UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO
CAROLINA FIORINI RAMOS GIOVANINI

INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS:
tutela preventiva, tutela específica e tutela ressarcitória

Juiz de Fora
2022

CAROLINA FIORINI RAMOS GIOVANINI

INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS:
tutela preventiva, tutela específica e tutela ressarcitória

Monografia apresentada à Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Bacharel. Na área de concentração Direito Privado sob orientação do Prof. Dr. Sergio Marcos Carvalho de Ávila Negri.

Juiz de Fora
2022

FOLHA DE APROVAÇÃO

CAROLINA FIORINI RAMOS GIOVANINI

INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS: tutela preventiva, tutela específica e tutela ressarcitória

Monografia apresentada à Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Bacharel. Na área de concentração Direito submetida à Banca Examinadora composta pelos membros:

Orientador: Prof. Dr. Sergio Marcos Carvalho de Ávila Negri.
Universidade Federal de Juiz de Fora

Prof. Ma. Maria Regina Detoni Cavalcanti Rigolon Korkmaz
Universidade Estadual do Rio de Janeiro

Prof. Nathan Paschoalini Ribeiro Batista
Universidade Federal de Juiz de Fora

PARECER DA BANCA

( ) APROVADO

( ) REPROVADO

Juiz de Fora, de de 2022

Dedico este trabalho a Cibelle, Nilma *(in memorian)* e Dorica *(in memorian)*, por todo o esforço que fizeram por mim.

RESUMO

A partir do cenário de vigência da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, abreviada como "LGPD") e da ocorrência de diversos incidentes de segurança envolvendo dados pessoais, o presente artigo, a partir de uma abordagem exploratória, procura demonstrar como diferentes formas de tutela podem ser aplicadas diante da ocorrência de tais eventos, promovendo respostas mais eficazes. A partir da compreensão de 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: proteção de dados; privacidade; incidentes de segurança; Lei Geral de Proteção de Dados.

ABSTRACT

Considering the scenario of the General Law of Personal Data Protection (Law No. 13,709/2018, abbreviated as "LGPD") and the occurrence of several security incidents involving personal data, this study, from an exploratory approach, seeks to demonstrate how different forms of guardianship can be applied before the occurrence of such events, to promote more effective responses. Based on the understanding that the LGPD adopts a risk-based approach, this paper seeks to demonstrate that preventive measures assume a particularly important role in the legal system. However, despite the adoption of preventive measures, security incidents may occur and, in these cases, we tried to point out that specific remedies may be used. Finally, about the compensation of damages in matters of privacy and data protection, this article investigates the challenges of identifying the causal nexus and of the demonstration and quantification of damage, concluding that alternative means of non-pecuniary compensation must be evaluated in concrete situations.

Keywords: data protection; privacy; security incidents; Brazilian General Data Protection Law.

SUMÁRIO

1. INTRODUÇÃO

O primeiro ano de vigência da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018, abreviada como "LGPD") foi marcado pela ocorrência de grandes incidentes de segurança da informação no cenário nacional. A título de exemplificação, é possível citar o "megavazamento" de dados de mais de 220 milhões de brasileiros, que ocorreu no início do ano de 2021 e revelou 37 bases contendo CPFs, nomes, gênero, endereços, escolaridade, classe social, ocupação, situação no Bolsa Família, score de crédito etc[1].

Diariamente, é possível observar 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 mais profundo, especialmente considerando as inúmeras questões jurídicas e potenciais violações de direitos humanos suscitadas por estes eventos. O cenário de crescente utilização de dados pessoais, para além das preocupações decorrentes das atividades de tratamento, também coloca em evidência a importância de garantir que as informações pessoais sejam tratadas com segurança adequada, de modo a evitar danos patrimoniais e extrapatrimoniais aos titulares de dados.

Nesse contexto, a LGPD apresenta disciplina específica para a segurança dos dados pessoais: (i) reconhece a segurança como um dos princípios a serem observados na realização de atividades de tratamento de dados pessoais (art. 6º, VII); (ii) disciplina a responsabilidade dos agentes de tratamento[2] pelos danos decorrentes de violações de segurança (Seção III do Capítulo IV, especialmente art. 44, caput e parágrafo único); (iii) determina a adoção de medidas de segurança (Capítulo VII); e (iv) possibilita a formulação de regras de boas práticas e de governança que estabeleçam normas de segurança (art. 50).

---

[1] Os dados pessoais vazados foram publicados em um fórum on-line caracterizado pela possibilidade de compra e venda de dados. G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 6 janeiro 2022.

[2] 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.

O presente artigo pretende analisar de que modo a tutela preventiva, a tutela específica e a tutela ressarcitória podem ser aplicadas em incidentes de segurança envolvendo dados pessoais. 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). A adoção de tal estratégia metodológica é justificável na medida em que a LGPD completou somente um ano de vigência e, até o momento, não foi possível observar nenhuma atuação da Autoridade Nacional de Proteção de Dados (ANPD) diante de incidentes de segurança, inclusive, a regulamentação do tema está pendente.

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. 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 incidentes de segurança à luz do ordenamento jurídico brasileiro.

Sendo assim, esta investigação, em primeiro lugar, pretende traçar os principais conceitos e referenciais teóricos que orientarão o desenvolvimento dos temas (item 2). Posteriormente, o trabalho discutirá possíveis formas de tutela passíveis de aplicação diante da ocorrência de incidentes de segurança envolvendo dados pessoais (itens 3, 4, 5 e 6).

2. AUTODETERMINAÇÃO INFORMATIVA E INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS

A tutela jurídica de dados pessoais ganha cada vez mais relevância diante do crescente tratamento de dados pessoais em atividades diárias. Nesse contexto, o *General Data Protection Regulation*, abreviado por "GDPR" (Regulamento Geral de Proteção dos Dados Pessoais) entrou em vigência em 2018 na União Europeia. No Brasil, foi publicada a Lei Geral de Proteção de Dados (Lei n° 13.709/2018), abreviada por "LGPD".

A LGPD entrou parcialmente em vigência em 2020 e, em agosto de 2021, passou a estar plenamente vigente, uma vez que as disposições que tratam das sanções também passaram a viger. Negri e Korkmaz (2019) apontam que a LGPD é apresentada como um imperativo da circulação controlada de dados pessoais, sendo um instrumento para a construção de uma cultura de proteção de dados no Brasil e gerando mudanças normativas no ordenamento jurídico.

Nesse sentido, para compreender a tutela estabelecida pelo modelo europeu de proteção de dados, que serviu de inspiração para a construção do modelo brasileiro, é importante ressaltar que o direito à privacidade deixa de se basear em torno do eixo "pessoa-informação-segredo", no paradigma da *zero-relationship*, e passa a estar fundamentado no eixo "pessoa-circulação-controle". Assim, a privacidade – em sua dimensão informacional – passa a ser compreendida 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 art. 2º, II, da LGPD. Danilo Doneda (2020), ao tratar do problema da interpretação sobre o que é a "autodeterminação", esclarece que, de um lado, a expressão poderia ser compreendida como a oportunidade de controlar informações a partir de parâmetros de ampla informação e solidariedade e, por outro lado, a partir de uma interpretação liberal, a autodeterminação estaria compreendida no ato do consentimento e assumiria contornos negociais.

No entanto, uma tutela de dados pessoais fundada em bases essencialmente proprietárias seria incompatível com a consideração da proteção de dados como um direito fundamental. A partir

da compreensão de que a matéria da proteção de dados pessoais não deve ser afastar do âmbito dos direitos da personalidade, entende-se que a autodeterminação informativa não deve ser sintetizada pela mera manifestação de consentimento, mas concretizada pela implementação de instrumentos de controle e *accountability* que assegurem o controle informacional por parte dos indivíduos.

Evidentemente, eventos marcados pela ocorrência de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados pessoais representam uma perda de controle informacional. Tais situações merecem atenção particular e ensejam a criação de instrumentos e técnicas para sua tutela.

Conforme aponta Danilo Doneda (2020), a disciplina da proteção de dados é marcada pela possibilidade de utilização combinada de formas de tutela. Assim, verifica-se que a proteção de dados se afasta do discurso abstrato da privacidade e passa a exigir o estabelecimento de técnicas efetivas de tutela.

Nesse sentido, a LGPD estabelece que os agentes de tratamento devem 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 forma de tratamento inadequado ou ilícito, conforme art. 46 da Lei. Verifica-se que o 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.

Menke e Goulart (2020) apontam, ainda, um quarto elemento: a resiliência. A resiliência é caracterizada pela capacidade de recomposição das estruturas e funcionalidades essenciais após a ocorrência de um evento adverso. O 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.

Nesse sentido, Menke e Goulart (2020) esclarecem que tais atributos 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. Assim, os controles são as medidas adotadas para impedir que um incidente ocorra ou para diminuir a probabilidade de sua ocorrência.

É importante notar que nem todos os incidentes de segurança envolvem dados pessoais. Os dados pessoais são informações que identificam uma pessoa natural – como nome, CPF, RG e demais vínculos direitos – ou a tornam identificável – por exemplo, número de telefone, geolocalização, número do cartão de crédito e outros vínculos indiretos. As informações envolvidas em um incidente de segurança, a depender do caso concreto, podem ser classificadas como dados pessoais, porém, 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.

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 artigo 46 da norma, 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. Observa-se, ainda, que o art. 46 reflete o princípio da segurança, previsto no art. 6º, VII, da LGPD.

A Autoridade Nacional de Proteção de Dados - ANPD (órgão da administração pública federal, integrante da Presidência da República, responsável por zelar pela proteção dos dados pessoais, e por orientar, regulamentar e fiscalizar o cumprimento da legislação) estabelece que um "incidente de segurança com dados pessoais" é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Desse modo, observa-se, em primeiro lugar, que a definição adotada pela ANPD acertadamente restringe os incidentes somente aos eventos adversos confirmados, ou seja, a mera suspeita não é classificada como "incidente de segurança com dados pessoais". Entende-se que tal restrição

conceitual é adequada pois, caso contrário, o escopo da definição seria demasiadamente amplificado e poderia ensejar inadequadamente a tomada de providências previstas pela lei.

No entanto, embora a definição adotada pela ANPD esteja amparada na redação do art. 46 da LGPD e faça referência somente aos eventos confirmados, trata-se de um conceito amplo e extensivo, uma vez que estabelece que, além de eventos adversos relacionados à violação de segurança, "qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais" pode ser considerada um incidente de segurança com dados pessoais.

Nesse sentido, 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. Em primeiro lugar, ressalta-se que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação em relação aos dados pessoais, mesmo após o término do tratamento (*security by design*), conforme prevê o art. 47 da LGPD.

Além disso, o art. 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.

Na mesma direção, o *European Data Protection Board*, 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 tratamento, o cumprimento dos demais princípios e o exercício efetivo dos direitos dos titulares.

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

Bioni e Dias (2020) questionam-se se, em caso de violação da segurança dos dados, o agente responderia se não adotasse as medidas de segurança aptas a protegê-los, ou se o tratamento não fornecesse a segurança que o titular dele pode esperar. Para os autores, o critério de adoção de medidas aptas é demasiadamente amplo, por isso, apontam que a análise da segurança esperada pelo titular seria mais frutífera. Desse modo, Bioni e Dias (2020) entendem 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.

No entanto, também 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 adotadas pelas áreas técnicas que lidam com a segurança da informação.

Assim, entende-se que a violação da segurança dos dados deve ser analisada a partir das justificativas 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 (MENKE; GOULART, 2020).

Vale ressaltar que 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, especialmente no caso de dados pessoais sensíveis. Desse modo, verifica-se que, 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.

Embora a ANPD possa dispor sobre padrões técnicos mínimos, é importante observar que, 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 art. 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.

O Decreto n° 8.771/2016 já apresentava relevante preocupação com o acesso às informações referentes ao tratamento de dados pessoais, 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. Conforme aponta Sombra (2019), o direito de acesso à informação é a principal matriz de garantias asseguradas aos titulares de dados.

Além disso, é importante observar que determinados setores possuem requisitos de segurança específicos ou exigem que os agentes regulados adotem determinadas estruturas e padrões técnicos. A título de exemplificação, é possível citar que a Agência Nacional de Energia Elétrica (Aneel) aprovou a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica, conforme Resolução Normativa nº 964/2021. O setor financeiro também é um exemplo de setor altamente regulado e que conta com requisitos próprios de segurança, conforme é possível extrair da Resolução CMN nº 1.893/2021 e Resolução BCB nº 85/2021.

A compreensão de que agentes de tratamento devem enxergar a segurança como um elemento sempre presente durante a atividade de tratamento de dados pessoais é reforçada pelo princípio da responsabilização e prestação de contas, previsto no art. 6º, X, da LGPD, que determina a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a

observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Desse modo, a implementação de medidas de segurança e padrões técnicos adequados durante todo o ciclo de vida dos dados pessoais é essencial. A segurança deve ser um fator considerado antes mesmo do início das atividades de tratamento, ou seja, a estruturação de rotinas e padrões que assegurem a segurança das informações não deverá ser iniciada somente após a ocorrência de um incidente.

É importante notar que incidentes de segurança podem desencadear uma série de violações às normas de proteção de dados. A título ilustrativo, é possível exemplificar que incidentes que acarretem alteração de dados pessoais ensejam violação ao princípio da qualidade (art. 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 (art. 18, da LGPD). Conforme aponta o *European Data Protection Board*, as violações de dados são problemas em si, mas também podem ser sintomas de um regime de segurança de dados vulnerável e possivelmente insuficiente.

Para além do aspecto jurídico, incidentes de segurança geram uma série de consequências para organizações que conduzem negócios: quebra da confiança de clientes e investidores, impactos reputacionais, paralização de operações, custos para gerenciar o evento e, quando necessário, cumprir o dever de comunicação etc. Em síntese, a ocorrência de um incidente de segurança poderá impactar ativos da organização e comprometer suas operações. Por isso, é necessário direcionar esforços para prevenir tais eventos adversos e, caso ocorram, implementar medidas para sua contenção.

O artigo 48 da LGPD estabelece 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. Desse modo, é possível observar que nem todos os incidentes de segurança envolvendo dados pessoais deverão ser notificados, mas tão somente aqueles que tenham o potencial de causar risco ou dano relevante aos titulares.

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 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 ressaltar que a ANPD iniciou, em 2021, o processo de regulamentação sobre incidentes de segurança, conforme prevê o art. 48 da LGPD e como parte de sua agenda regulatória, aprovada pela Portaria nº 21 de 27 de janeiro de 2021. Nesse contexto, foram apresentadas questões sobre critérios para avaliação de risco ou dano relevante, distinção entre risco ou dano, considerações a serem levadas em consideração na avaliação de risco ou dano, quais informações os controladores devem apresentar à ANPD e aos titulares, definição do prazo razoável para informar tanto a ANPD quanto os titulares e possíveis exceções quanto ao dever de notificação. No entanto, no presente momento, o processo de regulamentação ainda não foi concluído.

Em que pese a ausência de regulamentação, a ANPD fornece algumas orientações acerca da comunicação de incidentes de segurança[3], estabelecendo que é necessário avaliar internamente natureza, categoria e quantidade de titulares de dados afetados, bem como categoria e quantidade dos dados afetados pelo incidente, consequências concretas e prováveis do ocorrido. Além disso, a ANPD orienta que seja elaborada documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, conforme princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD).

Cabe ressaltar que a ANPD recomenda que controladores adotem posição de cautela e efetuem a comunicação mesmo nos casos em que a relevância dos riscos e danos envolvidos é incerta. Além disso, embora a LGPD não estabeleça critérios e metodologias para a avaliação de riscos, é importante que os agentes de tratamento estabeleçam uma metodologia e registrem as etapas de avaliação, uma que eventual e comprovada subavaliação dos riscos e danos por parte dos controladores poderá vir a ser caracterizada como descumprimento à legislação de proteção de dados pessoais.

[3] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de incidentes. Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>. Acesso em 04 fev. 2022.

No que diz respeito ao prazo para comunicação, a LGPD prevê que esta deverá ser realizada em "prazo razoável", porém, enquanto ainda não há regulamentação por parte da ANPD, o órgão recomenda que, após a ciência do evento adverso e havendo risco relevante, a comunicação à ANPD seja feita com a maior brevidade possível, indicando o prazo de 2 dias úteis, contados da data do conhecimento do incidente. Tal prazo é inspirado no Decreto nº 9936/2019, que regulamenta a Lei do Cadastro Positivo (Lei nº 12.414/2011).

Nota-se que o prazo sugerido pela ANPD é exíguo e, por vezes, será desafiador. Para além do prazo de comunicação, o contexto de ocorrência de um incidente de segurança envolvendo dados pessoais levanta diversas preocupações e efeitos jurídicos internos e externos, sendo essencial que os agentes de tratamento adotem posturas preventivas e se preocupem com o estabelecimento de procedimentos e rotinas internas relacionados a um incidente, assegurando que a contenção do incidente e a avaliação de riscos sejam endereçadas adequadamente[4].

[4] Cabe ressaltar que o artigo 52, §1º, inciso VIII, da LGPD estabelece que, ao aplicar sanções, a ANPD irá considerar a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados.

3. FORMAS DE TUTELA

3.1. Tutela preventiva: diálogos entre prevenção, precaução e abordagem baseada no risco

A LGPD estabelece o princípio da prevenção (art. 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. Desse modo, 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.

Por outro lado, embora não esteja expressamente previsto no texto da LGPD, o princípio da precaução pode ser observado no ordenamento jurídico brasileiro[5] e, no âmbito da privacidade e da proteção de dados, poderá contribuir para a consolidação de uma abordagem baseada no risco (*risk based approach*)[6]. 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.

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. O autor destaca que a avaliação de risco e o princípio da precaução andam juntos, pois são instrumentos que determinam conjuntamente a atribuição da avaliação dos riscos e do custo dos danos.

---

[5] Bioni e Luciano 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 (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. 210).

[6] Nesse sentido, Gellert esclarece que o risco sinaliza a ameaça de dano de modo mensurável, desse modo, a noção de risco pode ser compreendida como uma ferramenta para a tomada de decisões, possibilitando que eventos futuros sejam gerenciados para se tornarem certos e controláveis. Para o autor, a proteção de dados é uma regulação de risco (GELLERT, Raphael. Data protection: a risk regulation?: between the risk management of everything and the precautionary alternative. International Data Privacy Law,, [s. l], v. 5, n. 1, p. 3-19, mar. 2015. Disponível em: https://academic.oup.com/idpl/article-abstract/5/1/3/622981?redirectedFrom=fulltext. Acesso em: 16 jan. 2022).

Para a 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, não podem ser identificados. Assim, tratando especificamente da ocorrência de um evento adverso classificado como incidente de segurança da informação envolvendo dados pessoais, verifica-se que não há certeza técnica da ocorrência deste evento, mas é necessário implementar medidas que possam prevenir eventuais danos.

Gellert (2015) aponta que o princípio da precaução pode ser aplicado à proteção de dados e à abordagem baseada em risco de duas formas: (i) em primeiro lugar, a partir da incorporação de exercícios de participação pública, que possibilitem a avaliação de outros valores relevantes e de diferentes tipos de experiência e conhecimento, ou seja, a incorporação do princípio da precaução à disciplina da privacidade traria maior complexidade às ferramentas de gestão de risco; e (ii) em segundo lugar, por meio do enriquecimento do arcabouço legal já constituído em relação ao restante do quadro jurídico de proteção de dados poderia

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 um dever de cuidado. Conjuntamente, prudência e precaução implicam que as atividades devem ser realizadas de forma a evitar que efeitos prejudiciais atinjam outras pessoas, possibilitando o desenvolvimento com segurança.

Assim, o art. 47 da LGPD estabelece o dever de garantir a segurança da informação em relação aos dados pessoais, mesmo após o término do tratamento. Tal abordagem pode ser denominada *security by design*, uma vez que exige que os agentes de tratamento considerem os requisitos de segurança o mais cedo possível no design e desenvolvimento da atividade de tratamento, isto é, desde o momento da concepção desta atividade, de modo a prevenir a ocorrência de danos.

A previsão reflete o princípio da "segurança de ponta a ponta", presente na metodologia denominada *Privacy by Design*, desenvolvida por Ann Cavoukian, *information and privacy commissioner* de Ontario, no Canadá, em seu artigo "*Privacy by Design: the 7 Foundational Principles*". A partir do princípio da segurança de ponta a ponta, verifica-se que a implementação, por parte dos agentes de tratamento, de um Procedimento de *Privacy by Design* poderá impulsionar a adoção de medidas robustas de segurança desde o momento da concepção

de uma nova atividade de tratamento de dados pessoais. Cavoukian (2006) esclarece que a incorporação da privacidade desde o momento da concepção se estende com garantia de segurança por todo o ciclo de vida dos dados envolvidos. Desse modo, assegura-se que os dados sejam retidos com segurança e, em seguida, destruídos com segurança ao término do tratamento.

Assim, entende-se que os agentes de tratamento devem adotar medidas, rotinas e práticas que contribuem para a efetivação do princípio da prevenção e concretizam a tutela preventiva em matéria de privacidade e proteção de dados pessoais. Em primeiro lugar, cabe ressaltar que a construção de uma cultura de segurança das informações depende da realização de treinamentos e implementação de medidas de conscientização, por exemplo, infográficos, cartilhas, vídeos e ações transversais e multidisciplinares que reforcem a importância do tema e forneçam orientações para atuação adequada.

Para melhor incorporação do tema e funcionamento efetivo das rotinas de segurança estabelecidas, agentes de tratamento podem organizar os treinamentos conforme o público que participará destes. Nesse sentido, é possível realizar treinamentos formatos gerais – disponibilizados para toda a organização – e em formatos específicos e personalizados, envolvendo somente as áreas que efetivamente atuarão e tomarão decisões caso um incidente ocorra, de modo a possibilitar simulações práticas e objetivas.

O desenvolvimento e a efetiva implementação de uma Política de Segurança da Informação que estabeleça 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. Tal documento poderá estabelecer a coordenação entre diferentes áreas e funções por meio da definição de responsabilidades e linhas de reporte.

Além disso, observa-se que o art. 39 da LGPD determina que o controlador deverá verificar se o operador observa as normas de proteção de dados. Por isso, é necessário assegurar que operadores envolvidos em atividades de tratamento adotem padrões de segurança adequados. Tal dever legal ensejará a gestão de terceiros por meio de arranjos contratuais e avaliações de maturidade em privacidade (por exemplo, a partir da análise do histórico de ocorrências de incidentes em uma organização e de investigações e processos judiciais ou administrativos envolvendo a ocorrência de incidentes) e, eventualmente, da verificação de cumprimento de

determinados requisitos de segurança. 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.

Desse modo, a atuação preventiva e proativa do agente de tratamento poderá ser concretizada a partir de padrões técnicos, mas também por meio de uma estrutura de governança sólida. 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.

Evidentemente, a imposição de obrigações de fazer e não fazer adequadas à prevenção devem ser avaliadas à luz da proporcionalidade, de modo a não trazer um peso excessivo para o responsável, ou seja, a adoção de tais medidas deverá ser analisada de acordo com cada situação concreta. Por fim, ressalta-se que, ainda que as medidas preventivas sejam devidamente adotadas e efetivamente praticadas na rotina de uma organização, um incidente de segurança envolvendo dados pessoais poderá ocorrer e, nesse caso, outras formas de tutela poderão ser aplicadas.

3.2. Tutela específica: o incidente de segurança como momento patológico da relação contratual

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. No âmbito da privacidade e da proteção de dados pessoais, isso significa 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.

Um contrato envolvendo o tratamento de dados pessoais poderá prever cláusulas que disponham sobre a segurança do tratamento. Por exemplo, no caso de uma relação entre controlador e operador, é possível prever que, em caso de indícios de violação, há obrigações

como a necessidade de comunicação por parte do operador e a implementação imediata de procedimentos de contenção do evento. Por outro lado, no caso de relações entre controladores, há possibilidade de previsão de deveres de comunicação e tomada de decisão conjunta acerca das medidas necessárias para contenção, bem como prestação de auxílio mútuo.

O ordenamento jurídico brasileiro prevê diversos remédios passíveis de aplicação em situações envolvendo inadimplemento. No âmbito das relações contratuais, um incidente de segurança envolvendo dados pessoais poderá ser compreendido como um momento patológico quando originado pelo descumprimento do dever de segurança estabelecido entre as partes.

O Art. 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, tal dispositivo não deve ser interpretado no sentido de que a tutela ressarcitória seria o principal remédio para casos de inadimplemento contratual.

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 casa de impossibilidade de tutela específica ou de obtenção do resultado prático correspondente.

Desse modo, verifica-se 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.

Em matéria de privacidade e proteção de dados pessoais, é possível que – em relações contratuais – o outro agente de tratamento ou o próprio titular 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.

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 art. 12 do Código Civil[7] refere-se às técnicas de tutela específica, aplicáveis de ofício, enunciadas no art. 461 do Código de Processo Civil (nesse caso, faz-se referência ao CPC de 1973)[8], 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. A título de exemplificação, é possível vislumbrar – a depender das peculiaridades do caso concreto – a obtenção de tutelas consistentes na adoção de medidas voltadas para a contenção do incidente, na implementação das rotinas previstas no plano de resposta à incidentes, na varredura e remoção de bancos de dados vazados e disponibilizados na *web* e na *deep* web, na criação de página e canal de comunicação específico para orientações acerca de determinado incidente, no dever de comunicação previsto pelo artigo 48 da LGPD e diversas outras medidas capazes de coibir ameaças e evitar danos após a ocorrência de um incidente.

---

[7] Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.

[8] Art. 461. Na ação que tenha por objeto o cumprimento de obrigação de fazer ou não fazer, o juiz concederá a tutela específica da obrigação ou, se procedente o pedido, determinará providências que assegurem o resultado prático equivalente ao do adimplemento. Ressalta-se que, no CPC de 2015, o art. 497 é o dispositivo correspondente: Art. 497. Na ação que tenha por objeto a prestação de fazer ou de não fazer, o juiz, se procedente o pedido, concederá a tutela específica ou determinará providências que assegurem a obtenção de tutela pelo resultado prático equivalente.

Nesse sentido, vale ressaltar que a pesquisa "Relatório Anual de Jurimetria 2021" demonstra que 80% das condenações envolvendo a Lei Geral de Proteção de Dados geraram obrigações de fazer ou não fazer e em 20% dos casos, as condenações somente geraram indenização pecuniária[9]. 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 e, quando se verificar em concreto a impossibilidade da prestação, o credor poderá recorrer à execução pelo equivalente e ao direito potestativo de resolver o contrato e, consequentemente, extinguir a relação contratual, nos termos do artigo 475 do Código Civil, cabendo, em ambos os casos, perdas e danos.

3.3. Tutela ressarcitória: subsidiariedade e possibilidades de reparação não pecuniária

Conforme buscou-se demonstrar, a tutela ressarcitória, concretizada a partir da verificação das perdas e danos e consequente indenização, assume caráter subsidiário no ordenamento jurídico brasileiro. Doneda (2020) aponta que a tutela baseada na responsabilidade civil oferece uma visão predominantemente patrimonialista do problema. Evidentemente, 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 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. Para além dos desafios relacionados à demonstração do dano, nota-se que a aferição do nexo causal também poderá ser particularmente complexa. 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.

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

[9] LEGAL INNOVATION. LGPD Lookout Relatório Anual de Jurimetria 2021. Disponível em: <https://opiceblum.com.br/wp-content/uploads/2019/07/Relatorio_Anual_Jurimetria_28.01_versao_final.pdf>. Acesso em: 02 fev. 2022.

termos do art. 42, da LGPD. Assim, é necessário que, no caso concreto, seja verificada a existência de um dano[10].

Citron e Solove (2020) indicam a existência de quatro desafios relacionados aos danos à privacidade. Em primeiro lugar, os autores 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 por 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 do ponto de vista da sociedade há uma agravação do dano pela agregação.

Em terceiro lugar, Citron e Solove (2020) esclarecem 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, em quarto lugar, os autores destacam que os danos à privacidade geralmente envolvem não apenas os interesses individuais, mas também interesses coletivos, colocando em evidência a dimensão coletiva da privacidade.

No que diz respeito aos incidentes de segurança envolvendo dados pessoais, é importante que, no caso concreto, seja verificada a existência de um dano, caso contrário, não haverá aplicação do regime de responsabilidade civil. Nesse sentido, o parágrafo único do art. 44 da LGPD estabelece que o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46, der causa aos danos decorrentes da violação da segurança dos dados, responderá por estes danos.

No que diz respeito à reparação civil, é importante notar que o cenário de banalização das condenações – no qual é possível verificar diminuição de valores, confusões entre critérios

[10] Faz-se necessário ressaltar que, no processo civil, o juiz poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa, conforme art. 42, §3º, da LGPD.

patrimoniais e existenciais – demanda reflexões acerca da despatrimonialização da reparação (KONDER, 2021).

O processo de despatrimonialização da reparação abrange os meios não pecuniários, que podem ser aplicados para maximizar a promoção de interesses existenciais. Nesse sentido, destaca-se que o Supremo Tribunal Federa[11] 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.

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, a implementação destes mecanismos possivelmente gera gastos ao ofensor.

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 art. 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.

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,

---

11 STF, Tribunal Pleno, RE 580.252/MS, Rel. Min Teori Zavascki, Rel. p/ acórdão Min. Gilmar Mendes, j. 16/02/2017.

religiosas e associativas. Nesse contexto, os autores ressaltam 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: uma forma de reparação não pecuniária pode ter maior aptidão reparatória do que o mero recebimento de uma determinada quantia (FAJNGOLD, 2021).

Assim, 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.

4. CONCLUSÃO

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 execução 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 (dever de segurança), 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. Assim, 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 BIBLIOGRÁFICAS

ANEEL. Resolução Normativa nº 964/2021. Disponível em < https://www2.aneel.gov.br/cedoc/ren2021964.html>. Acesso em: 6 jan. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de incidentes de segurança. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>. Acesso em: 6 jan. 2022.

BANCO CENTRAL DO BRASIL. Resolução BCB nº 85/2021. Disponível em <https://www.in.gov.br/en/web/dou/-/resolucao-bcb-n-85-de-8-de-abril-de-2021-313194098>. Acesso em: 6 jan. 2022.

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: 6 jan. 2022.

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.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 6 jan. 2022.

_____. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Disponível em < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 6 jan. 2022.

_____. Decreto nº 8.771, de 11 de maio de 2016. **Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações**. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm>. Acesso em: 6 jan. 2022.

_____. Lei n° 13.105, de 16 de março de 2015. **Código de Processo Civil**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em: 6 jan. 2022.

_____. Lei n° 10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 6 jan. 2022.

CAVOUKIAN, Ann. The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices. Disponível em: <https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf>. Acesso em: 6 jan. 2022.

CITRON, Danielle Keats; SOLOVE, Daniel J.. Privacy Harms. **Boston University Law Review**, Boston, v. 102, p. 1-62, fev. 2021. Disponível em: https://ssrn.com/abstract=3782222. Acesso em: 16 jan. 2022.

CMN. Resolução CMN 4.893/2021. Disponível em < https://www.in.gov.br/en/web/dou/-/resolucao-cmn-n-4.893-de-26-de-fevereiro-de-2021-305689973>. Acesso em: 6 jan. 2022.

COSTA, Luiz. Privacy and the precautionary principle. **Computer Law & Security Review**, [s. l], v. 28, n. 1, p. 14-24, fev. 2012. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364911001804?via%3Dihub. Acesso em: 16 jan. 2022.

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: 6 jan. 2022.

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

GELLERT, Raphael. Data protection: a risk regulation?: between the risk management of everything and the precautionary alternative. **International Data Privacy Law**,, [s. l], v. 5, n.

1, p. 3-19, mar. 2015. Disponível em: https://academic.oup.com/idpl/article-abstract/5/1/3/622981?redirectedFrom=fulltext. Acesso em: 16 jan. 2022.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml>. Acesso em: 6 jan. 2022.

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

LEGAL INNOVATION. LGPD Lookout Relatório Anual de Jurimetria 2021. Disponível em: <https://opiceblum.com.br/wp-content/uploads/2019/07/Relatorio_Anual_Jurimetria_28.01_versao_final.pdf>. Acesso em: 02 fev. 2022.

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. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf. Acesso em: 6 jan. 2022.

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.

SOMBRA, Thiago Luís Santos. **Fundamentos da regulação da privacidade e proteção de dados pessoais**: pluralismo jurídico e transparência em perspectiva. São Paulo: Thomson Reuters Brasil, 2019.

SUPREMO TRIBUNAL FEDERAL, Tribunal Pleno, RE 580.252/MS, Rel. Min Teori Zavascki, Rel. p/ acórdão Min. Gilmar Mendes, j. 16/02/2017.

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.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679. Regulamento Geral sobre Proteção de Dados**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT >. Acesso em: 6 jan. 2022.

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. ISBN: 9788574538389.