ou apropriação de dados, que podem prejudicar a investigação e identificação do agente que deu causa do dano (Schreiber, 2021).

Nesse sentido, a LGPD prevê mecanismo de suma importância para prova do nexo de causalidade, fundada na inversão do ônus da prova, prevista no parágrafo segundo, do artigo 42, e que será aliada do titular de dados, em casos de responsabilização civil por ataques hacker. Em casos de danos decorrentes de ataques cibernéticos, através da inversão do ônus da prova, o agente de tratamento poderá realizar a prova positiva, demonstrando que cumpriu com o disposto na legislação, adotando medidas técnicas aptas a proteger os dados por ele armazenados e que as medidas foram insuficientes, o que direciona às excludentes de responsabilidade.

2.3 Excludentes de Responsabilidade

O artigo 43 da LGPD apresentou três excludentes de responsabilidade, sendo elas (i) quando o agente de tratamento não realizou o tratamento de dados pessoais que lhe é atribuído; (ii) que, embora tenha realizado o tratamento, não houve violação à legislação de proteção de dados; e (iii) quando o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. No caso, para fins de análise no presente artigo, observa-se a terceira hipótese,

visto que estamos diante da análise da possibilidade de responsabilização do agente de tratamento, em caso de ataque hacker.

Nesse caso, deve-se observar se a conduta de terceiro foi causa exclusiva para a perpetração do dano, pois, em casos de culpa concorrente, não cabe o afastamento da responsabilização do agente de tratamento, mas sim uma avaliação do quantum indenizatório pelo qual responderá, conforme a proporção de sua atuação para o evento danoso. Para que a excludente seja aplicável, deve-se comprovar que o fato que causou o dano não lhe é imputável de nenhuma forma (Schreiber, 2021).

Em casos de ataques hacker uma discussão interessante se vislumbra. Isso porque, é necessário avaliar se a invasão de um sistema que armazena dados pessoais, por pessoal mal-intencionada ou que não dispõe de autorização, poderia ensejar a culpa de terceiro. Tem-se que, nenhum sistema é completamente seguro, estando sujeito a vulnerabilidades, até porque as tecnologias evoluem constante e rapidamente. No entanto, a aplicabilidade da excludente de responsabilidade nestes casos, demandaria a demonstração inequívoca de que o agente de tratamento adotou todas as medidas técnicas e administrativas em seu ambiente visando a evitar a violação das informações, ou seja, comprovar que o ataque foi perpetrado por técnicas inovadoras e que as medidas de segurança adotadas eram razoáveis e eficientes às tecnologias da época (Maldonado e Blum, 2019).

3 ANÁLISE ECONÔMICA DO DIREITO E RESPONSABILIDADE CIVIL

A Análise Econômica do Direito, ou AED, é ferramenta que permite aos juristas analisar os fenômenos jurídicos à luz de princípios das ciências econômicas (Posner, 1986). No caso da responsabilidade civil, tal ferramenta possui ainda mais importância, considerando que, ao fim e ao cabo, a responsabilidade civil é disciplina jurídica que tem como objetivo a alocação do ônus pela reparação de danos sofridos entre sujeitos de direito (Rosenvald, 2013).

A doutrina clássica costuma analisar a responsabilidade civil no âmbito das relações entre sujeitos de direito envolvidos em uma relação específica, mas a AED permite extrapolar tal relação, e verificar os efeitos das regras de responsabilidade civil em uma escala macroeconômica. Essa análise mais abrangente das regras jurídicas que regem a responsabilidade civil nos permite medir não somente o custo da reparação do dano, mas o

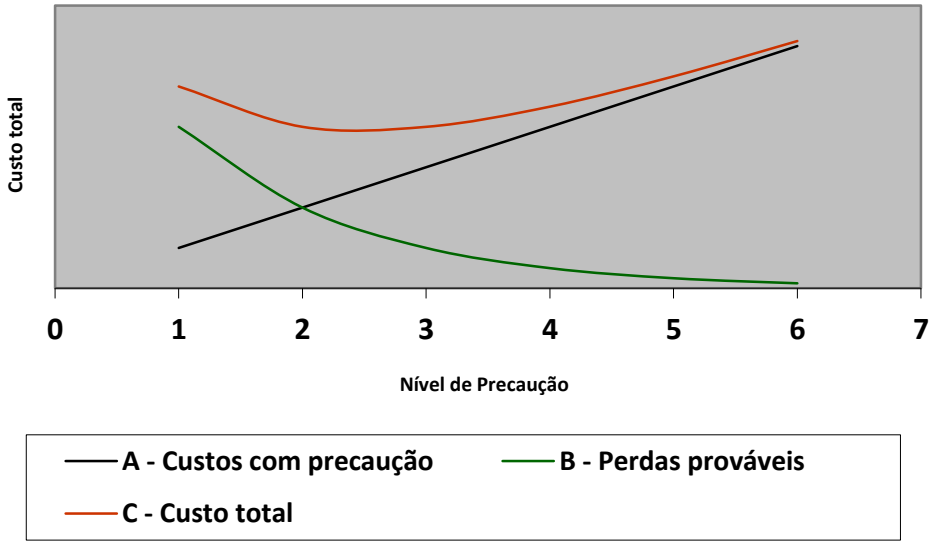
custo social — que corresponde à soma dos custos de prevenção e reparação, bem como as perdas a terceiros (Coase, 1960).

Nesse contexto, as regras de responsabilidade civil representam incentivos que guiam as ações daqueles que vivem em sociedade. Uma das principais abordagens no campo da AED foi a trazida pelo juiz Learned Hand em *United States v. Carrol Towing Co.* Neste julgamento, Hand analisou a responsabilidade civil do proprietário de uma balsa — *Carrol* — que se desprendeu do cais em virtude de rompimento das amarras e afundou outra balsa — Anna C — cuja carga pertencia ao governo dos Estados Unidos. Na decisão, Hand considerou três critérios para fins de apurar a existência de negligência: (i) a probabilidade do evento danoso; (ii) a gravidade do dano, caso ocorra o evento danoso e (iii) o custo de precaução. Esses critérios interagiram de forma a criar um parâmetro para a apuração de negligência por parte do causador do dano: se o custo de precaução (B) é inferior à multiplicação da chance de ocorrência do evento (P) pelo dano potencial (L), a não adoção da precaução constitui negligência, e dá causa à reparação. Assim, surgiu a fórmula B<PL como representativo da negligência, e B>PL como representativo da diligência. No caso concreto, se definiu que as medidas que poderiam ter sido adotadas para prevenir o acidente eram baixas em relação à probabilidade e o risco do acidente, motivo pelo qual a parte foi condenada a indenizar o governo americano[1].

Abaixo, podemos ver um gráfico que representa essa função:

Figura 1 – Representação Gráfica da Fórmula de Hand

[1] A medida preventiva em questão era ter um operador na balsa. Considerando que o porto estava lotado, e que o acidente ocorreu no período diurno, apurou-se que o risco do acidente era razoável, e que a medida era de baixo custo perante o prejuízo potencial de afundar outra embarcação.



Fonte: Figura dos autores

No gráfico acima podemos verificar que os custos com precaução aumentam em escala geométrica constante, enquanto as perdas prováveis reduzem de forma vertiginosa no início, e após tem um declínio no retorno em relação aos custos com precaução. No ponto 2, onde há a intersecção entre as curvas A e B, se encontra o ponto ótimo, no qual o custo total é o menor possível. Pela regra de Hand, a zona antes do ponto 2 — onde os gastos com precaução são inferiores ao ponto ótimo —é conhecida como zona de negligência, enquanto a zona posterior ao ponto 2 — onde os custos com precaução são superiores ao ponto ótimo — é conhecida como zona de diligência.

Além disso, é possível verificar que em algum momento entre os pontos 5 e 6, o custo total — Curva C, que corresponde à soma entre A e B — supera o custo inicial — onde há nenhuma ou quase nenhuma medida de precaução adotada. A partir desde ponto, é economicamente ineficiente continuar investindo em maiores medidas de precaução, porquanto o custo supera o benefício.

Esta análise é de vital importância, porquanto permite verificar a estrutura de incentivos que guiam a função preventiva da responsabilidade civil. Se o sistema de reparação distingue a indenização devida por aquele que é diligente daquela devida por quem é negligente com base em critério de racionalidade econômica, há incentivo para adotar

medidas de redução de danos até certo ponto. Por outro lado, se não houver distinção entre aquele que é diligente e aquele que é negligente, os incentivos penderão para a não adoção de medidas preventivas. Isso pois, no primeiro exemplo, o custo é maior para aquele que é negligente, enquanto no segundo o custo é maior para quem é diligente.

Essa assunção é válida tanto para os sistemas de responsabilidade civil objetiva quanto para o de responsabilidade civil subjetiva. A diferença está no fato de que um sistema de responsabilidade civil puramente objetiva tende a não criar incentivos para que as possíveis vítimas tomem medidas de precaução. Pelo viés do causador dos incidentes, a tendência é a de adotar medidas de redução da atividade, em local de medidas de redução do risco (Posner, 1986).

Assim, os regimes de responsabilidade civil objetiva tem evoluído para incluir hipóteses de exclusão de responsabilidade, como as já acima referidas, do art. 43 da LGPD.

4 SEGURANÇA DIGITAL

4.1 Privacy by Design

Marcos regulatórios como a LGPD e o GDPR, General Data Protection Regulation, conduzem as organizações para este momento, em que a privacidade dos indivíduos se torna cada vez mais presente, como uma obrigatoriedade da proteção de dados. As organizações precisam se reestruturar, ajustando modelos de negócios, com imposição da privacidade dos usuários desde o início, seja na construção do ambiente físico, na aquisição de novos produtos, sistemas e serviços, no desenvolvimento de políticas, normas e procedimentos, nos termos de uso e confidencialidade, para qualquer ramo do negócio, independentemente do tamanho da empresa. Isso é a privacidade acoplada no desenho, conhecida como Privacy by Design.

Embora a LGPD não mencione expressamente o termo, como ocorre no GDPR, o art. 46 define que: “os agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.”

Nesse sentido, a expressão “medidas de segurança”, apesar de não especificada, não impede que as organizações adotem as melhores práticas para aumento da proteção de seus ambientes críticos, pelo contrário, as incentiva. O art. 25, do GDPR apresenta a proteção de dados desde a concepção e por padrão em sua redação (*Privacy by Design e Privacy by Default*), o que também deverá ser adotado no Brasil, como boas práticas de segurança da informação.

A privacidade é, portanto, o ponto de partida, sendo que a segurança da informação está no seu entorno, considerando-a desde o princípio de projetos, sistemas e processos. Assim, tem-se que a metodologia se refere à proteção da privacidade do usuário desde a concepção de qualquer serviço/produto de tecnologia, informações ou práticas do negócio, o que caracteriza o *Privacy by Design*.

O *Privacy by Default*, por sua vez, é uma decorrência do anterior, e se refere à metodologia que adota por padrão a configuração de privacidade mais restrita possível na fase de coleta dos dados pessoais, garantindo a proteção de forma automática, ainda que o usuário não tenha interação com a máquina. Desse modo, mesmo que o usuário não interaja com a máquina, visando a proteger sua privacidade, esta permanecerá intacta, na medida em que seus dados serão coletados apenas após uma interação. Ainda, serão coletados apenas os dados indispensáveis para funcionamento das aplicações ou para a finalidade do negócio, em observância aos princípios da necessidade e finalidade, previstos na LGPD.

4.2 Segurança esperada pelo titular dos dados

Como visto anteriormente, o art. 44 da LGPD cria uma regra de responsabilização dos agentes de tratamento por não fornecerem a segurança que o titular dos dados pode esperar, em uma reprodução do “defeito de serviço” da esfera consumerista.

É importante destacar que a redação reforça o termo “poderia esperar”, seguida de critérios de apuração da existência ou não de legítima expectativa do titular dos dados. Isso serve para deixar claro que se trata de uma regra de proteção da legítima expectativa de proteção. A distinção é relevante. Se não houvesse essa clareza, o ponto de partida poderia ser o critério subjetivo de qual a expectativa do titular dos dados a qual poderia ser completamente irrazoável, haja vista que a grande maioria dos titulares de dados não possuem

conhecimento apurado sobre segurança digital, não possuindo sequer noção dos riscos do ambiente cibernético.

Nesse ponto, importante enfatizar que não existe sistema digital 100% seguro. Essa afirmação é baseada em diversos fatores. O primeiro deles é o fato de que todos os sistemas de informação atuais são criados por humanos, estando desde já sujeitos a erro por si só. Além disso, os sistemas são desenhados para se defender de uma série de problemas de segurança, pois o custo de uma arquitetura que prevenisse contra todo e qualquer ataque seria quase que proibitivo. O terceiro fator é que os ataques digitais evoluem (Schneier, 2004). Mesmo que se aja de forma proativa, é quase impossível prever todo e qualquer ataque novo que é diariamente criado.

Existe uma verdadeira corrida de armas entre ataque e defesa no ambiente digital, e os atacantes detém a vantagem por diversos fatores: (i) é mais fácil quebrar do que consertar; (ii) quanto mais complexo é um sistema, mais difícil é de prover sua segurança, e a complexidade tem aumentado significativamente; (iii) a natureza dos sistemas cibernéticos tornam mais fácil encontrar uma falha do que consertar todas as vulnerabilidades; (iv) um atacante pode focar em apenas uma espécie de ataque, enquanto um defensor tem que se preparar para todas as possibilidades; (v) a segurança de software em geral é ruim, pois é um nicho ainda muito incipiente. O foco dos desenvolvedores é a eficácia, e não a segurança. Embora isso esteja melhorando, ainda não é o suficiente; (vi) a segurança cibernética é muito técnica, e é muito fácil que o usuário comum erre e remova as camadas de segurança que tenha (Schneier, 2015).

Conhecer essa realidade é importante para fins de determinar qual a legítima expectativa do titular dos dados em relação à segurança dispensada pelos agentes de tratamento.

Nesse sentido, o inciso I do art. 44 da LGPD trata do modo pelo qual o tratamento realizado. Esse fator está intimamente ligado ao conceito de *Privacy by Design*, e ao regramento previsto no art. 46. Isso pois, se os dados forem tratados de forma a privilegiar a privacidade do usuário desde a sua captura, serão menores os potenciais riscos em caso de vazamento.

O inciso II, do art. 4 da LGPD, por sua vez, está ligado à fórmula de Hand explicada no capítulo anterior. Isso porquanto introduz uma análise de custo/benefício. No caso, se

exigirá maior precaução daquele que possuir uma atividade mais lucrativa e/ou que que possua maiores riscos. Ou seja, ao analisar a responsabilidade do agente de tratamento, o julgador deverá sopesar no cuidado exigido o risco da atividade e os resultados que ela proporciona. A título exemplificativo: o *standard* esperado de uma grande empresa que possui os dados como sua principal ferramenta de trabalho — como Facebook ou Google — será diferente de uma pequena empresa que coleta os dados como uma atividade-meio para sua atividade-fim — como uma empresa pequena de e-commerce que coleta os dados apenas para fins de emissão de nota fiscal e entrega da mercadoria.

Por fim, o inciso III trata de avaliar se a vulnerabilidade poderia ter sido evitada pelos métodos disponíveis à época em que o tratamento foi realizado. Esse critério apresentará grande desafio para o Poder Judiciário, por ser eminentemente técnico, e demandar conhecimento acerca da constante evolução dos padrões de segurança digital. No ponto, importante repisar as lições dantes trazidas acerca dos desafios da segurança digital, de que os atacantes sempre estão em vantagem em relação aos defensores, bem como o caráter eminentemente técnico e complexo da segurança digital.

O desafio da tecnicalidade pode ser abordado de, ao menos, duas formas: realização de perícias judiciais e delegação dos critérios de segurança à ANPD – Agência Nacional de Proteção de Dados. A primeira, conquanto mais precisa, apresentará um custo elevado, e será um desafio nos casos de pequena monta. A segunda, por outro lado, tende a ser a mais adotada em casos menos complexos, e auxiliará na padronização dos sistemas de segurança esperados.

É claro que tais critérios devem ser articulados entre si, e apenas a partir da análise da aplicação dos dispositivos é que se poderá traçar uma regra objetiva quanto às expectativas.

4.3 Quem são os *hackers*?

Como visto anteriormente, a segurança digital é uma eterna corrida entre defensores e atacantes, na qual os invasores detém a vantagem. Na linguagem coloquial, o termo *hacker* é associado a atividades infracionais. Na linguagem técnica, contudo, um *hacker* é um entusiasta de tecnologia, que tem como profissão ou hobby estudar os detalhes de um sistema de informação (Caldwell, 2011).

Dentre os *hackers*, existem ao menos três categorias, cuja critério de distinção é a ética profissional: *white hats*, *black hats* e *grey hats*.

Os w*hite hats* são *hackers* que atuam de forma a testar vulnerabilidades e desenvolver formas de resolvê-las. Geralmente, atuam como consultores de segurança digital das empresas, ou participando de programas de recompensas lançados por empresas, nos quais são remunerados por encontrar novas vulnerabilidades.

Os *black hats* são hackers que atuam de forma a explorar as vulnerabilidades dos sistemas para ganho pessoal próprio. Exemplos de sua atuação são invasão de sistemas para roubar dados destinados à revenda, ou "sequestrar" dados e cobrar por seu resgate. Esses são os clássicos *hackers* retratados em filmes.

Por fim, existem os *grey hats* que, como o nome indica, atuam em uma área cinzenta, muitas vezes empregando métodos de moral duvidosa em prol de causas nobres. Via de regra, são ciberativistas, ou entusiastas que agem com base em um código de ética próprio, podendo inclusive lucrar com seus objetivos.

Existem também os *crackers*, uma subcategoria de *black hats* e *grey hats* cujo método de operação é simplesmente causar danos aos sistemas de informação.

Essa distinção é importante, na medida em que a utilização de *white hats* é uma das principais formas pela qual os agentes de tratamento podem aprimorar a segurança de seus sistemas. Além disso, considerando que a probabilidade de um ataque hacker é um dos fatores importantes para fins de fixação da responsabilidade do agente de tratamento, entender as motivações por trás dos ataques de *black hats* e *grey hats* é um dado importante para determinar se os dados em tratamento são um alvo em potencial.

Um exemplo recente foi a invasão da Nvidia realizada pelo grupo Lapsus$ (Alecrim, 2022). Este grupo de hackers invadiu os servidores da empresa e roubou cerca de 1 terabyte de dados confidenciais, e ameaçou divulgá-los publicamente caso a empresa não atendesse uma série de reivindicações, tais como: o desbloqueio do potencial de processamento de placas de vídeo da empresa para a mineração de criptomoedas, bem como a liberação do código-fonte dos drivers da empresa sob licença de software livre.

No caso acima, os hackers atuaram como ciberativistas, mas a empresa se colocou como um alvo ao limitar o poder de processamento de suas placas de vídeo para mineração de criptomoedas, considerando que destravar tal limitação importaria um ganho substancial para

aqueles que exploram tal atividade. Havendo incentivo desta magnitude para a quebra de tal limitação, era de se presumir que a probabilidade de a empresa ser um alvo era altíssima.

4.4 Ataques Hacker e suas espécies

O problema de segurança digital possui componentes tecnológicos, mas é sobretudo um problema das pessoas (Schneier, 2004). Isso pois os usuários são, muitas vezes, a vulnerabilidade do sistema digital. Em um acesso, existem pelo menos três pontos de falha: o usuário, a conexão e o sistema:

Figura 2 – Alvos possíveis no processo de acesso

Fonte: Figura dos autores

A partir desse critério — alvo do ataque — será proposta classificação que auxilia na aplicação das regras de responsabilidade civil da LGPD.

4.3.1 Engenharia social

A maioria dos ataques hackers acontecem por meio de fraude ao usuário. Através de sofisticados esquemas de fraude, os hackers utilizam os dados disponíveis sobre o usuário para convencê-lo a fornecer os dados que precisam — usuário, senha, conta bancária, dentre outros. Tais ataques são denominados como “engenharia social”, e não demandam grande

conhecimento técnico por parte dos hackers. Pontue-se que o usuário, pode ser tanto o titular dos dados, quanto um funcionário dos agentes de tratamento.

A maior proteção contra esse tipo de ataque é a educação dos usuários e a adoção de medidas administrativas que reduzam os danos que a captura dos dados de um simples usuário possa causar.

Uma vez adotadas essas medidas, contudo, a responsabilidade pelo ataque é quase que exclusiva do titular dos dados ou do terceiro, atraindo a incidência da hipótese de exclusão de responsabilidade prevista no art. 43, III, da LGPD.

Exemplos de golpes envolvendo tal tática são: golpes envolvendo ligações falsas e *phishing*.

4.3.2 *Man in the Middle*, ou interceptação

Um segundo ponto de vulnerabilidade é a conexão entre o usuário e o sistema. Nessa espécie de ataque, o hacker se interpõe entre o usuário e o sistema, interceptando os dados trocados, e se aproveitando deles para avançar no seu ataque. Esse tipo de ataque é chamado de *Man in the Middle*, ou MITM. Nessa modalidade, há a necessidade de certa sofisticação técnica, e a vulnerabilidade pode estar na ponta do usuário, na ponta do sistema, ou até em um dos pontos intermediários.

Devido à multiplicidade de possibilidades, e à possibilidade de inversão do ônus da prova prevista pelo art. 42, §2º, da LGPD, a tendência é que o agente de tratamento tenha dificuldades para comprovar que há culpa exclusiva do titular dos dados ou de terceiros. Assim, a melhor estratégia será buscar demonstrar que foram adotadas medidas de proteção que reduzam as chances de um ataque de MITM.

4.3.3 Invasão

Por fim, existem ataques de invasão que tem como método a exploração de falhas do sistema. Esses ataques são o maior desafio por parte dos profissionais de segurança digital. Esses são também o maior desafio na aplicação das regras de responsabilidade civil presentes na LGPD, devido aos nuances técnicos envolvidos.

Para compreender a magnitude do desafio, a cada dia, são detectadas 450.000 novas ameaças, já existindo cerca de 1,4 bilhões de ameaças identificadas (AV-Test Institute, 2022). E isso apenas considerando programas maliciosos que se propagam pela rede — *malwares*. Além deles, existem vulnerabilidades nos sistemas de informação que são explorados por *hackers*, bem como ferramentas que auxiliam na decodificação de senhas a partir dos chamados ataques de força bruta e quebra de criptografia (Schneier, 2004).

A dinamicidade desse ambiente de segurança digital demonstra o desafio da aplicação do disposto no art. 44, III, da LGPD. Sem que a ANPD crie padrões de segurança digital mínimos, que passem por atualização periódica, será quase impossível que esse dispositivo seja aplicado na prática. Essas regras devem também contemplar diferentes níveis de exigência, de forma a diferenciar os agentes de tratamento que são alvos de alta prioridade daqueles que não possuem tanto risco de invasão.

O desafio da aplicação dessas regras, contudo, esbarra na especificidade do conhecimento necessário para avaliar se a empresa está adotando as medidas necessárias, bem como distingui-las das medidas adotadas por mera sinalização.

Um exemplo dado por Schneier (2004) é o da adoção de firewalls por empresas: a maioria dos firewalls são mal configurados e possuem baixa efetividade, mas se popularizaram devido à exigência por parte de auditorias especializadas. Com isso, essa solução acabou sendo adotada por padrão apenas para sinalizar preocupação com a segurança, e para evitar reprovação da auditoria.

Outro ponto é que, assim como existem um número quase infinito de vulnerabilidades a serem exploradas, também existem múltiplas formas de tentar combater o problema. Contudo, devido à tecnicalidade envolvida, é difícil acreditar que um julgador tenha conhecimento suficiente para discernir se a metodologia aplicada por determinado agente de tratamento é adequada.

Não obstante, a partir de uma análise criteriosa dos métodos de invasão, é possível estabelecer alguns parâmetros de análise, que auxiliam a criar zonas de clareza, em meio a toda a incerteza.

No caso de invasão pelo uso de *malwares*, a utilização pelo agente de tratamento de um sistema confiável de rastreamento dessas ameaças constantemente atualizado pode ser considerada uma forma de redução da responsabilidade, pois é uma alternativa relativamente

barata de bloquear um número imenso de ameaças. Por outro lado, não adotar qualquer solução dessa natureza pode ser considerado como um fator de negligência, que atrai a responsabilidade pelos danos causados.

Outro campo de aplicação é o das vulnerabilidades. A cada dia são descobertas novas falhas. Quando essas falhas são recentes e pouco conhecidas, são chamadas de *zero day*. O desconhecimento destas falhas não pode ser causa de responsabilização de um agente de tratamento, exatamente por serem falhas de difícil conhecimento. Uma vez divulgadas por órgãos de segurança, contudo, passa a ser possível a responsabilização daqueles que foram atacados através dessas falhas, a depender do nível de segurança esperada do agente de tratamento. Por outro lado, falhas que já estejam listadas como conhecidas e já estejam há algum tempo sem correção denotam negligência por parte do agente de tratamento, atraindo a responsabilidade por danos causados.

Existem também ataques de força bruta, que são programas que tentam acertar a senha de determinado usuário através do método automatizado de tentativa e erro. Antigamente esses ataques eram de baixa sofisticação, e simplesmente tentavam todas as combinações possíveis, mas com o tempo foram sendo aprimorados, e atualmente possuem dicionários das senhas mais utilizadas e algoritmos de geração de senhas padrão com base nos dados do usuário — data de nascimento, data de casamento, data de nascimento, nome dos filhos, ou até mesmo listas de senhas vazadas, por exemplo — que reduzem o número tentativas necessárias para encontrar a senha do usuário. A forma de reduzir a efetividade desses ataques é obrigar os usuários a usarem senhas com um tamanho razoável, utilizando letras minúsculas, maiúsculas, números e caracteres especiais, o que dificulta a utilização de senhas padrão. A exigência de troca periódica da senha é outra medida de baixo custo que reforça a segurança.

Além dessas medidas de cunho administrativo, o agente de tratamento também pode utilizar mecanismos para reduzir a velocidade/eficácia dos ataques automatizados, tais como solicitar testes de *captcha*. Todas essas medidas indicadas possuem baixo custo/complexidade, e tem a capacidade de reduzir de forma significativa as chances de acesso indevido por *hackers*. Assim, em caso de acesso da conta do usuário por meio de ataques de força bruta, deve ser mitigada a responsabilidade de uma empresa que utilize tais métodos, pois é uma demonstração de diligência.

Se por um lado a existência de regras padrão possa parecer incentivar estagnação no meio de segurança digital, é importante lembrar que as regras de responsabilidade civil não são o único incentivo envolvido na equação de tomada de decisão. A imagem dos agentes de tratamento e sua credibilidade perante o mercado são ativos valiosos. Uma empresa que demonstre um alto índice de incidentes de vazamento/invasão, mesmo que alegue estar seguindo as regras padrão eventualmente estipuladas pela ANPD, acabará atraindo desconfiança de titulares de dados e acionistas, e sofrerá consequências econômicas pela perda de usuários e redução do valor de suas ações.

5 CONCLUSÃO

Ao longo do artigo viu-se que a LGPD não deixou claro qual o regime de responsabilidade civil adotou, o que se reflete em ampla divergência doutrinária acerca do assunto. No entanto, nesse artigo concluiu-se que foi adotado um sistema misto de responsabilidade civil baseado na teoria do risco: regras de responsabilidade objetiva aliadas a hipóteses subjetivas de exclusão/mitigação da responsabilidade. Tal conclusão, contudo, não descarta o fato de que a verdadeira resposta acabará sendo dada pela pragmática.

Em seguida, foram trazidos conceitos básicos da análise econômica do direito a fim de se compreender os efeitos das regras de responsabilidade além da mera relação entre titular e agente de tratamento de dados. Dentre os conceitos explorados, o mais importante é o da fórmula de Hand, que permite distinguir o agente negligente do diligente, e que mais adiante é trazida como critério razoável para apuração da "segurança esperada pelo titular dos dados" prevista no caput do art. 44 da LGPD, refletida no critério previsto em seu inciso II.

Adiante, foi explorada a importância da segurança digital, explicando como ela pode ser implementada desde o desenvolvimento do sistema e da coleta dos dados — *Privacy by Design* e *Privacy by Default* — passando pela identificação dos responsáveis pelos ataques hackers, apresentação dos desafios técnicos de sua implementação, finalizando com a proposição de uma classificação baseada nos pontos de vulnerabilidade explorada pelo atacante na relação de acesso.

Com base nessa classificação proposta, foram trazidas e explicadas três categorias de ataque *hacker*: engenharia social, interceptação — ou *Man in the Middle* — e invasão, e

expostas algumas situações nas quais é possível distinguir de forma clara os agentes de tratamento que atuam de forma diligente e, portanto, estão sujeitos às hipóteses de exclusão/mitigação de responsabilidade por indenizar, bem como aqueles que claramente atuam de forma negligente e, portanto, devem ser obrigados a indenizar o dano em sua integridade.

A classificação aqui proposta não é definitiva, e tem como objetivo, a partir de um critério único, lançar luzes sobre a discussão em um nível multidisciplinar, permitindo evolução de doutrina qualificada sobre o assunto.

REFERÊNCIAS

ALECRIM, E. 2022. Hackers que atacaram ConecteSUS invadem Nvidia e exigem drivers open source. Disponível em: https://tecnoblog.net/noticias/2022/03/02/hackers-que-atacaram-conectesus-invadem-nvidia-e-exigem-drivers-open-source/. Acesso em: 18 jul. 2022.

BRASIL. 2018. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 2024.

AV-TEST INSTITUTE. 2022. Malware. Disponível em: https://www.av-test.org/en/statistics/malware/. Acesso em: 18 jul. 2022.

CALDWELL, T. 2011. Ethical hackers: putting on the white hat. Network Security, (7):10-13.

COASE, R. 1960. The problem of social cost. The Journal of Law and Economics, 3:p. 1-44.

FARIAS, C.C.; NETTO, F.B.; ROSENVALD, N. 2019. Manual de direito civil. 4. ed. Salvador: Juspodivm.

MALDONADO, V.N.; BLUM, R. O. (coord.). 2019. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil.

POSNER, R. 1986. Economic analysis of law. 3. ed. [S.l.]: Wolters Kluwer.

ROSENVALD, N. 2013. As funções da responsabilidade civil: a reparação e a pena civil. São Paulo: Atlas.

SCHNEIER, B**.** 2015. Data and Goliath: the hidden battles to collect your data and control your world. [S.l.]: W. W. Norton.

SCHNEIER, B**.** 2004. Secrets & lies: digital security in a networked world. 2. ed. [S.l.]: John Wiley.

SCHREIBER, A. 2021. Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. In: L.S. MENDES et al. (org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense.