INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS: FORMAS DE TUTELA JURÍDICA

PERSONAL DATA BREACHES: LEGAL REMEDIES

Sergio Marcos Carvalho de Avila Negri[1]

Carolina Fiorini Ramos Giovanini[2]

RESUMO

A partir do cenário de vigência da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, abreviada como "LGPD") e do registro de ocorrência de diversos incidentes de segurança envolvendo dados pessoais, o presente artigo, a partir de uma abordagem exploratória, procura demonstrar diferentes formas de tutela que podem ser aplicadas diante de tais eventos. Considerando-se que a LGPD adota uma abordagem baseada no risco, buscou-se demonstrar que a tutela preventiva assume papel de especial relevância no ordenamento jurídico. No entanto, em que pese a adoção de medidas preventivas, é possível que incidentes de segurança ocorram e, nesses casos, procura-se apontar que a tutela específica poderá ser utilizada. Por fim, no que diz respeito à tutela ressarcitória em matéria de privacidade e proteção de dados, o presente artigo investiga os desafios de identificação do nexo causal e de demonstração e quantificação do dano, concluindo que meios alternativos de reparação não pecuniária devem ser avaliados nas situações concretas.

Palavras-chave: Incidentes de segurança; Lei Geral de Proteção de Dados; Proteção de dados; Tutela específica; Tutela ressarcitória.

ABSTRACT

Based on the enforcement of the Brazilian General Data Protection Law (Federal Law No. 13,709/2018, abbreviated as "LGPD") and the occurrence of several security incidents involving personal data, this paper, from an exploratory approach, seeks to demonstrate different forms of protection that can be applied in the face of such events. Considering that the LGPD adopts a risk-based approach, we seek to demonstrate that preventive protection plays a particularly important role in the legal system. However, despite the adoption of preventive measures, it is possible that security incidents may

[1] Professor da Faculdade de Direito da Universidade Federal de Juiz de Fora (UFJF) e do Corpo Permanente do PPGD em Direito e Inovação da UFJF. Mestre e Doutor em Direito Civil pela Universidade do Estado do Rio de Janeiro. Lattes: http://lattes.cnpq.br/3282764176353256.

[2] Mestranda em Direito e Inovação no PPGD da Universidade Federal de Juiz de Fora (UFJF). Pós-graduada em Direito Digital pelo CEPED/UERJ. Lattes: http://lattes.cnpq.br/3480301751804187.

occur, and, in these cases, we pointed out that the specific remedy can be used. Finally, regarding the compensation of damages in matters of privacy and data protection, this paper investigates the challenges of identifying the causal nexus and the demonstration and quantification of damage, concluding that alternative means of non-pecuniary compensation must be considered in concrete situations.

Keywords: Brazilian General Data Protection Law; Compensation for damages; Data protection; Security incidents; Specific remedy.

1 INTRODUÇÃO

Os primeiros anos de vigência da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, abreviada como "LGPD") foram marcados pela ocorrência de incidentes de segurança. Fato é que, diariamente, observa-se o surgimento de notícias relatando falhas de segurança e exposição de dados pessoais no setor público e no setor privado, configurando um fato jurídico que justifica estudo aprofundado em razão das inúmeras questões técnicas, sociais e jurídicas, bem como potenciais violações de direitos fundamentais decorrentes de tais eventos.

Para além das preocupações decorrentes das atividades de tratamento de dados[3], o cenário de crescente utilização de dados pessoais coloca em evidência a importância de garantir que as informações sejam tratadas com segurança adequada, de modo a evitar danos patrimoniais e extrapatrimoniais aos titulares de dados[4], seja em perspectiva individual, seja em perspectiva coletiva.

Nesse contexto, a LGPD apresenta disciplina específica para a segurança dos dados pessoais: (i) reconhece a segurança como um dos princípios a serem observados em atividades de tratamento de dados pessoais (artigo 6º, VII); (ii) disciplina a

[3] O tratamento de dados é compreendido como qualquer operação envolvendo dados pessoais. Nesse sentido, o artigo 5º, inciso X, da LGPD define o tratamento como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[4] Titular de dados é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, conforme prevê o artigo 5º, inciso V, da LGPD.

responsabilidade dos agentes de tratamento[5] pelos danos decorrentes de violações de segurança (artigo 44, caput e parágrafo único); (iii) determina a adoção de medidas de segurança (Capítulo VII); e (iv) autoriza e incentiva a formulação de regras de boas práticas e de governança que estabeleçam normas de segurança (artigo 50).

Para além do aspecto jurídico, é importante notar que incidentes de segurança envolvendo dados pessoais podem gerar uma série de consequências para organizações, como quebra da confiança de clientes e investidores, impactos reputacionais, paralisação de operações e custos relacionados ao gerenciamento do evento e do cumprimento do dever de comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados, quando aplicável.

Em síntese, a ocorrência de um incidente de segurança poderá impactar ativos da organização e comprometer suas operações, sendo necessário direcionar esforços de prevenção. Além disso, caso tais eventos ocorram, é essencial que os agentes de tratamento tenham uma estrutura de governança em privacidade e proteção de dados, com rotinas e procedimentos internos formalizados, de modo que seja efetivamente possível implementar medidas de contenção e mitigação de riscos e potenciais danos.

Nesse contexto, o presente trabalho pretende analisar de que modo a tutela preventiva, a tutela específica e a tutela ressarcitória podem ser aplicadas a incidentes de segurança envolvendo dados pessoais. Para tanto, o trabalho será metodologicamente estruturado como uma pesquisa de abordagem exploratória, que busca delinear uma visão geral do problema, tornando-o evidente e compreensível (GIL, 2008).

Referida metodologia de pesquisa é adotada em razão do ainda curto período de vigência da LGPD e, consequentemente, do baixo número de posicionamentos da Autoridade Nacional de Proteção de Dados (ANPD)[6] em casos envolvendo incidentes de

[5] Os agentes de tratamento são os controladores e os operadores (art. 5º, IX, da LGPD). Em síntese, o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, da LGPD), tendo total autonomia para agir. Assim, o controlador atua em uma camada essencialmente estratégica, tomando decisões essenciais para o tratamento de dados. Por outro lado, o operador pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, da LGPD), sendo responsável somente por decisões operacionais e não essenciais.

[6] A Autoridade Nacional de Proteção de Dados é o órgão responsável por fiscalizar o cumprimento da Lei Geral de Proteção de Dados.

segurança. Desse modo, a partir da abordagem exploratória, busca-se uma familiaridade com o problema de pesquisa desenvolvido, com intuito de formulação de hipóteses mais robustas posteriormente.

Para tanto, o tema será desenvolvido a partir de análise das disposições da Lei Geral de Proteção de Dados, com o objetivo de investigar os conceitos delineados pela norma e as obrigações impostas aos agentes de tratamento. Em complementação, analisa-se a minuta de "Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais" divulgada pela ANPD para consulta pública.

Adota-se a estratégia de revisão bibliográfica de trabalhos que abordam a estrutura da disciplina de privacidade e proteção de dados na União Europeia e no Brasil, bem como trabalhos nacionais que abordam especificamente os incidentes de segurança à luz do ordenamento jurídico brasileiro.

Desse modo, a presente investigação pretende, em primeiro lugar, traçar os principais conceitos e referenciais teóricos que orientarão o desenvolvimento dos temas. Posteriormente, o trabalho discutirá possíveis formas de tutela jurídica passíveis de aplicação em situações de incidentes de segurança envolvendo dados pessoais.

2 PROTEÇÃO DE DADOS E INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS

A tutela jurídica de dados pessoais ganha cada vez mais relevância diante do crescente uso de dados pessoais em atividades econômicas. Nesse contexto, diversas normas sobre privacidade e proteção de dados surgiram ao redor do mundo, sendo que, de acordo com a Conferência das Nações Unidas sobre Comércio e Desenvolvimento, 137 de 194 países adotaram legislação sobre este tema.

No Brasil, foi publicada a Lei Geral de Proteção de Dados (Lei n° 13.709/2018, abreviada por "LGPD"), que estabelece regras para o uso lícito de dados pessoais. Acerca da norma, Negri e Korkmaz (2019) apontam que a LGPD é apresentada como imperativo da circulação controlada de dados pessoais, sendo um instrumento para a construção de uma cultura de proteção de dados no Brasil e, consequentemente, gerando mudanças

normativas no ordenamento jurídico nacional.

A relevância do tema é evidenciada na medida em que a proteção de dados passa a ser compreendida como um direito fundamental autônomo, que, inclusive, fornece instrumentos e garantias para o exercício de outros direitos, como a liberdade de expressão e a liberdade de associação. Nesse contexto, destaca-se que, em fevereiro de 2022 foi promulgada a Emenda Constitucional nº 115, consagrando expressamente o direito à proteção de dados como direito fundamental autônomo[7] no ordenamento jurídico brasileiro.

Ao tratar do direito à proteção de dados, é importante estabelecer sua relação com o direito à privacidade, que, em sua dimensão informacional, passa a ser compreendido como o direito de manter controle sobre as próprias informações (RODOTÀ, 2008). Tal compreensão é marcada pela noção de autodeterminação informativa, que, inclusive, é um dos fundamentos da disciplina de proteção de dados no Brasil, conforme artigo 2º, II, da LGPD, sendo concretizada pela implementação de instrumentos e práticas de *accountability* que assegurem o controle informacional por parte dos indivíduos.

A relação entre controle informacional e incidentes de segurança envolvendo dados pessoais é relevante porque incidentes de segurança são eventos marcados pela ocorrência de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados pessoais que, consequentemente, representam uma perda de controle informacional. Por tal razão, incidentes de segurança são situações que merecem atenção particular e ensejam a aplicação de proteções especiais, uma vez que, conforme apontava Doneda (2019), a disciplina da proteção de dados é marcada pela possibilidade de utilização combinada de formas de tutela jurídica.

É importante notar que nem todos os incidentes de segurança envolvem dados pessoais. Os dados pessoais[8] são informações que identificam uma pessoa natural

[7] Vale ressaltar que, no Brasil, em âmbito jurisprudencial o direito à proteção de dados já era reconhecido como direito fundamental autônomo, conforme decisão proferida pelo Supremo Tribunal Federal em sede da ADI 6.387 MC-Ref/DF, julgamento em 6 e 7.mai.2020.

[8] Em relação ao conceito de dados pessoais, destaca-se que alguns autores, como Pierre Catala e Massimo Durante, adotam o entendimento de que há uma distinção entre dado e informação na medida em que a informação seria alcançada apenas quando os dados passam por um processo de interpretação, ou seja, quando se atribui algum significado a eles. Por outro lado, para fins do presente trabalho, os termos

diretamente – como nome, CPF, RG e demais vínculos direitos – ou a tornam indiretamente identificável – por exemplo, número de telefone, geolocalização, número do cartão de crédito e outros vínculos indiretos. Ocorre que é possível que um incidente envolva somente informações que não são enquadradas nesta categoria jurídica, por exemplo, dados de pessoas jurídicas, informações referentes a segredo de negócio etc. Nesse contexto, faz-se necessário esclarecer que o presente trabalho busca investigar formas de tutela jurídica a serem aplicadas a eventos que efetivamente envolvam dados pessoais e atraiam a aplicação das disposições da LGPD.

A LGPD procurou endereçar em diversos dispositivos a importância da segurança das informações pessoais, mas não trouxe uma definição específica para conceituar o que seria um "incidente de segurança da informação envolvendo dados pessoais". Tal definição poderia ser extraída do princípio da segurança, previsto no artigo 6º, VII, da LGPD, segundo o qual um incidente de segurança seria quaisquer situações de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Na mesma direção, a minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais divulgada pela ANPD para consulta pública conceitua o incidente de segurança com dados pessoais como qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais.

Verifica-se que referido dispositivo é fundamentado pelos atributos da segurança da informação, quais sejam: (i) confidencialidade, isto é, garantia de que as informações sejam acessadas somente por aqueles que são devidamente autorizados; (ii) integridade, baseada na veracidade das informações, evitando perdas e alterações; e (iii) disponibilidade, ou seja, a garantia de que as informações estarão acessíveis às pessoas autorizadas. A definição trazida pela minuta divulgada pela ANPD considera também a autenticidade como uma das propriedades da segurança da informação, embora este não

"dados" e "informações" são compreendidos como sinônimos, uma vez que não se analisa atividades de tratamento e/ou processos decisórios que atribuem significado aos dados pessoais, mas tão somente a ocorrência de incidentes de segurança.

seja um elemento comumente reconhecido como atributo da segurança da informação. Menke e Goulart (2020) apontam, ainda, um quarto elemento: a resiliência, caracterizada pela capacidade de recomposição das estruturas e funcionalidades essenciais após a ocorrência de um evento adverso. Para fins de comparação, ressalta-se que, no âmbito da União Europeia, o Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*, abreviado por "GDPR"), ao dispor sobre a segurança no tratamento de dados pessoais, elenca a resiliência como um dos atributos das medidas de segurança, ao lado da confidencialidade, da integridade e da disponibilidade.

Para Menke e Goulart (2020), os atributos de confidencialidade, integridade, disponibilidade e resiliência levam em consideração os conceitos de vulnerabilidade, ameaça, incidente e controle. A vulnerabilidade é caracterizada por ser uma fraqueza que atinge sistemas, ambientes, processos, protocolos etc., enquanto a ameaça é uma situação que explora vulnerabilidades e pode causar um evento de segurança classificado como incidente de segurança. Por fim, os controles são as medidas adotadas para impedir que um incidente ocorra ou para diminuir a probabilidade de sua ocorrência.

Ainda em relação à definição de incidente de segurança, a Autoridade Nacional de Proteção de Dados (ANPD), em suas orientações sobre o tema[9], esclarece que tal evento pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda indevidas ou acessos não autorizados a dados pessoais, independentemente do meio em que estão armazenados. Além disso, a ANPD destaca que a mera existência de uma vulnerabilidade em um sistema de informação não constitui um incidente de segurança, porém, a exploração da referida vulnerabilidade pode resultar em um incidente.

Observa-se que a definição adotada pela ANPD acertadamente restringe os incidentes somente aos eventos adversos confirmados, ou seja, a mera suspeita não é

[9] A ANPD publicou página de orientações sobre a comunicação de incidentes de segurança, porém, ressalta-se que tais orientações são recomendações e não se confundem com a regulamentação da comunicação de incidentes e especificação do prazo de notificação, que está prevista para a Fase 1 da Agenda Regulatória para o biênio 2023-2024. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de incidentes de segurança. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 07 mar. 2023.

categorizada como incidente de segurança com dados pessoais. Entende-se que tal restrição conceitual é adequada pois, caso contrário, o escopo da definição seria demasiadamente amplo, podendo, inclusive, ensejar comunicações desnecessárias à ANPD e aos titulares de dados.

Desse modo, a partir da definição de incidentes de segurança envolvendo dados pessoais e seus respectivos aspectos, buscar-se-á refletir acerca do papel da segurança da LGPD e, posteriormente, debater acerca das possíveis formas de tutela aplicáveis em tais situações. Para tanto, na próxima seção, são abordados os principais dispositivos para compreensão das regras traçadas pela LGPD em relação à segurança dos dados pessoais.

3 SEGURANÇA NA LEI GERAL DE PROTEÇÃO DE DADOS

A compreensão de que incidentes de segurança envolvendo dados pessoais merecem tutela jurídica especial por parte do ordenamento também passa pela análise dos dispositivos previstos na LGPD. Além do princípio da segurança, comentado anteriormente, a LGPD estabelece que agentes de tratamento ou demais entidades que venham a intervir no tratamento de dados pessoais devem garantir a segurança de tais informações, mesmo após o término do tratamento (*security by design*), conforme se extrai do artigo 47 da referida norma. Na mesma direção, o artigo 49 da LGPD estabelece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança, os princípios gerais previstos na norma e às demais normas regulamentares.

Vale destacar que, no âmbito da União Europeia, o *European Data Protection Board* (EDPB)[10], ao tratar da metodologia de *Privacy by Design*, esclarece que a segurança dos dados pessoais requer medidas adequadas destinadas a prevenir e gerenciar incidentes de violação de dados, bem como garantir a boa execução das atividades de

[10] O *European Data Protection Board* é um órgão independente da União Europeia cujo objetivo é garantir a aplicação do *General Data Protection Regulation* (GDPR), regulamento europeu que prevê regras para o uso de dados pessoais.

tratamento, o cumprimento dos demais princípios e o exercício efetivo dos direitos dos titulares.

O artigo 44, parágrafo único, da LGPD, estabelece que o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no artigo 46, der causa aos danos decorrentes da violação da segurança dos dados, responderá por sua conduta. Nesse sentido, Bioni e Dias (2020) apontam que a LGPD estabelece duas hipóteses para a configuração da responsabilidade civil dos agentes de tratamento de dados: a "violação à legislação de proteção de dados pessoais" e a "violação da segurança dos dados".

Tais hipóteses devem ser analisadas em conjunto à noção de tratamento irregular, compreendido como a situação na qual (i) o tratamento de dados pessoais deixa de observar a legislação; ou (ii) tratamento de dados pessoais não fornece a segurança que o titular pode esperar, conforme previsto no caput artigo 44 da LGPD. Nesse contexto, Bioni e Dias (2020) questionam se, em caso de violação da segurança dos dados, o agente seria responsabilizado (i) se não adotasse as medidas de segurança aptas a proteger os dados pessoais; ou (ii) se o tratamento não fornecesse a segurança que o titular dele pode esperar. Diante do questionamento apresentado, os autores entendem que a hipótese de adoção de medidas aptas é demasiadamente ampla e, por isso, apontam que a análise da segurança esperada pelo titular seria mais frutífera.

Embora Bioni e Dias (2020) entendam que a irregularidade do tratamento deve ser analisada com base nas legítimas expectativas de segurança que um titular médio pode esperar do tratamento de dados em questão, entende-se que é necessário considerar que a análise a partir da perspectiva do "titular médio" ainda ensejaria elevado nível de subjetividade – especialmente considerando que o conhecimento sobre padrões técnicos de segurança é essencialmente restrito aos profissionais que atuam na área – e, até mesmo, poderia contrariar parâmetros e boas práticas de segurança da informação.

Considerando tais argumentos, entende-se que a violação da segurança dos dados deve ser analisada a partir das justificativas técnicas que fundamentaram a adoção das medidas de segurança analisadas no caso concreto, isto é, quais orientações, boas práticas e parâmetros foram considerados ao estabelecer determinado nível de segurança (por

exemplo, natureza e volume de dados tratados, risco do tratamento, titulares de dados afetados etc.). Posteriormente, a partir da definição das medidas de segurança por parte do agente de tratamento, é possível construir a visão de confiança esperada pelo titular por meio do fornecimento de informações, advertências e instruções qualificadas, conforme apontam Menke e Goulart (2020).

Ainda que a LGPD tenha tratado das medidas de segurança e padrões técnicos de forma neutra e aberta, é importante que os agentes de tratamento estejam implementando tais ações conforme as operações que realizam. Palhares, Prado e Vidigal (2021) ressaltam que a liberdade de determinação de quais medidas de segurança serão adotadas não significa que padrões de segurança insuficiente serão legitimados pela LGPD, na verdade, tal abertura legislativa tem a função de assegurar que as medidas adotadas sejam compatíveis aos riscos presentes em cada contexto específico de tratamento de dados pessoais.

Inclusive, a ANPD poderá dispor sobre padrões técnicos mínimos, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia. Além disso, no que diz respeito ao tratamento de dados pessoais que ocorre por meio da Internet, haverá aplicação do Decreto n° 8.771/2016, que regulamenta o Marco Civil da Internet (Lei nº 12.965/2014). O artigo 13 do referido Decreto apresenta diretrizes sobre padrões de segurança, que devem ser observadas por provedores de conexão e de aplicações durante a guarda, armazenamento e tratamento de dados pessoais e comunicações privadas.

Ressalta-se que o Decreto n° 8.771/2016 já apresentava relevante preocupação com o acesso às informações e, consequentemente, com a construção da expectativa de segurança por parte do usuário, determinando que as informações sobre os padrões de segurança adotados pelos provedores de aplicação e provedores de conexão devem ser divulgadas de forma clara e acessível a qualquer interessado, preferencialmente por meio de seus sítios na internet, respeitado o direito de confidencialidade quanto aos segredos empresariais.

Em síntese, para fins de avaliação da irregularidade de determinada atividade de tratamento de dados pessoais, entende-se que é necessário avaliar, à luz do caso concreto,

as medidas de segurança adotadas e as respectivas justificativas técnicas para adoção, de modo a avaliar se tais medidas, de fato, poderiam ser consideradas aptas naquele contexto específico. Diante da definição das medidas de segurança, o agente de tratamento poderá contribuir para a construção da expectativa de segurança dos titulares por meio da implementação de medidas de transparência e disponibilização de informações sobre o tema.

Outra disposição relevante é a previsão de que o controlador deverá comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, conforme artigo 48 da LGPD. Observa-se que o dever de notificação previsto pela LGPD busca, de um lado, assegurar que a ANPD tenha ciência do ocorrido e possa atuar junto aos agentes de tratamento, determinando a adoção de medidas de contenção e providências que auxiliem na reversão ou mitigação dos efeitos decorrentes do incidente. Por outro lado, a comunicação aos titulares concretiza os preceitos de transparência e possibilita que os afetados adotem práticas mitigatórias e estejam atentos às possíveis consequências do incidente (por exemplo, tentativas de fraudes e golpes).

É importante notar que nem todos os incidentes de segurança envolvendo dados pessoais deverão ser notificados, mas somente aqueles que tenham o potencial de causar risco ou dano relevante aos titulares. No entanto, a LGPD não prevê critérios e metodologia para fins de avaliação do risco de incidentes de segurança envolvendo dados pessoais. Diante desse cenário, a ANPD iniciou, em 2021, o processo de regulamentação sobre incidentes de segurança, conforme prevê o artigo 48 da LGPD e como parte de sua agenda regulatória, aprovada pela Portaria nº 21 de 27 de janeiro de 2021.

Nesse contexto, a minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais divulgada pela ANPD para consulta pública apresenta critérios para avaliação de risco ou dano relevante, lista as informações que controladores devem apresentar à ANPD e aos titulares e define o prazo razoável para notificação do evento à ANPD e aos titulares. Ressalta-se que, até o presente momento, em que pese a divulgação da minuta do Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais para consulta pública, o processo de regulamentação ainda não foi

concluído. No entanto, ainda que não haja regulamentação do tema via resolução administrativa, a ANPD fornece aos agentes de tratamento uma página de orientações acerca do tema, caracterizadas como recomendações e, portanto, não vinculantes e obrigatórias.

A partir das orientações da ANPD, é possível extrair os seguintes fatores - não cumulativos - de avaliação de criticidade do incidente: (i) envolvimento de dados pessoais sensíveis, nos termos do artigo 5º, II, da LGPD; (ii) envolvimento de dados pessoais de indivíduos em situação de vulnerabilidade, como crianças, adolescentes e idosos; (iii) potencial de ocasionar danos materiais/morais aos indivíduos afetados; (iv) volume significativo de dados pessoais; (v) volume significativo de titulares afetados; (vi) intenções maliciosas da pessoa responsável pela concretização do evento; e (vii) facilidade de identificação dos indivíduos afetados pelo evento.

Além dos critérios elencados pela ANPD, destaca-se a existência de diversas metodologias para avaliação de criticidade de incidentes, desenvolvidas, por exemplo, por organizações do setor privado. Nesse sentido, ressalta-se a metodologia globalmente reconhecida e desenvolvida pela *European Union Agency for Network and Information Security* (ENISA), a qual considera os seguintes fatores: (i) contexto, compreendido como o elemento que analisa a natureza dos dados pessoais envolvidos no evento; (ii) facilidade de identificação, isto é, a probabilidade de os dados pessoais envolvidos no evento levarem à identificação dos indivíduos afetados; e (iii) circunstâncias do incidente, para fins de avaliação de eventual intenção maliciosa de exposição/tratamento inadequado dos dados pessoais envolvidos no evento.

No que diz respeito ao prazo para comunicação, a LGPD prevê que esta deverá ser realizada em "prazo razoável". A ANPD, em caráter de recomendação, orienta que, após a ciência do evento adverso e havendo risco relevante, a comunicação seja feita com a maior brevidade possível, indicando o prazo de 2 dias úteis, contados da data do conhecimento do incidente, prazo inspirado no Decreto nº 9936/2019, que regulamenta a Lei do Cadastro Positivo (Lei nº 12.414/2011).

Por sua vez, a minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais divulgada pela ANPD para consulta pública prevê que a

comunicação do incidente à ANPD e aos titulares deverá ser realizada no prazo de três dias úteis, contados do conhecimento do incidente de segurança. Possivelmente, referido prazo tem como referência o *General Data Protection Regulation* (GDPR) – legislação de proteção de dados vigente no âmbito da União Europeia – que prevê o prazo de 72 horas.

Além disso, é interessante notar que, à luz da LGPD, incidentes de segurança podem desencadear uma série de violações às normas de proteção de dados, indo além das disposições relacionadas à comunicação do evento aos titulares e à ANPD. A título de exemplificação, incidentes que acarretem alteração de dados pessoais ensejam violação ao princípio da qualidade (artigo 6º, V, da LGPD), assim como incidentes que tenham como consequência a perda de dados pessoais podem inviabilizar o atendimento de direitos exercidos pelos titulares (artigo 18, da LGPD).

Nessa direção, o *European Data Protection Board* aponta que as violações de dados são problemas em si, mas também podem ser sintomas de um regime de segurança de dados vulnerável e possivelmente insuficiente. Portanto, a implementação de medidas de segurança e padrões técnicos adequados durante todo o ciclo de vida dos dados pessoais é essencial, de modo que a segurança deve ser um fator considerado antes mesmo do início das atividades de tratamento.

Desse modo, constata-se que, sob a perspectiva da LGPD, há a exigência de adoção de medidas de segurança técnicas e administrativas, o que pressupõe uma estrutura de governança em privacidade e proteção de dados. A partir deste contexto, questiona-se quais seriam as possíveis formas de tutela jurídica aplicáveis a incidentes de segurança envolvendo dados pessoais.

4 TUTELA PREVENTIVA: DIÁLOGOS ENTRE PREVENÇÃO, PRECAUÇÃO E ABORDAGEM BASEADA NO RISCO

A LGPD estabelece o princípio da prevenção (artigo 6º, VIII), segundo o qual é necessário observar a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Nesse sentido, a partir de uma interpretação sistemática

da LGPD, é possível compreender que o agente de tratamento deverá agir com cautela e adotar as medidas de segurança aptas a prevenir a ocorrência de incidentes de segurança.

Para além da prevenção, expressamente prevista pela LGPD, o princípio da precaução também pode ser observado no ordenamento jurídico brasileiro. Bioni e Luciano (2019) apontam que o princípio da precaução surge em decorrência da insuficiência dos métodos tradicionais de regulação de risco diante de incertezas. Tal princípio originou-se na década de 1970 a partir de iniciativas de proteção ambiental que buscavam evitar danos ambientais marcados pela incerteza e indeterminação do tipo de dano.

No âmbito da privacidade e da proteção de dados, a aplicação do princípio da precaução poderá contribuir para a consolidação de uma abordagem baseada no risco (*risk based approach*). Tal abordagem é comumente adotada por normas de proteção de dados, inclusive pela LGPD, e, assim como o princípio da precaução, está relacionada a condutas baseadas em prudência e transparência. Nesse sentido, a partir de uma abordagem baseada no risco, os agentes de tratamento devem implementar rotinas de avaliação de riscos em atividades de tratamento de dados pessoais e endereçar as medidas para mitigação dos riscos identificados.

Costa (2012) aponta que, pelo princípio da precaução, em situações nas quais existam ameaças de danos graves ou irreversíveis, mesmo que não haja plena certeza científica, é necessário tomar medidas de proteção sem esperar que esses riscos se tornem plenamente aparentes. Nessa direção, o autor destaca que a avaliação de risco e o princípio da precaução são instrumentos que caminham juntos, pois determinam conjuntamente a atribuição da avaliação dos riscos e do custo dos danos.

Em relação à matéria de privacidade e proteção de dados, o princípio da precaução apresenta-se como uma garantia contra riscos potenciais que, no atual momento do tratamento de dados pessoais, podem não ser identificados. Para Costa (2012) o princípio da precaução beneficia a proteção da privacidade na medida em que coloca em evidência os valores normativos de prudência e transparência, criando para os agentes de tratamento um dever de cuidado. Conjuntamente, prudência e precaução implicam que as atividades devem ser realizadas de forma a evitar que seus potenciais efeitos prejudiciais atinjam

outras pessoas, possibilitando a realização do tratamento de dados pessoais com segurança.

Considerando-se especificamente os incidentes de segurança da informação envolvendo dados pessoais para uma leitura sob a ótica do princípio da precaução, verifica-se que tais eventos são marcados pela incerteza técnica de sua ocorrência, porém, isso não elimina a necessidade de implementar medidas que possam prevenir a ocorrência de incidentes e, consequentemente, evitar potenciais danos aos titulares de dados.

Nessa direção, ressalta-se o artigo 47 da LGPD, que estabelece o dever de garantir a segurança da informação em relação aos dados pessoais, mesmo após o término do tratamento. Conforme mencionado anteriormente, esta abordagem – também denominada *security by design* – exige que os agentes de tratamento considerem os requisitos de segurança durante todo o ciclo de vida das informações, isto é, desde o momento inicial de concepção da atividade até o momento de encerramento e eliminação dos dados pessoais envolvidos, prevenindo a ocorrência de danos.

Entende-se que os agentes de tratamento devem adotar medidas, rotinas e práticas que contribuam para a efetivação do princípio da prevenção e concretizem a tutela preventiva em matéria de privacidade e proteção de dados pessoais. O desenvolvimento e a efetiva implementação de normas e procedimentos internos (como a política de segurança da informação) que estabeleçam medidas e padrões de segurança a serem adotados, regras para uso de sistemas, acesso a instalações e equipamentos também é essencial para incorporar a tutela preventiva nas rotinas de uma organização.

Além disso, é necessário assegurar que eventuais terceiros envolvidos em atividades de tratamento, como prestadores de serviços e parceiros, adotem padrões de segurança adequados. Por tal razão, a gestão de terceiros deve ser incorporada como uma forma de tutela preventiva, evitando que agentes de tratamento que não adotam medidas de segurança adequadas sejam engajados nas cadeias de atividades que envolvem dados pessoais.

Nessa direção, Menke e Goulart (2020) apontam que a segurança é aplicada aos sistemas e estruturas utilizadas no tratamento de dados (medidas técnicas) e ao ambiente geral do agente de tratamento (medidas organizativas), de modo que a adoção de medidas

técnicas não será suficiente se não for complementada por rotinas essencialmente organizacionais, como os treinamentos e as políticas internas. Portanto, a atuação preventiva do agente de tratamento é concretizada não só a partir de padrões técnicos, mas também por meio de uma estrutura de governança sólida.

5 TUTELA ESPECÍFICA: O INCIDENTE DE SEGURANÇA COMO MOMENTO PATOLÓGICO DA RELAÇÃO CONTRATUAL

Ainda que os agentes de tratamento atuem preventivamente, a ocorrência de incidentes de segurança é possível. Inclusive, por vezes, tais eventos estão relacionados a elementos externos, como a atuação de outros agentes na cadeia de tratamento de dados pessoais. Assim, para além das rotinas e medidas que buscam prevenir a ocorrência de incidentes de segurança, também é necessário analisar eventuais cláusulas contratuais relacionadas à atividade de tratamento de dados pessoais.

Um contrato que define direitos e deveres relacionados ao tratamento de dados pessoais poderá prever cláusulas que disponham sobre a adoção de medidas de segurança e ações a serem tomadas em caso de incidentes de segurança. Por exemplo, no caso de uma relação entre controlador e operador, é possível estipular cláusula contratual para que, em caso de indícios de ocorrência de incidente de segurança, o operador notifique o controlador acerca da situação. Por outro lado, no caso de relações entre controladores, cita-se a possibilidade de previsão de cláusula contratual que estabelece o dever de comunicação acerca da suspeita de incidente de segurança, bem como cláusulas sobre tomada de decisão conjunta acerca das medidas necessárias para contenção e prestação de auxílio mútuo.

Diante do contexto de definição de obrigações contratuais, ressalta-se que Negri (2021) aponta que o caráter dinâmico da relação obrigacional coloca em evidência o fato de que o adimplemento está relacionado a execução da prestação em toda sua complexidade, incluindo os deveres anexos inerentes à complexidade intra-obrigacional. Em síntese, é importante notar que o adimplemento não mais se confunde com a mera realização da prestação principal, podendo ocorrer também em razão de deveres anexos.

Ao trazer esta discussão para o âmbito da privacidade e da proteção de dados pessoais, nota-se que é possível que a prestação principal relacionada a um tratamento de dados seja cumprida, mas o dever de segurança – que visa impedir a ocorrência de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão – seja descumprido. Em cenários como este narrado, ainda que a prestação principal relacionada ao tratamento de dados pessoais tenha sido cumprida, o descumprimento do dever anexo de segurança caracteriza inadimplemento.

Diante da possibilidade de previsão de cláusulas contratuais acerca da segurança dos dados em relações envolvendo atividades de dados pessoais, faz-se necessário refletir sobre as consequências de eventual inadimplemento, uma vez que o incidente de segurança poderá ser compreendido como um momento patológico da relação contratual se originado pelo descumprimento dos deveres de segurança estabelecidos pelas partes. Nesse contexto, o ordenamento jurídico brasileiro prevê diferentes remédios passíveis de aplicação em situações envolvendo inadimplemento.

O Artigo 389 do Código Civil estabelece que, caso a obrigação não seja cumprida, o devedor responderá por perdas e danos, mais juros e atualização monetária segundo índices oficiais regularmente estabelecidos, e honorários de advogado. No entanto, ressalta-se que tal dispositivo não deve ser interpretado no sentido de que a tutela ressarcitória seria o único ou o principal remédio para casos de inadimplemento contratual. Na verdade, verifica-se que a tutela ressarcitória é subsidiária, enquanto o principal remédio disponibilizado pelo ordenamento jurídico é o cumprimento específico da obrigação, ou seja, o cumprimento daquilo que foi contratualmente prometido.

Nesse sentido, o artigo 499 do Código de Processo Civil determina que a obrigação somente será convertida em perdas e danos se o autor o requerer ou se impossível a tutela específica ou a obtenção de tutela pelo resultado prático equivalente. Na mesma direção, o parágrafo primeiro do artigo 84 do Código de Defesa do Consumidor estabelece que a conversão da obrigação em perdas e danos somente será admissível por opção do autor ou em caso de impossibilidade de tutela específica ou de obtenção do resultado prático correspondente.

Verifica-se, portanto, que a tutela específica é o principal remédio para a promoção da tutela satisfativa da obrigação em concreto, enquanto a tutela ressarcitória assume caráter subsidiário ou complementar. Tepedino (2012) destaca que deve ser atribuído ao credor exatamente aquilo que lhe foi estabelecido contratualmente, ou seja, a prioridade é a execução *in natura* e, caso seja verificada a impossibilidade de execução específica, busca-se alcançar o resultado prático equivalente e, somente em último caso, a reparação por perdas e danos.

Inclusive, mesmo no caso da obrigação de fazer (por exemplo, obrigação de implementar determinadas medidas de segurança durante o tratamento de dados pessoais), a tutela obrigacional não está atada à tutela ressarcitória. Fato é que, atualmente, o ordenamento jurídico conta com mecanismos de execução indireta para persuadir o agente inadimplente a realizar o comportamento pactuado.

Nesse sentido, o artigo 536 do Código de Processo Civil estabelece que, no cumprimento de sentença que reconheça a exigibilidade de obrigação de fazer ou de não fazer, o juiz poderá, de ofício ou a requerimento, determinar, entre outras medidas, a imposição de multa, a busca e apreensão, a remoção de pessoas e coisas, o desfazimento de obras e o impedimento de atividade nociva, podendo, caso necessário, requisitar o auxílio de força policial.

É inegável que, a depender do caso concreto, a execução específica da obrigação restará prejudicada, por exemplo, quando se verificar em concreto a impossibilidade da prestação. A título de exemplificação, é possível imaginar cenário no qual há obrigação de devolução dos dados pessoais envolvidos na atividade, porém, tais dados foram apagados em razão da ocorrência de incidente de segurança e não há um *backup*. Neste exemplo, observa-se a impossibilidade de execução específica da obrigação de devolução dos dados pessoais em razão da perda de disponibilidade e integralidade, gerada pelo incidente de segurança.

Desse modo, nos casos de inadimplemento absoluto, além da execução pelo equivalente, a parte lesada pelo inadimplemento possui o direito potestativo de resolver o contrato, havendo a extinção da relação obrigacional, cabendo em qualquer dos casos, indenização por perdas e danos, conforme artigo 475 do Código Civil. Ressalta-se que a

qualificação do inadimplemento como absoluto ou relativo não é uma escolha das partes, trata-se, na verdade, de uma qualificação que decorre do fato objetivo de a prestação ter ou não se tornado inútil à parte lesada pelo inadimplemento, ou ter ou não se impossibilitado para a parte inadimplente.

Tratando-se do tema de privacidade e proteção de dados pessoais, é possível que – em relações contratuais – um agente de tratamento envolvido na atividade ou o próprio titular de dados peça a execução específica de cláusulas contratuais, com destaque para aquelas que envolvem a adoção de medidas de segurança adequadas, o dever de comunicação sobre incidentes de segurança envolvendo dados pessoais e a prestação de auxílio mútuo diante da ocorrência de tais eventos, conforme mencionado anteriormente.

Especificamente em relação à tutela coletiva, Zanatta e Souza (2019) apontam que, a partir da interpretação conjunta da Lei da Ação Civil Pública (Lei nº 7.347/1985), do Código de Defesa do Consumidor (Lei nº 8.078/1990) e da LGPD, observa-se que a ação civil pública poderá ser proposta não só para a reparação de danos, mas também para a obtenção da tutela específica, ou seja, aplicando-se também uma tutela inibitória coletiva. No caso de situações envolvendo somente a tutela individual da proteção de dados, entende-se que o racional de possibilidade de obtenção da tutela específica também seria aplicável.

Na mesma direção e, especificamente no que diz respeito aos direitos da personalidade, observa-se o enunciado 140 na III Jornada de Direito Civil, promovida pelo Centro de Estudos Judiciários do Conselho da Justiça Federal, em 2004, segundo o qual a primeira parte do artigo 12 do Código Civil refere-se às técnicas de tutela específica, aplicáveis de ofício, enunciadas no artigo 461 do Código de Processo Civil (nesse caso, faz-se referência ao CPC de 1973), devendo ser interpretada com resultado extensivo.

Desse modo, verifica-se que a tutela específica poderá estar presente em situações individuais ou coletivas, envolvendo relações contratuais travadas entre agentes de tratamento e entre agentes de tratamento e titulares de dados. Em relação aos incidentes de segurança envolvendo dados pessoais, é possível vislumbrar – exemplificativamente, uma vez que a tutela específica varia a depender das peculiaridades do caso concreto –

obrigações como (i) a adoção de medidas voltadas para a contenção do incidente; (ii) atividades de monitoramento e varredura para remoção de bancos de dados expostos na *web* e na *deep web*; (iii) a criação de página e canal de comunicação específico para orientações acerca do incidente; (iv) o dever de comunicação previsto pelo artigo 48 da LGPD etc.

O direito privado, ao priorizar a tutela específica das obrigações, deixou de lado a compreensão de que obrigações de fazer e não fazer seriam inexequíveis. Ainda que não haja previsão expressa de mecanismos típicos de tutela específica, esta assume o papel de principal remédio para o inadimplemento contratual. Esse é um cenário relevante para relações contratuais envolvendo o tratamento de dados pessoais, especialmente diante de cláusulas que estabeleçam deveres anexos de segurança.

5 TUTELA RESSARCITÓRIA: SUBSIDIARIEDADE E POSSIBILIDADES DE REPARAÇÃO NÃO PECUNIÁRIA

Conforme se procurou demonstrar, a tutela ressarcitória, concretizada a partir da verificação das perdas e danos e consequente indenização, assume caráter subsidiário no ordenamento jurídico brasileiro. Em que pese a possibilidade de tutelar a privacidade e a proteção de dados por meio da responsabilidade civil, é necessário reconhecer que a tutela ressarcitória não deve ser o principal instrumento de tutela, privilegiando-se uma atuação específica em prol da pessoa humana.

Nesse sentido, de acordo com Doneda (2019), a tutela baseada na responsabilidade civil oferece uma visão predominantemente patrimonialista do problema. Desse modo, entende-se que a lesão à personalidade humana, por estar relacionada aos interesses existenciais, não é compatível com a mera recondução do prejudicado ao estado anterior.

Em que pese a subsidiariedade da tutela ressarcitória, sua análise é importante e assume especial relevância em situações nas quais se verifica a impossibilidade da tutela específica. Nesse sentido, a LGPD estabelece que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano

patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo, nos termos do artigo 42, da LGPD.

Desse modo, considerando-se os elementos da responsabilidade civil, é necessário que, no caso concreto, seja verificada a existência de um dano. A demonstração do dano é o primeiro desafio a ser enfrentado para responsabilização em matéria de privacidade e proteção de dados. Nessa direção, Citron e Solove (2020) apontam que os tribunais reconhecem impactos menores porque são tangíveis, mas deixam de reconhecer problemas graves relacionados à privacidade porque, geralmente, são marcados pela intangibilidade.

Em segundo lugar, Citron e Solove (2020) chamam atenção para o fato de que, por vezes, os danos à privacidade são pequenos, mas numerosos. Tais danos podem atingir o mesmo indivíduo diversas vezes, mas em razão da conduta de diferentes atores e, consequentemente, se tornarem significativamente mais prejudiciais. Por outro lado, também é possível que uma organização cause um dano pequeno, mas em escala muito grande, atingindo diversos indivíduos, sendo que, nesses casos, do ponto de vista de cada indivíduo, o dano é mínimo, mas há uma agravação pela agregação.

Citron e Solove (2020) esclarecem, ainda, que o dano pode não ser totalmente reconhecível por estar na forma de um risco futuro de lesões, que podem ser variadas, ou seja, o dano poderá vir a se manifestar somente no futuro. Por fim, os autores destacam que o desafio relacionado ao fato de que os danos à privacidade geralmente envolvem não apenas os interesses individuais, mas também interesses coletivos.

Para além dos desafios relacionados à demonstração do dano, nota-se que a aferição do nexo causal também poderá ser particularmente complexa. Por exemplo, em relação aos incidentes de segurança, Schreiber (2021) ressalta que, por vezes, um vazamento de dados pessoais envolverá sucessivas transferências ou apropriações de dados, de modo que a fonte originária de dados pessoais expostos indevidamente nem sempre é passível de identificação.

Desse modo, em relação aos incidentes de segurança envolvendo dados pessoais, é importante que, no caso concreto, seja possível demonstrar (i) a existência de dano gerado pelo evento; e (ii) o nexo de causalidade entre o dano sofrido e o incidente de

segurança. Nesse sentido, o parágrafo único do artigo 44 da LGPD estabelece que o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no artigo 46, der causa aos danos decorrentes da violação da segurança dos dados, responderá por tais danos.

Acerca deste tema, em que pese a relevância da reparação civil, é importante notar que o cenário de banalização das condenações – no qual é possível verificar diminuição de valores, confusões entre critérios patrimoniais e existenciais – demanda reflexões acerca da despatrimonialização da reparação, conforme ensina Konder (2021), isto é, meios não pecuniários que podem ser aplicados para maximizar a promoção de interesses existenciais.

Nesse sentido, destaca-se que o Supremo Tribunal Federal já entendeu que os mecanismos de reparação *in natura* permitem a tutela mais efetiva dos direitos fundamentais, sendo plenamente compatíveis com a Constituição Federal, que assegura o direito à indenização pelos danos morais, mas não elege um meio específico para efetivação do ressarcimento, ou seja, nem sempre é necessário realizar a reparação pecuniária, havendo margem para discussão sobre métodos de reparação não pecuniária.

O enunciado 589 da VII Jornada de Direito Civil, realizada pelo Conselho da Justiça Federal, ao tratar da interpretação da cláusula geral de responsabilidade civil prevista no caput do artigo 927 do Código Civil, estabelece que a compensação pecuniária não é o único modo de reparar o dano extrapatrimonial, sendo admitida a reparação *in natura*, na forma de retratação pública ou outro meio.

Como bem sintetiza Leonardo Fajngold (2021), a reparação não pecuniária pode ser compreendida a partir das situações nas quais a reparação de um dano extrapatrimonial não consiste na transferência de dinheiro à vítima com o objetivo de incremento do seu capital. O autor destaca que a lógica não pecuniária não significa que os mecanismos a serem empregados não possuem expressão patrimonial. Na verdade, nota-se que a implementação de mecanismos de reparação não pecuniária, em regra, gera custos pecuniários ao ofensor.

No âmbito da privacidade e da proteção de dados pessoais, observa-se que incidentes de segurança podem vir a causar danos de natureza patrimonial (por exemplo,

perdas financeiras, perda de oportunidades e demais situações passíveis de valoração econômica) ou extrapatrimonial, como danos à reputação, discriminação e restrições de liberdades civis.

O dano extrapatrimonial decorrente de um incidente de segurança envolvendo dados pessoais representa a lesão a um interesse jurídico referente à personalidade humana. Por exemplo, Citron e Solove (2020) apontam que as violações de privacidade podem causar danos ao inibir as pessoas de exercerem a liberdade de expressão e de se envolverem em atividades políticas, religiosas e associativas. Os autores ressaltam, inclusive, que tais violações podem ser especialmente impactantes para mulheres, minorias e grupos marginalizados, dada a vigilância desproporcional que recai sobre esses grupos.

Em tais situações, o movimento de deslocamento do foco do direito privado para a pessoa, coloca em evidência a necessidade de adotar formas de tutela que possibilitem a máxima promoção dos interesses existenciais. Como esclarece Fajngold (2021), uma forma de reparação não pecuniária pode ter maior aptidão reparatória do que o mero recebimento de uma determinada quantia.

Desse modo, entende-se que o debate sobre a aplicação de mecanismos de reparação não pecuniária diante de danos gerados por incidentes de segurança envolvendo dados pessoais é essencial. Por vezes, diante da perda de confidencialidade, integridade ou disponibilidade de dados pessoais, a tutela *in natura* se apresentará como meio que possibilita a maior promoção dos interesses existenciais dos titulares envolvidos em determinado incidente.

Portanto, em que pese a existência de diversos mecanismos voltados para a tutela preventiva e a possibilidade de exigência de tutela específica, a tutela ressarcitória também representa papel relevante para a efetivação dos preceitos da lei. Especificamente no campo da reparação de danos extrapatrimoniais, caberá refletir acerca das possibilidades de reparação não pecuniária diante de incidentes de segurança envolvendo dados pessoais e empreender esforços para assegurar a adequada tutela de interesses existenciais.

6 CONSIDERAÇÕES FINAIS

O crescente uso de tecnologias e o aumento do fluxo informacional são fatores que impulsionam o tratamento de dados pessoais. Evidentemente, na sociedade de informação, as relações evoluíram e são travadas em ambientes digitais cada vez mais complexos e dinâmicos. Nesse contexto, é possível observar – em diversos setores, no setor público e no setor privado, em organizações de portes variados – um crescente número de ataques cibernéticos e incidentes de segurança envolvendo dados pessoais.

A partir do cenário de vigência da Lei Geral de Proteção de Dados e aumento da ocorrência de incidentes de segurança envolvendo dados pessoais, procurou-se demonstrar que, diante da ocorrência de incidentes de segurança envolvendo dados pessoais, é possível aplicar diferentes formas de tutela, que oferecem respostas mais eficazes aos efeitos gerados por estes eventos e, consequentemente, oferecer melhor proteção aos interesses jurídicos.

A tutela preventiva assume especial relevância na LGPD, que adota abordagem baseada no risco e institui mecanismos de avaliação de riscos à proteção de dados. Inclusive, para fins de verificação da necessidade de comunicar a ocorrência de um incidente à ANPD e aos titulares, é necessário avaliar se tal incidente pode acarretar risco ou dano relevante aos titulares. Nesse contexto, foi demonstrado que a participação da Autoridade Nacional e a divulgação do fato aos titulares também poderá contribuir para a adequada tutela da proteção de dados.

Em relação à tutela contratual, procurou-se demonstrar que a tutela específica deve ser considerada como o principal remédio em casos de inadimplemento dos deveres contratuais, incluindo deveres anexos. Desse modo, entende-se que, diante da ocorrência de incidentes, deve-se buscar, primeiramente, o resultado que decorreria do cumprimento da obrigação estabelecida, caso seja verificada utilidade e possibilidade desta prestação.

Por fim, foram abordados os desafios da tutela ressarcitória, caracterizada pela determinação das perdas e danos, em matéria de privacidade e proteção de dados, demonstrando-se que esta não deve ser considerada como o único ou o principal remédio para situações envolvendo incidentes de segurança com dados pessoais.

Portanto, procurou-se demonstrar que a construção de uma cultura de proteção de dados e a efetivação da proteção da privacidade da pessoa humana dependem de instrumentos de tutela adequados para incidentes de segurança. As formas de tutela em matéria de privacidade e proteção de dados não devem se resumir aos pedidos de indenização pecuniária, pelo contrário, é necessário considerar a abordagem baseada no risco para implementar formas de tutela preventiva e, em caso de ocorrência de incidentes, avaliar as possibilidades de tutela específica no caso concreto.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Comunicação de incidentes de segurança**. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 07 mar. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Minuta de Regulamento de Comunicação de Incidentes com Dados Pessoais. **Consulta Pública Plataforma Participa + Brasil**. Disponível em: https://www.gov.br/participamaisbrasil/regulamento-de-comunicacao-de-incidente-de-seguranca-com-dados-pessoais#:~:text=A%20ANPD%20determinar%C3%A1%20ao%20controlador,tenha%20sido%20comunicado%20pelo%20controlador. Acesso em: 21 jun. 2023.

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**. Rio de Janeiro, a. 9, n. 3, 2020. Disponível em: http://civilistica.com/responsabilidade-civil-na-protecao-de-dados-pessoais/. Acesso em: 07 mar. 2023.

BIONI, Bruno; LUCIANO, Maria. O princípio da precaução da regulação da inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência Artificial e Direito**. São Paulo: Thomson Reuters Brasil, 2019. p. 207-232.

CITRON, Danielle Keats; SOLOVE, Daniel J. Privacy Harms. **Boston University Law Review**, Boston, v. 102, p. 1-62, 2021. Disponível em: https://ssrn.com/abstract=3782222. Acesso em: 07 mar. 2023.

CONSELHO DA JUSTIÇA FEDERAL. **III Jornada de Direito Civil**. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/iii-jornada-de-direito-civil-1.pdf. Acesso em: 07 mar. 2023.

CONSELHO DA JUSTIÇA FEDERAL. **VII Jornada de Direito Civil**. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/vii-jornada-direito-civil-2015.pdf. Acesso em: 07 mar. 2023.

COSTA, Luiz. Privacy and the precautionary principle. **Computer Law & Security Review**, v. 28, n. 1, p. 14-24, 2012. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364911001804?via%3Dihub. Acesso em: 31 jan. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 4/2019 on Article 25 Data Protection by Design and by Default**. Disponível em https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en. Acesso em: 07 mar. 2023.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. **Recommendations for a methodology of the assessment of severity of personal data breaches**. Disponível em: https://www.enisa.europa.eu/publications/dbn-severity. Acesso em: 07 mar. 2023.

FAJNGOLD, Leonardo. **Dano moral e reparação não pecuniária**: sistemática e parâmetros. São Paulo, Thomson Reuters Brasil, 2021.

KONDER, Carlos Nelson. Prefácio. *In*: FAJNGOLD, Leonardo. **Dano moral e reparação** não pecuniária: sistemática e parâmetros (prefácio). São Paulo, Thomson Reuters Brasil, 2021.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. *In*: DONEDA, Danilo et al (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 339-360.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon. A normatividade dos dados sensíveis na Lei Geral De Proteção De Dados: ampliação conceitual e proteção da pessoa humana. **Revista de Direito, Governança e Novas Tecnologias**, Goiânia, v. 5, n. 1, p. 63-85, jun. 2019, p.81.

Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em: 3 jan. 2023.

NEGRI, Sergio Marcos Carvalho de Avila. A tutela específica nos contratos de computação em nuvem (cloud computing). *In*: TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz (org.). **Inexecução das Obrigações Volume II**: pressupostos, evolução e remédios. Rio de Janeiro: Processo, 2021. p. 967-988.

PALHARES, Felipe; PRADO, Luis Fernando; VIDIGAL, Paulo. **Compliance Digital e LGPD**. Coleção Compliance. Coord. NOHARA, Irene; Almeida, Luiz Eduardo. São Paulo: Thomson Reuters Brasil, 2021.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHREIBER, Anderson. **Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais**. *In*: DONEDA, Danilo et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021. p. 319-338.

TEPEDINO, Gustavo. **Inadimplemento contratual e tutelas específicas das obrigações**. Soluções práticas de direito. São Paulo: Revista dos Tribunais, v. II, 2012.
UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Data Protection and Privacy Legislation Worldwide**. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 3 jan. 2023.

ZANATTA, Rafael; SOUZA, Michel. A tutela coletiva na proteção de dados pessoais: tendências e desafios. *In*: DE LUCCA, Newton; ROSA, Cíntia. **Direito & Internet IV**: Proteção de Dados Pessoais. São Paulo: Quartier Latin, 2019.